MSBTE NOTES PRESENTS

Best notes on msbte notes free

Syllabus

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics
UNIT - I Artificial Intelligence (06m, 4 hrs) [Refer chapter 1]	1a) Describe the concept of AI. 1b) State the components of AI. 1c) List applications of AI 1d) Differentiate between machine learning & deep learning.	**1.1 Introduction of AI** • Concept • Scope of AI • Components of AI • Types of A I • Application of AI **1.2 Concept of machine learning and deep learning.**

UNIT - II Internet of Things (18m, 12 hrs) [Refer chapters 2 and 3]	2a. State the domains and application areas of Embedded Systems
	2b. Describe IoT systems in which information and knowledge are inferred from data.
	2c. Describe designs of IoT.
	2d. State IoT Issues and challenges in deployment.
		2.1 Embedded Systems:
		• Embedded system concepts, purpose of Embedded Systems, Architecture of Embedded Systems, Embedded Processors- PIC, ARM, AYR, ASIC
		2.2 IoT : Definition and characteristics of IoT
		• Physical design of IoT,
		  ○ Things of IoT
		  ○ IoT Protocols
		• Logical design of IoT,
		  ○ IoT functional blocks,
		  ○ IoT Communication models
		  ○ IoT Communication APIs,
		• IoT Enabling Technologies
		• IoT levels and deployment templates.
		• IoT Issues and Challenges, Applications
		• IoT Devices and its features; Arduino, Uno, Raspberry, Pi, Node Microcontroller Unit.

UNIT- III Unit III: Basics of Digital Forensics (Sm-5 hrs) [Refer chapter 3]	3a. Describe the history of digital forensics 3b. Define digital forensics. 3c. List the rules of digital forensic 3d. Describe the given model of digital forensic investigation. 3e. State the ethical and unethical issues in digital forensics	**3.1 Digital forensics** • Introduction to digital forensic • History of forensic • Rules of digital forensic • Definition of digital forensic • Digital forensics investigation and its goal **3.2 Models of Digital Forensic Investigation** • Digital Forensic Research Workshop Group (DFRWS) Investigative Model • Abstract Digital Forensics Model (ADFM) • Integrated Digital Investigation Process (IDIP) • End to End digital investigation process (EEDIP) • An extended model for cyber crime investigation • UML modeling of digital forensic process model (UMDFPM)

Unit	Unit Outcomes (TOs) (in cognitive domain)	Topics and Sub-topics
		3.3 **Ethical Issues in digital forensic** • General ethical norms for investigators • Unethical norms for investigation
UNIT-IV *Digital Evidence* Refer chapter 5	4a. Define digital evidence. 4b. List the rules of digital evidence. 4c. State characteristics of digital evidence. 4d. Describe the given type of evidence. 4e. Describe the given evidence handling procedures.	4.1 **Digital Evidences** • Definition of Digital Evidence • Best Evidence Rule • Original Evidence 4.2 **Rules of Digital Evidence** 4.3 **Characteristics of Digital Evidence** • Locard's Exchange Principle • Digital Stream of bits 4.4 **Types of evidence** • Authentication of evidence • Chain of custody • Evidence validation 4.6 **Volatile evidence**
UNIT-V *Basics of Hacking* Refer chapter 6	5a) Define hackers. 5b) Describe the need to hack your own systems. 5c) Describe the dangers in systems. 5d) Describe the Ethical hacking Process. 5e) Identify the Hacker's Mindset	5.1 **Ethical Hacking** • How Hackers Beget Ethical Hackers • Defining hacker, Malicious users 5.2 **Understanding the need to hack your own systems** 5.3 **Understanding the dangers your systems face** • Nontechnical attacks • Network-infrastructure attacks • Operating-system attacks • Application and other specialized attacks 5.4 **Obeying the Ethical hacking Principles** • Working ethically • Respecting privacy • Not crashing your systems 5.5 **The Ethical hacking Process** • Formulating your plan • Selecting tools • Executing the plan • Evaluating results • Moving on 5.6 **Cracking the Hacker Mindset** • What You're Up Against? • Who breaks in to computer systems? • Why they do it? • Planning and Performing Attacks • Maintaining Anonymity
UNIT-VI Basics of Hacking Refer chapter 6	6a. Describe Network Infrastructure Vulnerabilities (wired/wireless) 6b. List operating system Vulnerabilities 6c. Describe Messaging Systems	6.1 **Network Hacking Network Infrastructure:** • Network Infrastructure Vulnerabilities • Scanning-Ports • Ping sweep

Unit	Unit Outcomes (UOs) (in cognitive domain)	Topics and Sub-topics

	Vulnerabilities
	6d. Describe Web Vulnerabilities
	6e. Describe Database Vulnerabilities
		• Scanning SNMP
		• Grabbing Banners
		• Analysing Network Data and Network
		  Analyzer
		• MAC – daddy attack
		• Wireless LANs:
		• Implications of Wireless Network
		  Vulnerabilities,
		• Wireless Network Attacks
		
		6.2 Operating System Hacking
		• Introduction of Windows and Linux
		  Vulnerabilities
		
		6.3 Applications Hacking Messaging Systems
		• Vulnerabilities,
		• E-Mail Attacks- E-Mail Bombs,
		  Banners,
		• Best practices for minimizing e-mail security
		  risks
		
		Web Applications:
		• Web Vulnerabilities,
		• Directories Traversal and Countermeasures,
		
		Data base system
		• Database Vulnerabilities
		• Best practicesfor minimizing database
		  security risks

□□□

CHAPTER 1

Introduction of AI

Introduction

1.1.1 Introduction of intelligence

- Intelligence is a quick and accurate response to a situation. As in the examination, scoring of marks up to a certain level of excellence measures the intelligence of the person concerned.

- The response score has to be obtained in a given time.

- How accurately one answers a question is important. How accurately one answers corresponds to quickness, Stipulated or scheduled time corresponds to accuracy, and the right answer to accuracy.

- This is what we observe in practice, day-to-day activities too.

- There are two other domains of knowledge i.e. philosophy and psychology, which conceptualize and define the term Intelligence in a different way; but it turns out to be the same manifestation (understanding) as it is accepted by the common man.

- Intelligence is concerned with reasoning in general and logical approach in particular. Even if one answers accurately a numerical problem but due to lack of logical approach to the problem, he or she may not score equal or more in comparison to the person who makes a logical approach but with a wrong answer.

- Logical approach with approximate numeric answer in philosophy and also in practice is associated with the level of appreciation of the actor (who works).

- In psychology, intelligence involves learning, adaptation and self-organization in response to known or unknown situations or stimuli.

- The response to a learnt situation, through adaptation and self-organization to an unknown situation, displays the sign of intelligence for humans as well as animals.

- These concepts in philosophy and psychology correspond to human beings, but not to machine, the inanimate entity which is still an open problem.

1.1.1.1 Introduction of Artificial Intelligence (AI)

- The art and science of bringing learning, adaptation and self-organization to the machine is that the art of AI.

- Artificial intelligence, in essence, is not only the science of computation but also the logic of cognition.

- As the information processing paradigm of human beings induced the model of a computing system, likewise the logic of cognition generated the methodologies for the origin of AI and its dimensions.

- The IBM sponsored a summer workshop at Dartmouth, New Hampshire, USA, in June 1956.

- Pioneer researchers in the area of computer science, logic, geometry, mathematics and cognitive psychology gathered to discuss the specific topics such as automatic theorem proving and new programming languages.

- Among the participants in the seminal conference were Claude Shannon from IBM, John McCarthy from MIT, and Edward Feigenbaums from Stanford University, along with Herbert Simon and Allen Newell, and many others.

- The important outcome of the conference was the coining of the term Artificial intelligence, which encompasses many concepts and methods deployed by researchers in many diverse fields of computation and cognition.

1.1.2 Components of AI

- The core components and constituents of AI are derived from the concept of logic, cognition and computation; and the compound components, built-up through core components are knowledge, reasoning, search, natural language processing, vision, etc. as shown in Table 1.1.1.

Table 1.1.1 : Three-level compound of AI

Level	Core	Compound	Coarse compound
Logic	Induction	Knowledge	Knowledge based systems
	Proposition	Reasoning	
	Tautology	Control	Heuristic search
	Model logic	Search	Theorem proving
	Temporal		
	Learning	Belief	Multi-agent system
Cognition	Adaptation	Desire	
	Self-organization	Intention	Cooperation
			Coordination
			AI programming languages
Functional	Memory	Vision	Natural language processing
	Perception	Utterance	Speech processing

- The physical entities generate some functions to make the compound components.

- The compound components are made of some combination of the logic and cognition stream.

- These are knowledge reasoning and control generated from constituents of logic such as predicate calculus, induction and tautology and some from cognition (such as learning and adaptation).

- Similarly, belief, desire and intention are models of mental states that are predominantly based on cognitive components but less on logic.

- Vision, utterance (vocal) and written) are combined effect of memory and perceiving organs or body sensors such as car, eyes and vocal.

- The gross level contains the constituents at the third level which are knowledge-based systems (KBS), heuristic search, automatic theorem proving, and multi-agent systems.

- AI languages such as PROLOG and LISP, Natural language processing (NLP), Speech processing and vision are based mainly on the principle of pattern recognition.

AI Dimension

- The philosophy of AI in three-dimensional representations consists in logic, cognition and computation in the x-direction, knowledge, reasoning and interface in the y-direction.

- The x-y plane is the foundation of AI. The z-direction consists of correlated systems of physical origin such as language, vision and perception as shown in Fig. 1.1.1.

- The core entities are inseparable constituents of AI in that these concepts are fused at atomic level.

- The concepts derived from logic are propositional logic, tautology, predicate calculus, model and temporal logic.

- The concepts of cognitive science are of two types; one is functional which includes learning, adaptation and self-organization, and the other is memory and perception which are physical entities.
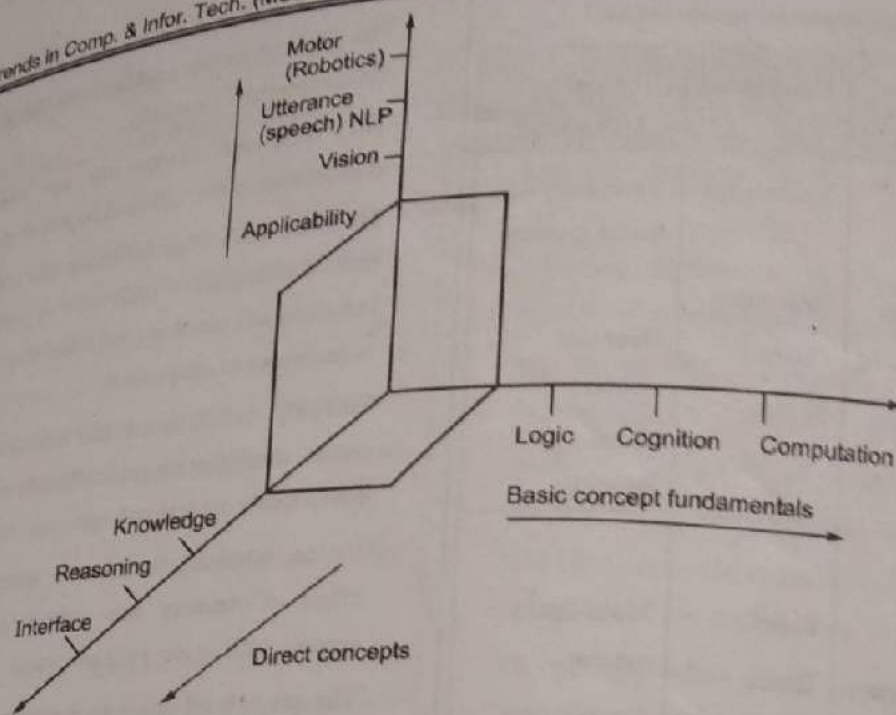
Fig. 1.1.1 : Three dimensional Model of AI

The First Dimension (Core)

– The theory of logic, cognition and computation constitutes the fusion factors for the formation of one of the foundations on coordinate x-axis. Philosophy from its very inception of origin covered all the facts, directions and dimensions of human thinking output.

– Aristotle's theory of syllogism Descartes and Kant's critic of pure reasoning and contribution of many other philosophers made knowledge-based on logic.

– It was Charles Babbage and Boole who demonstrated the power of computation logic. Although the modem philosophers such as Bertrand Russell correlated logic with mathematics but it was Turing who developed the theory of computation for mechanization in the 1960s. Marvin Minsky pushed the logical formalism to integrate reasoning with knowledge.

Cognition

– Computers became so popular in a short span of time due to the simple reason that they adapted and projected the information processing paradigm (IPP) of human beings: sensing organs as input, mechanical movement organs as output and the central nervous system(CNS) in brain as control and computing devices, short-term and long-term memory were not distinguished by computer scientists but, as a whole, it was in conjunction termed memory.

– In further deepening level, if one goes into the EPP, the interaction of stimuli with the stored information to produce new information requires the process of learning, adaptation and self-organization.

– These functionalities in the information processing at a certain level of abstraction of brain activities demonstrate a state of mind which exhibits certain specific behaviour to qualify as intelligence.

– Computational models were developed and incorporated in machines which mimicked the functionalities of human origin.

– The creation of such traits of human beings in the computing devices and processes originated the concept of intelligence in machine as virtual mechanism.

– These virtual machines were termed in due course of time artificial intelligent machines.

Computation

- The theory of computation developed by Turing finite state automation was a turning point in mathematical model to logical computational.

- Chomsky's linguistic computational theory generated a model for syntactic analysis through a regular grammar.

The Second Dimension

- The second dimension contains knowledge, reasoning and interface which are the components of knowledge-based system (KBS) Knowledge can be logical, it may be processed as information which is subject to further computation.

- This means that any item on the y-axis is correlated with any item on the x-axis to make the foundation of any item on the z-axis.

- Knowledge and reasoning are difficult to prioritize, which occurs first: whether knowledge is formed first and then reasoning is performed or as reasoning is present, knowledge is formed.

- Interface is a means of communication between one domain to another. Here, it connotes a different concept then the user's interface.

- The formation of a permeable membrane or transparent solid structure between two domains of different permittivity is termed interface.

- For example, in the industrial domain, the robot is an interface.

- A robot exhibits all traits of human intelligence in its course of action to perform mechanical work. In the KBS, the user's interface is an example of the interface between computing machine and the user. Similarly, a program is an interface between the machine and the user.

- The interface may be between human and human, i.e. experts in one domain to experts in another domain. Human-to-machine is program and machine-to-machine is hardware.

- These interfaces are in the context of computation and AI methodology.

The Third Dimension

- The third dimension leads to the orbital or peripheral entities, which are built on the foundation of x—y plane and revolve around these for development.

- The entities include an information system. NLP, for example, is formed on the basis of the linguistic computation theory of Chomsky and concepts of interface and knowledge on y-direction.

- Similarly, vision has its basis on some computational model such as clustering, pattern recognition computing models and image processing algorithms on the x-direction and knowledge of the domain on the y-direction.

- The third dimension is basically the application domain. Here, if the entities are near the origin, more and more concepts are required from the x-y plane.

- For example, consider information and automation, these are far away from entities on ;direction, but contain some of the concepts of cognition and computation model respectively on x-direction and concepts of knowledge (data), reasoning and interface on the y-direction.

- In general, any quantity in any dimension is correlated with some entities on the other dimension.

- The implementation of the logical formalism was accelerated by the rapid growth in electronic technology, in general and multiprocessing parallelism in particular.

1.1.3 Types of AI

Based on the functionality of AI-based systems, AI can be categorized into the following types:

1.	Reactive Machines AI
2.	Limited Memory AI
3.	Theory of Mind AI
4.	Self-aware AI

1. Reactive Machine AI

– This type of AI includes machines that operate solely based on the present data, taking into account only the current situation.

– Reactive AI machines cannot form inferences from the info to judge their future actions.

– They can perform a narrower range of pre-defined tasks.

2. Limited Memory AI

– Name itself suggested that Limited Memory AI, can make informed and improved decisions by studying the past information from its memory.

– Such an AI features a short-lived or a short lived memory which will be wont to store past experiences and hence evaluate future actions.

3. Theory of Mind AI

– The Theory of Mind AI may be a more advanced sort of AI.

– This category of machines is alleged to play a serious role in psychology.

– This type of AI will focus mainly on emotional intelligence in order that human believes and thoughts are often better comprehended.

4. Self-Aware AI

– This type of AI is a little farfetched given the present circumstances.

– However, within the future, achieving a stage of super intelligence could be possible.

1.1.4 Applications of AI

– Following are the areas of AI applications. In engineering, there are various disciplines such as civil, computer, chemical, communication, electrical, electronics, industrial, mechanical, metallurgy, mining and production engineering in which AI finds its wide and well accepted applications.

– We describe some of the areas or domains in discipline where AI finds its scope in application for algorithm, methods, tools and techniques.

1. Civil Engineering

– Computer-aided design (CAD) reflects primarily the design data in a generic manner where the data dominates the design knowledge. But in the knowledge-based systems or expert systems, program consist of the views and solution strategy of the expert in soil mechanics, structure, architect engineering and contractors.

– It is difficult to find all the experts at different times for their opinion at users who are engaged in the construction of an entity of social/public and individual use.

– The expert systems bring together, for any time to use, expertise in different sub disciplines of civil engineering.

– Water resources management is another subarea of civil engineering that focuses on the use of water through proper management and control policy in colony, municipality, and industry. Above all, the resource is through river, canal and tanks, and reservoir.

– The utilization, storage (reservoir) and distribution of water needs a knowledge-based expert system to meet the requirement of different kinds of uses from rural (for irrigation) to urban (for drinking) having a large and complex network. Even the environment science to control pollution of different kinds needs a comprehensive approach by experts of different fields. Thus, it provokes the development of knowledge-based system.

2. Computer Engineering

– Computer science and engineering is concerned with the design and development of computing systems capable of performing the tasks for which human efforts are fruitless in specific time and unacceptable with accuracy.

- Broadly AI is integrated with the design of hardware-based system, their fault tolerant increased capacity, scheduling and load balancing of parallel computer multiprocessors.

- One of the emerging and broad areas of AI in computing is its integration into software engineering.

- The knowledge-base systems are being widely used in reusability, module verification, requirement analysis, functional design and program validation.

- The expel systems have been developed for determining the computer configuration according to the user's requirement (XCON), scheduling and person loading of software development projects (COCOMO1) guiding managers in shaping the performance of subroutines.

- Other expects systems are MASK: assists help-line personal diagnose use problems for complex software program. Component-based design and design patterns are recent trends for AI to SE; PPFAS debugs operating system software: IPT: Intelligent Peripheral Trouble-shooter.

3. Industrial Automation and Manufacturing

- Industrial Automation (IA) is concerned with introduction, incorporation and intervention of automation starting from raw material handling, planning and production of items and their assembly leading to higher capable equipment and their inventory.

- Automation means less human interference, more computing with knowledge enriched environment. Flexible manufacturing system (FMS) has emerged to tie up with AI for industrial automation in most of the leading and pioneering industries in the world.

- Important expert systems for the purpose are EXPERT PROB allows factory workers to perform quality control tasks: DISPATCHER Selects transports and delivers parts for assembly while maintaining inventory records: FAISI: Helps to create optimum schedules: WELD. SCHEDULER/Selector Helps in the selection of proper welding procedures and welding electrodes.

4. Equipment Maintenance

- Detection and diagnosis of faults, repair and proper maintenance schedule, replacement policy are the basic tasks in the maintenance of equipment.

- This requires knowledge gathering from different resources as well as proper methodology for fault computing in any equipment.

- Many expert systems have been developed for troubleshooting different kinds of equipment.

- In the mechanical equipment the expert systems are: PUMPRO diagnoses problems in centrifugal pumps: TUROMAT diagnoses vibration problem in large turbo machinery.

- RED (Rotating equipment diagnostic) diagnoses unusual vibration in routing equipment: MENTOR (preventive maintenance) needs a large central air conditioner. In the telephone industry, the diagnostic expert systems are: ACE (automated cable expertise) analyzes phone company repair data and identifies area for preventive maintenance and further repair. COMPASS assists in telephone system maintenance by analyzing operating data and recommending maintenance actions: IDEA assists telephone technicians in diagnosing problems with a LAN; BDS troubleshoots a large signal switching network, base band distribution system: GAMSTTA diagnoses fault in telephone trunks. For electrical system the expert system is TOGA. It analyzes insulation oil to diagnose faults in large utility transformers.

5. Management and Finance

- Locating (dotting), generating and distributing resources; material, man, and money, is management.

- Various expert systems have been developed to address many facts and interdisciplinary issues of management. Here we mention some of expert systems for the purpose such as the MANAGER ADVISOR: It assists corporate managers with business planning; LENDING ADVISOR assists credit managers in analyzing commercial loan applications and structuring appropriate loan packages.

- PLAN POWER helps the financial institutions in analyzing the personal needs of the clients to offer investment or other financial advice. It is implemented in LISP, basically an object-oriented model.

- CANAM TREATY advises on legal aspects of international trade transactions. EXPERTAX assists in corporate tax planning using common LISP.

- CFA: (Corporate Financial Advisor) aids in corporate financial planning using LISP. FEADV SYS: Foreign exchange advising system assists the foreign currency investors on trading decision using ART (an expert systems shell). INGOT Helps in financial forecasting using FORTRAN SALESTAX ADVISOR extends advice on the sales tax status of financial transactions for advertising agencies, commercial artists and designers using fix online class expert systems shell.

6. Office Automation

- The basic aim of the office automation is not only to provide computer as an office aid but also a media for knowledge dissemination to lateral and lower level of colleagues and employees as well as a knowledge acquisition system from higher and lateral levels to the required level.

- For the very purpose that any particular level of hierarchy, transfer of knowledge makes the personnel at any node, in particular to take decision and inform his boss or subordinate at any node in the horizon or any level on the hierarchy.

- Nowadays networking in general and information technology in particular, www makes possible the knowledge transfer and interface in an office. However, data and knowledge trade-off requires a paradigm for their integration and conversion for the purpose of office automation.

- The development of expert systems in this direction is Letter of Credit Advisor: It is a small rule-based system developed by Helix (UK) to assist clerical personnel in preparing and paying letters of credit. CV FILTER helps the user to decide whether an applicant should be interviewed; developed on Expert Edge (Helix ES).

- Data classifier helps the user to classify the value of their data, developed on Ex sys (Ex System Corporation).

7. Robotics

- Robotics is one of the prime areas of AI applications shown in the 3D view of AI.

- AI methodology is applicable to robotics in two ways. One is design and control of robot and the other is application of robots to various fields such as manufacturing, mining, medicine (surgery).

- The design of various types of robots or manipulator is primarily of mechanical engineering concern, but its control needs an interdisciplinary approach such as electrical engineering concepts for design of special purpose electrical machines: super motor or d.c. motor or micromotors, sensors for feedback; power electronics for implementing controllers.

- Other aspects such as robotics vision require electronics and communication engineering for building mobile robots with vision modems for remote control, high speed image processor and adapter.

- Design and development of multi-robot working in cooperation and coordination with the perception and pervasiveness like human (humanoid robot) is a very challenging problem for AI or knowledge-based system approach.

- Humanoid robots imitating many activities of human motor actions, as well as emotions, pose many challenging facts to AI community.

- Robot path planning and movement in collision free environment deploy some heuristic search technique such as A* and Iterative Deepening Algorithm (IDA*).

- The application of robotic system, in places where human movement is restricted as in nuclear power plant or mines, works intelligently in such places and atmosphere where hazards prevail for human with high probability, robots need incorporation of intelligence for learning, self-organization and adaptation.

- Reasoning with uncertainties and mechanization (mechanical or automatic reasoning) enhances the intelligence in robot. Nowadays, very interesting but complex phenomenon in robotics application is in game playing.

- For the last few years in Seoul Robotic Football (Robocup) game has been played continuously which deploys a good quality and high calibre of knowledge-based system methodology.

- Robotics in surgery is another surprising event in medical application that interacts with the expertise from medical and AI community, respectively.

8. Medical Computing and Informatics

- The first and firm application of AI was the design and development of the expert system named MYCIN at Stanford University by Shortliffe and Buchernan in the mid-1970s. Many expert systems in different fields of medicine were developed. Among them are INTERIES:

- a consultant for general medicine, PIP: Present Illness Program, VM: The Ventilator Manager, PUFF: Pulmonary function, CASNET; Causal Associative Network to represent the pathogenesis of a disease, in terms of patient's findings.

- Many other expert systems have been developed for detection and interpretation of diseases depicted in the bioelectrical signals such as ECG, EMG, and EEG with the advent of information technology, the telemedicine has marked a very important role in bringing IT, medicine and AI at one platform.

- The impact of AI on hospital system(H/S) can be seen in developing object-oriented model of different aspects of H/S such as patient monitoring system, drug delivery system, hospital administration, ward management and clinical testing (pathological, microbiological, radiographic images (CT and ultra sound, MRI), and signals (EEG, ECG, and EMG). The most effective contribution of IT and AI together is the telemedicine and robotics in surgery.

9. E-services

E-services are concerned with the performing business, e-commerce, and governess on www. E-commerce performs sales and purchase with customer relationship management (CRM).

10 Transportation

- Transportation system is basically concerned with scheduling and planning.

- Scheduling departures and maintenance involve manipulating the relationships between certain objects, namely vehicles, destinations, and service facilities.

- Addition and subtraction of selected change in mutes are occasional but more attention is paid for maximizing the profitability of the current fleet serving current routes.

- The expert systems for the purpose are: SEATES assists analysts in adjusting the number of discount seats available on airline routes; AALPS configures air cargo shiploads; NAVEX monitors control on space shuttle flights.

11. Agriculture

- Producers and traders of agro goods are main benefactors of expert systems applications in agriculture.

- An expert system assists farmers to produce crops, troubleshoot the crops once it is on ground and when to harvest it.

- Commodities loading are a complex business, which requires the expertise in understanding the marketing pattern, production of the grain, and distribution profile of the same.

- Some of the important expert systems in this area are WHEAT COUNSELOR. It is used for two purposes: buying guide for farmers shopping for agrochemical, and as sales aid for chemical manufacturing sales people; AQUAREF: Reference library for agriculture as a front end. PLANTING: It gives advice for various planting equipment. PGMA: It assists farmers to select the best way to market their grain.

12. Oil Exploration, Minerals and Metallurgy

- The extraction of minerals and their metallurgical processing involves many phases and expertise ranging from geologists, material technologists, and metallurgical engineers.

Similarly, oil exploration requires expertise from geology, petroleum and chemical engineering groups. Following are the expert systems in practice.

- DRILLING ADVISOR: A knowledge-based system developed by a French oil company that assists oil rig supervisor in resolving and, subsequently, avoiding problem situations.

- MUDMAN diagnoses problems with "mud" used in oil well drilling and recommends new compositions.

- WAVES aids in developing data processing control strategies for seismic survey data.

13. Electrical Engineering

The various areas of electrical engineering that require the knowledge-based system approach are:

1. **Power system** : Generation, distribution, load flow analysis, load management, power protection, power system control, high voltage transmission and distribution.

2. **Electrical machines** : Design of various motor alternators and generators needs a knowledge-based approach rather than computer-aided design (CAD), because consideration of different types of loads (primarily modelled as R, L, C and their combination) and drives (mechanical or electrical) pose uncertainties in the design parameter (change) and performance (degradation).

3. **Control** : Depending on the plant (object to be controlled) characteristics, the controllers are designed to have a desire performance of the plant. The plant may be a motor, robot, or a mechanical system. The basic controllers are Proportional (P), Derivative (D), Integral (I), PI and PID. Depending on the characteristics of the plant, the controllers may be linear/nonlinear, deterministic/stochastic, continuous/discrete, lumped/distributed, time invariant/variant. Most of the controllers do not require Knowledge-based system methodologies for their design but complex mathematical models, instead.

4. **Power electronics** : It consists of design and development of converter (from a.c. to d.c.) and inverter (from d.c to a.c.) and control of power using

various techniques such as chopper control cyclomete (frequency control), PWM (pulse width modulation), recently ANN and some heuristic search techniques have been deployed for the purpose.

5. **Drive control** : This field combines electrical machine, drives and control principles. Thus, different experts from the respective fields are required to show knowledge, control, and management for design, development and diagnosis of problems in railways, paper and pulp industries, textile industries, hoist and mills. It emerged from the knowledge of different disciplines for its effective use. Important components of KBS used in such problems are knowledge representation, inference and uncertainty measurement and users interface (graphics). Some of the expert systems are hoist diagnosis developed by INSIGHT INC. for diagnosis of faults on hoist equipments. DELTA (diesel electric locomotive trouble shooting aid) developed by General Electric company assists in assessing maintenance needs and prescribes appropriate action to assist diesel locomotive maintenance personnel.

▶▶ 1.2 Concept of Machine Learning & Deep Learning

Machine Learning

- Before talking about machine learning lets mention another concept that's called data processing.

- Data mining may be a technique of examining an outsized pre-existing database and extracting new information from that database, it's easy to know, right, machine learning does an equivalent, in fact, machine learning may be. a sort of data processing technique.

Here's may be a basic definition of machine learning –

- "Machine Learning may be a technique of parsing data, learn from that data then apply what they need learned to form an informed decision"

- Now a days many of massive companies use machine learning to offer there users a far better experience, a number of the examples are, Amazon using machine

learning to offer better product choice recommendations to there costumers supported their preferences.

- Netflix uses machine learning to offer better suggestions to their users of the Tv series or movie or shows that they would like to watch.

Deep Learning

- Deep learning is really a subset of machine learning. It technically is machine learning and functions within the same way but it's different capabilities.

- The primary difference between deep and machine learning is, machine learning models become good progressively but the model still needs some guidance to get improve.

- If a machine learning model derives an approximate prediction then the programmer must give idea of that problem explicitly but within the case of deep learning, the model does it by himself.

- Automatic car driving system may be a exemplar of deep learning.

- Let's take an example to know both machine learning and deep learning :

- Suppose we've a flashlight and that we teach a machine learning model that whenever someone says "dark" the flashlight should get on, now the machine learning model will analyse different phrases said by people and it'll look for the word "dark" and because the word comes the flashlight are going to be on but what if someone said "I am not able to see anything the sunshine is extremely dim", here the user wants the flashlight to get on but the sentence doesn't the consist the word "dark" therefore the flashlight will not be on. so it concludes that deep learning is different from machine learning.

- If it were a deep learning model it might on the flashlight, a deep learning model is in a position to find out from its own method of computing.

▶▶ 1.3   Multiple Choice Questions for Online Exam

Q. 1 The performance of an agent can be improved by _____

a) Learning   b) Observing

c) Perceiving   d) None of the mentioned

Ans. : (a)

Q. 2 External actions of the agent is selected by _____

a) Perceive   b) Performance

c) Learning   d) Actuator

Ans. : (b)

Q. 3 The action of the Simple reflex agent completely depends upon _____

a) Perception history

b) Current perception

c) Learning theory

d) Utility functions

Ans. : (b)

Q. 4 Which of the following could be the approaches to Artificial Intelligence?

a) Strong Artificial Intelligence

b) Weak Artificial Intelligence

c) Applied Artificial Intelligence

d) All of the mentioned

Ans. : (d)

Q. 5 An Artificial Neural Network Is based on?

a) Strong Artificial Intelligence approach

b) Weak Artificial Intelligence approach

c) Cognitive Artificial Intelligence approach

d) Applied Artificial Intelligence approach

Ans. : (c)

Q. 6 The Face Recognition system is based on ?

a) Strong Artificial Intelligence approach

b) Weak Artificial Intelligence approach

c) Cognitive Artificial Intelligence approach

d) Applied Artificial Intelligence approach

Ans. : (d)

Q. 7 A completely automated chess engine (Learn from previous games) is based on?

a) Strong Artificial Intelligence approach

b) Weak Artificial Intelligence approach

c) Cognitive Artificial Intelligence approach

d) Applied Artificial Intelligence approach

Ans. : (a)

Q. 8 A basic line following robot is based on _____

a) Strong Artificial Intelligence approach

b) Weak Artificial Intelligence approach

c) Cognitive Artificial Intelligence approach

d) Applied Artificial Intelligence approach

Ans. : (b)

Q. 9 Which of the following task/tasks Artificial Intelligence could not do yet?

a) Understand natural language robustly

b) Web mining

c) Construction of plans in real time dynamic systems

d) All of the mentioned

Ans. : (d)

Q. 10 What among the following is/are the example of the intelligent agent/agents?

a) Human   b) Robot

c) Autonomous Spacecraft

d) All of the mentioned

Ans. : (d)

Q. 11 What is Machine learning?

a) The autonomous acquisition of knowledge through the use of computer programs

b) The autonomous acquisition of knowledge through the use of manual programs

c) The selective acquisition of knowledge through the use of computer programs

d) The selective acquisition of knowledge through the use of manual programs

Ans. : (a)

Q. 12 Which of the factors affect the performance of learner system does not include?

a) Representation scheme used

b) Training scenario

c) Type of feedback

d) Good data structures

Ans. : (d)

Q. 13 Different learning methods does not include?

a) Memorization

b) Analogy

c) Deduction

d) Introduction

Ans. : (d)

Q. 14 14. In language understanding, the levels of knowledge that does not include?

a) Phonological

b) Syntactic

c) Empirical

d) Logical

Ans. : (c)

Q. 15 A model of language consists of the categories which does not include ?

a) Language units

b) Role structure of units

c) System constraints

d) Structural units

Ans. : (d)

Q. 16 The performance of an agent can be improved by _____

a) Learning

b) Observing

c) Perceiving

d) None of the mentioned

Ans. : (a)

Q. 17 External actions of the agent is selected by _____

a) Perceive

b) Performance

c) Learning

d) Actuator

Ans. : (b)

Q. 18 Which of the following could be the approaches to Artificial Intelligence ?

a) Strong Artificial Intelligence

b) Weak Artificial Intelligence

c) Applied Artificial Intelligence

d) All of the mentioned

Ans. : (d)

Q. 19 What is the term used for describing the judgmental or commonsense part of problem solving ?

a) Heuristic

b) Critical

c) Value based

d) Analytical

e) None of the above

Ans. : (a)

Q. 20 What stage of the manufacturing process has been described as "the mapping of function onto form" ?

a) Design

b) Distribution

c) project management

d) field service

e) None of the above

Ans. : (a)

Q. 21 Which kind of planning consists of successive representations of different levels of a plan ?

a) hierarchical planning

b) non-hierarchical planning

c) All of the above0

e) project planning

e) None of the above

Ans. : (a)

Q. 22 What was originally called the "imitation game" by its creator ?

a) The Turing Test

b) LISP

c) The Logic Theorist

d) Cybernetics

e) None of the above

Ans. : (a)

Q. 23 To invoke the LISP system, you must enter

a) AI

b) LISP

c) CL (Common Lisp)

d) both b and c

e) None of the above

Ans. : (e)

Q. 24 Prior to the invention of time sharing, the prevalent method of computer access was:

a) Batch processing

b) Telecommunication

c) Remote access

d) All of the above

e) None of the above

Ans. : (a)

Q. 25 The original LISP machines produced by both LMI and Symbolics were based on research performed at:

a) CMU

b) MIT

c) Stanford University

d) RAMD

e) None of the above

Ans. : (b)

Chapter Ends...

❑❑❑

CHAPTER 2

Embedded Systems

►► 2.1 Embedded System

➤ 2.1.1 Introduction

- An embedded system is an electronic/electro-mechanical system designed to perform a specific function and is a combination of both hardware and firmware (software).

- Every embedded system is exclusive, and therefore the hardware similarly as the firmware is very specialised to the appliance domain.

- Embedded systems are becoming an invitable part of any product or equipment in all fields including household appliances, telecommunications, medical equipment, industrial control, consumer products etc.

➤ 2.1.2 Embedded System Application

1. Consumer electronics: Camcorders, cameras, etc.

2. Household appliances: Television, DVD players, washer, fridge, microwave, etc.

3. Home automation and security systems: Air conditioners, sprinklers, intruder detection alarms, loop television cameras, fire alarms, etc.

4. Machine industry: Anti-lock breaking systems, engine control, ignition systems, automatic navigation systems, etc.

5. Telecom: Cellular telephones, telephone switches, handset multimedia applications, etc.

6. Computer peripherals: Printers, scanners, fax machines, etc.

7. Computer networking: Network routers, switches, hubs, firewalls, etc.

8. Healthcare: Different sorts of scanners, EEG, ECG machines etc.

9. Computation & Instrumentation: Digital multi meters, digital CROs, logic analyzers PLC systems, etc.

10. Banking & Retail: cash machine machines and currency counters, point of sales

11. Card Readers: Barcode, open-end credit readers, hand-held devices etc.

➤ 2.1.3 Purpose of Embedded Systems

As mentioned within the previous section, embedded systems are utilized in various domains like consumer electronics, home automation, telecommunications, automotive industry, healthcare, control & instrumentation, retail and banking applications etc. Within the domain itself, consistent with the appliance usage context, they'll have different functionalities. Each embedded system is meant to serve the aim of anybody or a mixture of the subsequent tasks:

1. Data collection/Storage/Representation
2. Digital communication
3. Data (signal) processing
4. Monitoring
5. Control
6. Application specific interface

1. Data Collection/Storage/Representation:

- Embedded systems designed for the purpose of data collection perform acquisition of data from the external world.

- Data collection is typically done for storage, analysis, manipulation and transmission.

- The term "data" refers all types of data, viz. text, voice, image, video, electrical signals and the other measurable quantities.

- Data are often either analog (continuous) or digital (discrete).

- Embedded systems with analog data capturing techniques collect data directly within the type of analog signals whereas embedded systems with digital data collection mechanism converts the analog signal to corresponding digital signal using analog to digital (A/D) converters and then collects the binary equivalent of the analog data.

- If the info is digital, it are often directly captured with none additional interface by digital embedded systems.

- The collected data could also be stored directly within the system or could also be transmitted to another system or it's going to be processed by the system or it's going to be deleted instantly after giving a meaningful representation.

- These actions are purely hooked in to the aim that the embedded system is meant.

- Embedded systems designed for pure computation applications without storage & used in manage and machine domain, gather data and provides a meaningful representation of the gathered data by means of graphical presentation or quantitative value and removes the gathered data when new data arrives at the info collection terminal.

- Analog and digital CROs without storage memory are typical samples of this.

- Any measuring equipment used in the medical domain for monitoring without storage functionality also comes below this category.

- Some embedded systems stores the gathered data for processing and reasoning. Such systems incorporate a built-in cache memory for storing the gathered data. Some of them give the user a meaningful presentation of the collected info by visual (graphical/quantitative) or audible means using display elements. Examples are: measuring instruments with storage memory and monitoring instruments with storage memory utilized in medical applications.

- Certain embedded systems store the info and cannot provide a representation of an equivalent to the user, whereas the info is employed for internal processing.

- A camera may be a typical example of an embedded system with data collection/storage/ representation of knowledge.

- Images are captured and the captured image may be stored within the memory of the camera. The captured image also can be presented to the user through a graphic LCD unit.

2. Data Communication

- Embedded data communication systems are deployed in applications starting from complex satellite communication systems to simple home networking systems.

- As mentioned earlier during this chapter, the info collected by an embedded terminal may require transferring of an equivalent to another system located remotely.

- The transmission is carried either by a wire-line medium or by a wire-less medium of transmission. Wire-line medium was the foremost common choice altogether olden days embedded systems.

- As technology is changing, wireless medium is becoming the de-facto standard for digital communication in embedded systems.

- A wireless medium offers cheaper connectivity solutions and make the communication link free from the effort of wire bundles. Data can be transmitted either by analog means or by digital means.

- The data gathering embedded terminal itself can incorporate digital communication units like wireless modules (Bluetooth, ZigBee, Wi-Fi, EDGE, GPRS, etc.) or wire-line modules (RS-232C, USB, TCP/IP, PS2, etc.).

- Certain embedded systems act as a dedicated transmission unit between the sending and receiving terminals, offering sophisticated functionalities like data packetizing, encrypting and decrypting.

- Network, hubs, routers, switches, etc. are typical samples of dedicated data transmission embedded systems.

- They act as mediators in data communication and provide various features like data security, monitoring etc.

3. Data (Signal) Processing

- As mentioned earlier, the data (voice, image, video, eke-Meal signals and other measurable quantities) collected by embedded systems may be used for various kinds of data processing.

- Embedded systems with signal processing performances are joined in applications challenging signal processing like synthesis, audio video codec, transmission applications, etc.

- A digital hearing element may be a typical example of an embedded system employing processing. Digital hearing elements improve the hearing capacity of hearing impaired persons.

4. Monitoring

- Embedded systems falling below this category are specifically designed for monitoring purpose.

- Almost all embedded products coming below the medical domain are with monitoring performances only. They are used for finding the state of some variables using input sensors. They cannot forces control over variables.

- A very exemplar is that the electro cardiogram (ECG) machine for monitoring the heartbeat of a patient.

- The machine is build to do the monitoring of the heartbeat. It cannot forces control over the heartbeat.

- The sensors used in ECG are the different electrodes which are connected to the patient's body.

- Some other samples of embedded systems with monitoring function are computation instruments like digital CRO, digital multimeters, logic analyzers, etc. used in Control & Instrumentation applications. They are used for knowing (monitoring) the status of few variables like current, voltage etc. They cannot control the variables in turn.

5. Controls

- Embedded systems with control functionalities impose control over some variables consistent with the changes in input variables.

- A system with manage working contains both sensors and actuators.

- Sensors are joined to the input port for collecting the changes in environmental variable or computing variable.

- The actuators connected to the output port are managed consistent with the changes in input variable to place an impression on the managing variable to bring the managed variable to the specified range.

- Air conditioner system utilized in our home to regulate the space temperature to a specified limit may be a typical example for embedded system for control purpose. An air-conditioned contains an area temperature-sensing element (sensor) which can be a

thermistor and a handheld unit for fixing (feeding) specified temperature.

- The handheld unit could also be connected to central embedded unit residing inside the conditioning through a wireless link or through a wire link. The air compressor unit FS02Inflift acts as actuator.

- The compressor is controlled according to current room temperature and the desire temperature set by the user.

- Here the input variable is that the current temperature and therefore the controlled variable is additionally the space temperature.

- The managing variable is cool air flow by the compressor unit.

- If the controlled variable and input variable are not at the same value, the controlling variable tries to equalize them through taking actions on the cool air flow.

6. Application Specific User Interface

- These are embedded systems with application-specific based on user coherence like buttons, switches, keypad, lights, bells, display units etc.

- Mobile phone is an example for this. In mobile the interface is provided through the keypad, graphic LCD module, system speaker, vibration alert, etc.

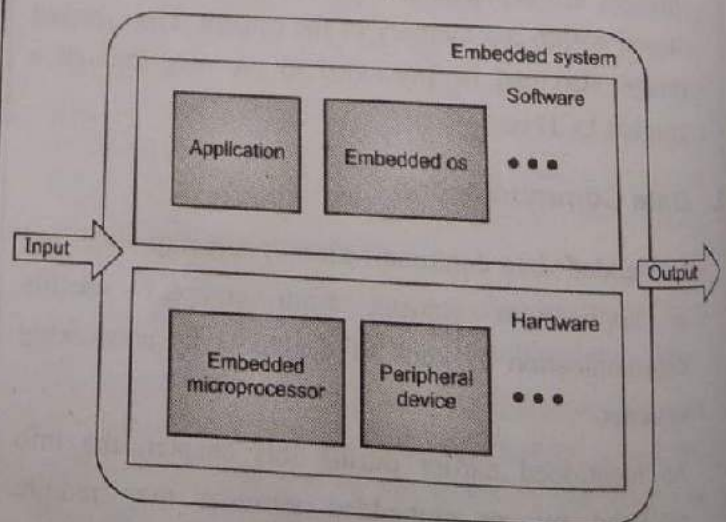### 2.1.4 Typical Architecture of an Embedded System

Fig. 2.1.1 : Typical architecture of an Embedded System

Emer. Trends in Comp. & Infor. Tech. (MSBTE Sem. 6)   2-5

Embedded Systems

- Fig. 2.1.1 shows a configuration diagram of a typical embedded system consisting of two main parts: embedded hardware and embedded software.

- The embedded hardware mainly contains the processor, memory, bus, peripheral devices, I/O ports, and various controllers.

- The embedded software usually includes the embedded OS and various applications.

- Input and output are characteristics of any open system, and therefore the embedded system is not any exception.

- In the embedded system, the hardware and software often collaborate to affect various input signals from the surface and output the processing results through some form.

- The input could also be an ergonomic device (such as a keyboard, mouse, or touch screen) or the output of a sensor circuit in another embedded system.

- The output could also be within the sort of sound, light, electricity, or another analog signal, or a record or file for a database.

Typical Hardware Architecture

The basic computer system components microprocessor, memory, and input and output modules are interconnected by a system bus in order for all the parts to communicate and execute a program (see Fig. 2.1.2).
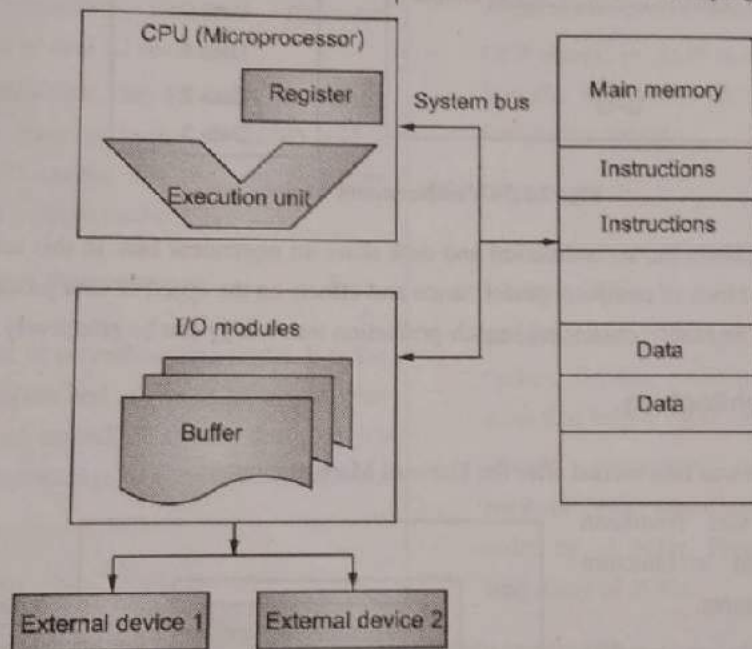

Fig. 2.1.2 : Typical Hardware Architecture

- In embedded systems, the microprocessor's role and performance are usually an equivalent as those of the CPU during a general-purpose computer: control machine operation, execute instructions, and process data.

- In many cases, the microprocessor in an embedded system is additionally called the CPU. Memory is used to store instructions and data. I/O modules are liable for the info exchange between the processor, memory, and external devices.

- External devices include auxiliary storage devices (such as flash and hard disk), communications equipment, and terminal equipment.

- The system bus gives data and controls signal communication and transmission for the processor, memory, and I/O modules.

- There are basically two sorts of architecture that apply to embedded systems: von Neumann architecture and Harvard architecture.

2.1.4.1 Von Neumann Architecture

- Von Neumann architecture (also referred to as Princeton architecture) was first proposed by John von Neumann.
- The most important feature of this architecture is that the software and data use an equivalent memory; that's, "the program is data, and therefore the data is that the program" (as shown in Fig. 2.1.3)
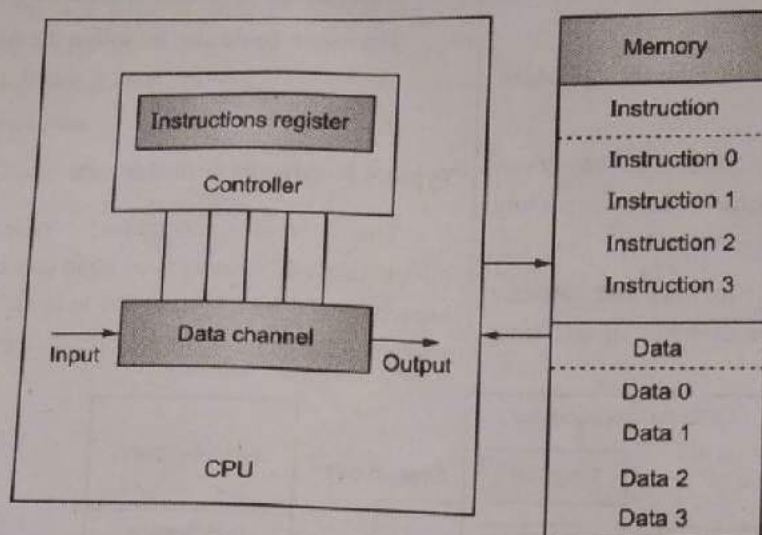

Fig. 2.1.3 : Von Neumann Architecture

- In the von Neumann architecture, an instruction and data share an equivalent bus. In this architecture, the transfer of knowledge becomes the block of computer performance and affects on the speed of data processing; so, it's often called the von Neumann block. In reality, cache and branch-prediction technology can be effectively resolving this problem.

2.1.4.2 Harvard Architecture

- The Harvard architecture was first named after the Harvard Mark computer.

- Compared with the von Neumann architecture, a Harvard architecture processor has 2 main features.

- First, instructions and data are stored in 2 different memory modules; instructions and data don't coexist in the same module. Second, two inter dependent buses are used as specialized communication paths in between the CPU and memory; there's no connection in between the 2 buses.
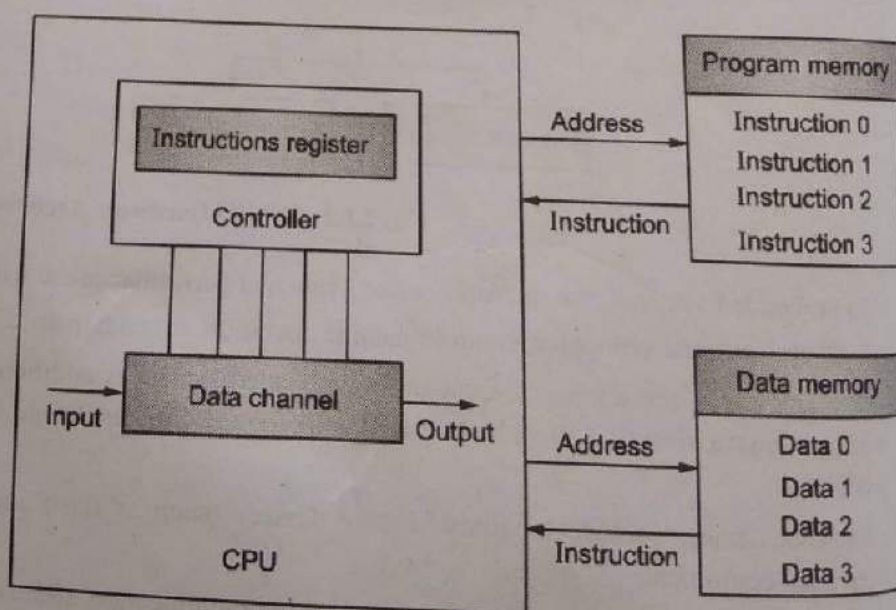
- The Harvard architecture is shown in Fig. 2.1.4.

Fig. 2.1.4 : Harvard Architecture

- Because the Harvard architecture has different program memory and data memory, it can give greater data-memory bandwidth, making it the perfect choice for digital signal processing.

- Most systems mainly designed for digital signal processing to adopt the Harvard architecture.

- The von Neumann architecture functions simple hardware design and flexible program and data storage and is typically the one chosen for common-purpose and most embedded systems.

- To efficiently perform memory reads/writes, the processor isn't directly connected to the most memory, but to the cache.

- Commonly, the sole difference between the Harvard architecture and therefore the von Neumann architecture is single or dual L1 cache.

- In the Harvard architecture, the L1 cache is usually divided into an instruction cache (I cache) and a knowledge cache (D cache), but the von Neumann architecture features a single cache.

2.1.5 Embedded Processors

Processor is the heart of an embedded system. It is the essential unit that takes inputs and produces an output after processing the info. For an embedded system designer, it's necessary to possess the knowledge of both microprocessors and microcontrollers.

Processors in a System

A processor has two essential units –

- Program Flow Control Unit (CU)

- Execution Unit (EU)

- The CU contains a fetch unit for collecting instructions from the memory.

- The EU has circuits that implement the statements concerning data transfer operation and convert from one form to another.

- The EU includes the Arithmetic and Logical Unit (ALU) and also the circuits that execute instructions for a program control task like interrupt, or jump to a different set of instructions.

- A processor performs the cycles of fetch and performs the instructions in the same sequence as they're fetched from memory.

Types of Processors

Processors can be of the following categories –

- General Purpose Processor (GPP)
  (a) Microprocessor
  (b) Microcontroller
  (c) Embedded Processor
  (d) Digital Signal Processor
  (e) Media Processor

- Application Specific System Processor (ASSP)

- Application Specific Instruction Processors (ASIPs)

- GPP core(s) or ASIP core(s) on either an Application Specific Integrated Circuit or a Very Large Scale Integration circuit.

Microprocessor

- A microprocessor may be a one single VLSI chip having a CPU.

- In additionally, it's going to have other units like caches, floating point processing AU and pipelining units that help in rapid execution of statements.

- Earlier generation microprocessors' gather-and-perform cycle was directed by a clock frequency of order of ~1 MHz. Processors now work at a clock frequency of 2GHz

Microcontroller

- A microcontroller may be a single-chip VLSI unit (also called microcomputer).

- Microcontrollers are particularly employing in embedded systems for real-time control applications with on-chip program memory and devices.

PIC Microcontroller

- Peripheral Interface Controller (PIC) is microcontroller designed by a Microchip; PIC microcontroller is rapid and straightforward.

- The ease of programming and straightforward to interfacing with another peripherals PIC becomes successful microcontroller.

- We know that microcontroller is an integrated chip which is consists of RAM, ROM, CPU, and TIMER and COUNTERS.

- The PIC may be a microcontroller which also consists of RAM, ROM, CPU, timer, counter, ADC (analog to digital converters), DAC (digital to analog converter). PIC Microcontroller supports the protocols for example CAN, SPI, UART for coherence with additional peripherals.

- PIC always wont to change Harvard architecture and also supports RISC by the above maintain requirement RISC and Harvard we will simply that PIC is quicker than the 8051 based controllers which is ready from Von-Newman architecture.

AVR Microcontroller

- AVR microcontroller was developed by Atmel Corporation within the year of 1996.

- The constructional design of AVR was developed by the Alf-Egil Bogen and Vegard Wollan. AVR derives its name from its developers and stands for Alf-Egil Bogen Vegard Wollan RISC microcontroller, also referred to as Advanced Virtual RISC.

AVR Microcontrollers are Available in three Categories:

- **TinyAVR :** Less memory, small size, appropriate only for simpler applications

- **MegaAVR :** These are the mainly popular ones having an quantity of memory (up to 256 KB), higher no of inbuilt peripherals and appropriate for moderate to complex applications.

- **XmegaAVR :** utilized in commercial for complex applications, which require large program memory and high speed.

ARM Processor

- An ARM processor is additionally one among a family of CPUs supported the RISC architecture developed by Advanced RISC Machines.

- RISC processors are designed to perform a small of sorts of computer statements in order so that will operate at a better speed, performing extra statements per second. By stripping out unre statements and optimizing pathways, RISC proces give excellent performance at a neighbourhood of facility demand of CISC actions.

- ARM processors are utilized in customer electro devices like smart phones, tablets, multimedia play and other mobile devices, like wearable. Because their reduced to instruction set, they have few transistors, which enable a smaller die size of integrated circuitry (IC).

- The ARM processors, smaller size reduced difficult and lower power spending makes them suitable f increasingly miniaturized devices.

▶▶ 2.2　Multiple Choice Questions for Online Exam

Q. 1　Name the processor which helps in floating point calculations.

a) microprocessor

b) microcontroller

c) coprocessor

d) controller

Ans. : (c)

Q. 2　Which is the coprocessor of 8086?

a) 8087　　b) 8088

c) 8086　　d) 8080

Ans. : (a)

Q. 3　Which of the following processors can perform exponential, logarithmic and trigonometric functions?

a) 8086　　b) 8087

c) 8080　　d) 8088

Ans. : (b)

Q. 4 How many stack register does an 8087 have?

a) 4   b) 8   c) 16   d) 32

Ans. : (b)

Q. 5 Which one of the following offers CPUs as integrated memory or peripheral interfaces?

a) Microcontroller

b) Microprocessor

c) Embedded system

d) Memory system

Ans. : (a)

Q. 6 Which of the following offers external chips for memory and peripheral interface circuits?

a) Microcontroller

b) Microprocessor

c) Peripheral system

d) Embedded system

Ans. : (b)

Q. 7 Which of the following offers external chips for memory and peripheral interface circuits?

a) Microcontroller

b) Microprocessor

c) Peripheral system

d) Embedded system

Ans. : (d)

Q. 8 What is CISC?

a) Computing instruction set complex

b) Complex instruction set computing

c) Complimentary instruction set computing

d) Complex instruction set complementary

Ans. : (b)

Q. 9 Which of the following possesses a CISC architecture?

a) MC68020

b) ARC

c) Atmel AVR

d) Blackfin

Ans. : (a)

Q. 10 Which of the following is a RISC architecture?

a) 80286

b) MIPS

c) Zilog Z80

d) 80386

Ans. : (b)

Q. 11 Which one of the following is board based system?

a) Data bus

b) Address bus

c) VMEbus

d) DMA bus

Ans. : (c)

Q. 12 What does CCR stand for?

a) Condition code register

b) Computing code register

c) Complex code register

d) Code control register

Ans. : (a)

Q. 13 Which one of the following is an asynchronous communication channel?

a) SPI   b) MUDs

c) MOO   d) VOI

Ans. : (a)

Q. 14 What shows the brightness of the pixel in a digital signal processor?

a) luminance

b) transparent

c) chrominance

d) opaque

Ans. : (a)

Q. 15 Which of the following processor are designed to perform calculations in graphics rendering?

a) GPU

b) digital signal processor

c) microprocessor

d) microcontroller

Ans. : (a)

Q. 16 Which of the processor is a good match for applications such as video games?

a) GPU

b) VLIW

c) Coprocessor

d) Microcontroller

Ans. : (a)

Q. 17 Which of the following statement is true for concurrency?

a) different parts of the program executes physically

b) different parts of the program executes sequentially

c) different parts of the program executes conceptually

d) different parts of the program executes sequentially and physically

Ans. : (c)

Q. 18 Which is an imperative language?

a) C program

b) SQL

c) XQuery

d) Concurrent model of HDL

Ans. : (a)

Q. 19 What is ILP?

a) instruction-level parallelism

b) instruction-level panel

c) instruction-language panel

d) inter-language parallelism

Ans. : (a)

Q. 20 Which ILP supports the ALU division?

a) Subword parallelism

b) CISC

c) Superscalar

d) VLIW

Ans. : (a)

Q. 21 Which is the first company who defined RIS architecture?

a) Intel   b) IBM

c) Motorola   d) MIPS

Ans. : (b)

Q. 22 How is memory accessed in RISC architecture?

a) load and store instruction

b) opcode instruction

c) memory instruction

d) bus instruction

Ans. : (a)

Q. 23 Which of the following statements are true for von Neumann architecture?

a) shared bus between the program memory and data memory

b) separate bus between the program memory and data memory

c) external bus for program memory and data memory

d) external bus for data memory only

Ans. : (a)

Q. 24 What is CAM stands for?

a) content-addressable memory

b) complex addressable memory

c) computing addressable memory

d) concurrently addressable memory

Ans. : (a)

Q. 25 Which of the following are header files?

a) #include　　b) file

c) struct()　　d) proc()

Ans. : (a)

Q. 26 Which of the following gives the final control to the programmer?

a) linker　　b) compiler

c) locater　　d) simulator

Ans. : (a)

Q. 27 Which of the following can destroy the accuracy in the algorithms?

a) delays　　b) error signal

c) interrupt　　d) mmu

Ans. : (a)

Q. 28 Which of the following is replaced with the absolute addressing mode?

a) relative addressing mode

b) protective addressing mode

c) virtual addressing mode

d) temporary addressing mode

Ans. : (a)

Q. 29 What is the main purpose of the memory management unit?

a) address translation

b) large storage

c) reduce the size

d) provides address space

Ans. : (a)

Q. 30 Which of the following provides stability to the multitasking system?

a) memory　　b) DRAM

c) SRAM　　d) Memory partitioning

Ans. : (a)

Chapter Ends...

Ⅱ◻◻◻

CHAPTER 3

IoT : Definition and Characteristics of IoT

Syllabus

- Physical design of IoT,
  - Things of IoT
  - IoT Protocols
- Logical design of IoT,
  - IoT functional blocks,
  - IoT Communication models,
  - IoT Communication APIs,
- IoT Enabling Technologies
- IoT levels and deployment templates
- IoT Issues and Challenges, Applications
- IoT Devices and its features : Arduino, Uno, Raspberry Pi, Node Microcontroller Unit

---

3.1 IoT Definition and Characteristics

3.1.1 Introduction

- Internet of Things (IoT) comprises things that have unique identities and are connected to the Internet.

- While many existing devices, such as networked computers or 4G-enabled mobile phones, already have some form of unique identities and are also connected to the Internet, the focus on IoT is in the configuration, control and networking via the Internet of devices or "things" that are traditionally not associated with the Internet.

- These include devices such as thermostats, utility meters, a Bluetooth-connected headset, irrigation pumps and sensors, or control circuits for an electric car's engine.

- Internet of Things is a new revolution in the capabilities of the endpoints that are connected to the Internet, and is being driven by the advancements in capabilities (in combination with lower costs) in sensor networks, mobile devices, and wireless communications, networking and cloud technologies.

- Experts forecast that by the year 2020 there'll be a complete of fifty billion devices/things connected to the web. Therefore, the major industry players are excited by the prospects of new markets for their products.

- The products include hardware and software components for IoT endpoints, hubs, or control centres of the IoT universe.

- The scope of IoT is not limited to just connecting things (devices, appliances. machines) to the Internet.

- IoT allows these things to communicate and exchange data (control & information that could include data associated with users) while executing meaningful applications towards a common user or machine goal.

- Data itself does not have a meaning until it is contextualized processed into useful information.

- Applications on IoT networks extract and create information from lower level data by filtering, Processing, Categorizing, condensing contextualizing the data.

- This information obtained is then organized structured to infer knowledge about the system and its users, its environment, and its operations a progress towards its objectives, allowing a smart performance.

- To give meaning to the data, a context is added, which in this example can be that each tuple in data represents the temperature and humidity measured every minute. With this context added we know the meaning (or information) of the measured data tuples.

- Further information is obtained by categorizing condensing or processing this data. For example the average temperature and humidity readings for last five minutes are obtained by averaging the last five data tuples.

- The next step is to organize the information and understand the relationships between pieces of information to infer knowledge which can be put into action.

- For example an alert is raised if the average temperature in last five minutes exceeds 120E and this alert may be conditioned on the user's geographical position as well.

3.1.2 Definition and Characteristics of IoT Internet of Things (IoT) has been Defined as

☐ Definition : A dynamic world network infrastructure with self-configuring capabilities based on norm and compatible communication protocols wherever physical and virtual material that have identities, physical attributes, and virtual personalities and use intelligent interfaces, and are seamlessly integrated into the data network, usually communicate information related to users and their environments.

- Let us examine this definition of IoT further to put some of the terms into perspective.

☞ Self-Accommodate

- IoT devices and systems may have the capacity to adapt with the changing contexts and take actions based on their operating conditions.

- User's context or sensed environment. For example, consider a surveillance system comprising of a number of surveillance cameras. The surveillance cameras can adapt their modes (to normal or infra-red night modes) based on whether it is day or night.

- Cameras might switch from lower resolution to higher resolution modes once any motion is detected and alert near cameras to try to a similar. In this example the surveillance system is adapting itself based on the context and changing (e.g., dynamic) conditions.

- Self-Composition: IoT devices may have self-composition capability, allowing a large number of devices to work together to provide certain functionality (such as weather monitoring). These devices have the ability configure themselves (in association with the IoT infrastructure), setup the networking, and fetch latest software upgrades with minimal manual or user intervention.

- Interoperable Communication Protocols: IoT devices may be compatible with a number of communication protocols and may communicate with many devices and also with the infrastructure. We describe some of the commonly used communication protocols and models in later sections.

☞ Unique Identity

- Each IoT device has a unique identity and a unique identifier (such as an IP address or a URI).

- IoT systems may have intelligent interfaces which adapt based on the context; allow communicating with users and the environmental contexts.

- IoT device interfaces allow users to query the devices, monitor their status, and control them remotely in association with the control, configuration and management infrastructure.

☞ Integrated Into Information Network

- IoT devices are usually integrated into the information network that allows them to communicate and exchange data with other devices and systems.

- IoT devices can be dynamically discovered in the network, by other devices and/or the network, and have the capability to describe themselves (and their characteristics) to other devices or user applications.

- For example a weather monitoring node can describe its monitoring capabilities to another connected node so that they can communicate and exchange data. Integration into the information network helps in making IoT systems "smarter" due to the collective intelligence of the individual devices in collaboration with the infrastructure.

- Thus, the data from a large number of connected weather monitoring IoT nodes can be aggregated and analyzed to predict the weather.

☞ 3.1.3 Physical Design of IoT

☞ 3.1.3.1 Things in IoT

- The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.

- IoT devices can exchange data with other connected devices and applications (directly or indirectly), or collect data from other devices and process the data either locally or send the data to centralized servers or cloud-based application back-ends for processing the data, or perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints (i.e., memory, processing capabilities, communication latencies and speeds, and deadlines).

- An IoT device may consist of several interfaces for connections to other devices, both wired and wireless.

- These embrace (i) I/O interfaces for sensors, (ii) interfaces for Internet connectivity, (iii) memory and storage interfaces and (iv) audio/video interfaces shows in the Fig. 3.1.1.

- An IoT device can collect various types of data from the on-board or attached sensors, such as temperature, humidity, and light intensity.

- The sensed data can be communicated either to other devices or cloud-based servers/storage.

- IoT devices can be connected to actuators that allow them to interact with other physical entities (including non-IoT devices and systems) in the vicinity of the device.

...A SACHIN SHAH Venture

- For example, a relay switch connected to a IoT device can turn an appliance on/off based on the commands sent to IoT device over the Internet.
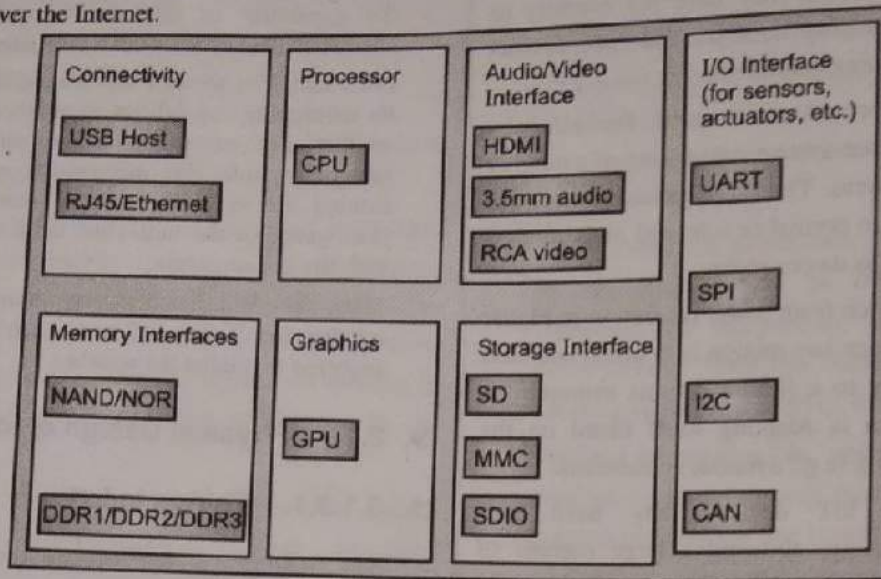

Fig. 3.1.1 : Generic Block Diagram of an IOT device

- IoT devices can also be of varied types, for instance, wearable sensors, smart watches, LED lights, automobiles and industrial machines.

- Almost all IoT devices generate information in some type or the opposite that once processed by information analytics systems ends up in helpful data to guide additional actions domestically or remotely.

- For instance, device information generated by a soil wet monitor in a garden, once processed will facilitate in decisive the optimum watering schedules.

📕 3.1.3.2   IoT Protocols

☞ Link Layer

- Link layer protocols determine how the data is physically sent over the network's physical layer or medium (e.g., cropper wire, coaxial cable, or a radio wave).

- The scope of the link layer is the local network connection to which host is attached. Hosts on the same link exchange data packets over the link layer using link layer protocols. Link layer determines how the packets arc coded and signalled by the hardware device over the medium to which the host is attached

(such as a coaxial cable). Let us now look at some link layer protocols which are relevant in the context of lot

☞ 802.3 - Ethernet

- IEEE 802.3 is a collection of wired Ethernet standards for the link layer.

- For example 802.3 is the standard for 10BASE5 Ethernet that uses coaxial cable as a shared medium. 802.3.i is the standard for 10BASE-T Ethernet over copper twisted-pair connections, 802.3.j is the standard for 10BASE-F Ethernet over fiber optic connections. 802.3ae is the standard for 10 Gbit/s Ethernet over fiber, and so on.

- These standards provide data rates from 10 Mb/s to 40 Gbh and higher.

- The shared medium in Ethernet can be a coaxial cable, twisted-pair wire or an optical fiber.

- The shared medium (i.e. broadcast medium) carries the communication for all the devices on the network, thus data sent by one device can received by all devices subject to propagation conditions and transceiver capabilities.

- The specifications of the 802.3 standards are available on the IEEE 802.3 working group website

802.11 - WW1

- IEEE 802.11 is a collection of wireless local area network (WLAN) communication standards, including extensive description of the link layer.

- For example 802.11a operates in the 5 GHz band. 802.11b and 802.11g operate in the 2.4 GHz band. 802.11n operates in the 2.4/5 GHz bands. 802.11ac operates in the 5 GHz band and 802.11ad operates in the 60 GHz band.

- These standards provide data rates from 1 Mb/s to upto 6.75 Gb/s. The specifications of the 802.11 standards are available on the IEEE 802.11 working group website.

802.16 - WiMax

- IEEE 802.16 is a collection of wireless broadband standards. Including extensive descriptions for the link layer (also called WiMax). WiMax standards provide data rates from 1.5 Mb/s to 1 Gb/s.

- The recent update (802.16m) provides data rates of 100 Mbit/s for mobile stations and 1 Gbit/s for fixed stations.

- The specifications of the 802.11 standards are readily available on the IEEE 802.16 working group website.

802.15.4 -LR-WPAN

- IEEE 802.15.4 is a collection of standards for low-rate wireless personal area networks (LR-WPANs). These standards form the basis of specifications for high level communication protocols such as ZigBee.

- LR-WPAN standards provide data rates from 40 Kb/s 250 Kb/s. These standards provide low-cost and low-speed communication for power constrained devices. The specifications of the 802.15.4 standards are available on the IEEE 802.15 working group website.

2G/3G/4G - Mobile Communication

- That arc different generations of mobile communication standards including second generation (2G- including GSM and CDMA) third generation (3G - including UMTS and CDMA2000) and fourth generation (4G -including LTE). IoT devices based on these standards can communicate over cellular networks. Data rates for these standards range from 9.6 Kb/s (for 2G to upto 100 Mb/s (for 4G) and are available from the 3GPP websites.

Network/Internet Layer

- The network layers are responsible for sending of IP datagram from the source network to the destination network. This layer performs the host addressing and packet routing.

- The datagram contain the source and destination addresses which are used to route them from the source to destination across multiple networks. Host identification is completed exploitation graded science addressing schemes like IPv4 or IPv6.

IPv4

- Internet Protocol version 4 (IPv4) is the most deployed Internet protocol that is used to identify the devices on a network using a hierarchical addressing scheme.

- IPv4 uses a 32-bit address scheme that allows total of 2^{32} or 4,294,967,296 addresses. As more and more devices got connected to the Internet these addresses got exhausted in the year 2011. IPv4 has been succeeded by IPv6.

- The IP protocols establish connections on packet networks but do not guarantee delivery of packets. Guaranteed delivery and data integrity are handled by the upper layer protocols (such as TCP). IPv4 is formally described in RFC 791.

IPv6

Internet Protocol version 6 (WI/6) is the newest version of Internet protocol and successor to IPv4. IPv6 uses 128-bit address scheme that allows total of 21128 or 3.4 x 1038 addresses. IPv4 is formally described in RFC 2460.

6LoWPAN

6LoWPAN (IPv6 over Low power Wireless Personal Area Networks) brings IP protocol to the low-power devices which have limited processing capability.

☞ Transport Layer

– The transport layer protocols give end-to-end message transfer capability freelance of the underlying network.

– The message transfer capability can be set up on connections either using handshakes (as in TCP) or without handshakes/acknowledgements (as in UDP).

– The transport layer provides functions such as error control, segmentation, flow control and congestion control.

☞ TCP

– Transmission Control Protocol (TCP) is the most widely used transport layer protocol, that is used by web browsers (along with HITTT: HTTPS application layer protocols) email programs (SMTP application layer protocol) and file transfer (FTP).

– TCP is a connection oriented and stateful protocol. While IP protocol deals with sending packets. TCP ensures reliable transmission of packets in-order.

– TCP also provides error detection capability so that duplicate packets can be discarded and lost packets are retransmitted.

– The How control capability of TCP ensures that rate at which the sender sends the data is not too high for the receiver to process.

– The congestion control capability of TCP helps in avoiding network congestion and congestion collapse which can lead to degradation of network performance. TCP is described in RFC 793.

☞ UDP

– Unlike TCP which requires carrying out an initial setup procedure.

– UDP is a connectionless protocol. UDP is useful for time-sensitive applications that have very small data units to exchange and do not want the overhead of connection setup.

UDP is a transaction oriented and stateless protocol. UDP does not provide guaranteed delivery, ordering of messages and duplicate elimination.

– Higher levels of protocols can ensure reliable delivery or ensuring connections created are reliable. UDP described in RFC 768.

☞ Application layer

– Application layer protocols define how the application interface with the lower layer protocols to send the data over the network.

– The application data, typically in tiles, is encoded by the application layer protocol and encapsulated in the transport layer protocol which provides connection of transaction oriented communication over the network.

– Port numbers are used for application addressing (for example port 80 for HTTP, port 22 for SSH. etc.)

– Application layer protocols enable process-to-process connections using ports.

☞ HTTP

– Hypertext Transfer Protocol (HTTP) is the application layer protocol that forms the foundation of the World Wide Web (WWW). HTTP includes commands such as GET, PUT, POST, DELETE, HEAD, TRACE, OPTIONS. etc.

– The protocol follows a request-response model where a client sends requests to a server using the HTTP commands.

– HTTP is a stateless protocol and each HTTP request is independent of the other requests. An HTTP client can be a browser or an application running on the client (e.g. an application running on an IoT device, a mobile application or other software).

– HTTP protocol uses Universal Resource Identifiers (URIs) to identify HTTP resources. HTTP is described in RFC 2616.

☞ CoAP

– Constrained Application Protocol (CoAP) is an application layer protocol for

– Machine-to-machine (M2M) applications meant for constrained environments with constrained devices and constrained networks. Like HTTP. CoAP is a web

transfer protocol and uses a request-response model; however it runs on top of UDP instead of TCP.

- CoAP uses a client-server architecture where clients communicate with servers using connectionless datagrams. CoAP is designed to easily interface with HTTP. Like HTTP.

- CoAP supports methods such as GET, PUT, POST and DELETE. CoAP draft specifications are available on IEFT Constrained environments (CORE) Working Group website.

☞ Web Socket

- Web Socket protocol allows full-duplex communication over a single socket connection for sending messages between client and server.

- Web Socket is based on TCP and allows streams of messages to he sent back and forth between the client and server while keeping the TCP connection open.

- The client can be a browser, a mobile application or an IoT device. Web Socket is described in RFC 6455.

☞ MQTT

- Message Queue Telemetry Transport (MQTT) is a light-weight messaging protocol based on the publish-subscribe model.

- MQTT uses a client-server architecture where the client (such as an IoT device) connects to the server (also called MQTT Broker) and publishes messages to topics on the server.

- The broker forwards the messages to the clients subscribed to topics. MQTT is compatible for strained environments wherever the devices have restricted process and memory resources and also the network information measure is low. MQTT specifications are available on IBM developer Works.

☞ XMPP

- Extensible Messaging and Presence Protocol (XMPP) is a protocol for real-time communication and streaming XML data between network entities.

- XMPP powers wide range of applications including messaging, presence, data syndication, gaming, multi-party chat and voice/video calls.

- XMPP allows sending small chunks of XML data from one network entity to another in near real-time. XMPP is a decentralized protocol and uses client-server architecture.

- XMPP supports both client-to-server and server-to-server communication paths. In the context of IoT. XMPP allows real-time communication between IoT devices. XMPP is described in RFC 6120.

☞ DOS

- Data Distribution Service (DDS) is a data-centric middleware standard for device-to-device or machine-to-machine communication.

- DDS uses a publish-subscribe model where publishers (e.g. devices that generate data) create topics to which subscribers (e.g.. devices that want to consume data) can subscribe.

- Publisher is an object responsible for data distribution and the subscriber is responsible for receiving published data DDS provides quality-of-service (QoS) control and configurable reliability. DDS is described in Object Management Group (OMG) DDS specification.

☞ AMQP

- Advanced Message Queuing Protocol (AMQP) is an open application layer protocol for business messaging.

- AMQP supports both point-to-point and publisher / subscriber models, routing and queuing.

- AMQP brokers receive messages from publishers (e.g. devices or applications that generate data) and route them over connections to consumers (applications that process data).

- Publishers publish the messages to exchanges which then distribute message copies to queues.

- Messages are either delivered by the broker to the consumers which have subscribed to the queues or the consumers can pull the messages from the queues.

- AMQP specification is available on the AMQP working group website.

3.1.4 Logical Design of IoT

Logical design of an IoT system refers to a conceptual representation of the entities and processes instead going into the low-level specifics of the implementation. In this section we describe the functional blocks of a IoT system and the communication APIs that are used for the examples in this book.

3.1.4.1 IoT Functional Blocks

An IoT system comprises of many numbers of functional blocks that helps to provide the system the capabilities for sensing, actuation, communication, and management as shown in Fig. 3.1.2. These functional blocks are described as follows:

☞ Device

An IoT system is combination of devices that provide sensing, actuation, and monitoring and control functions.

☞ Communication

This block handles the communication for the IoT system.

☞ Services

An IoT system uses various types of IoT services such as services for device monitoring, device control services, data publishing services and services for device discovery.

☞ Management

Management block provides various functions to govern the IoT system.

☞ Security

This functional block helps to secures the IoT system and by providing functions like authentication, authorization, message and content integrity and security.

☞ Application

- IoT applications provide an interface that the users can use to control and monitor many number of aspects the IoT system.

- Applications also allow users to view the system status and view or analyze the processed data.
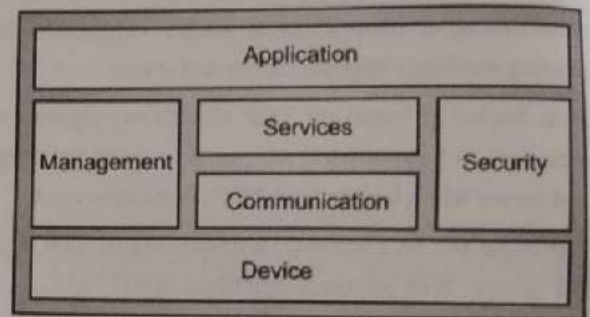
Fig. 3.1.2 : Functional Blocks of IoT

3.1.4.2 IoT Communication Models

☞ Request-Response

- Request-Response is a communication model in which the client sends requests to the server and the server responds to the requests.

- When the server receives an invitation, it decides the way to respond, fetches the info, retrieves resource representations, prepares the response, then sends the response to the client.

- Request-Response model is a stateless communication model and each request-response pair is independent of others.

- Fig. 3.1.3 shows the client-server interactions in the request-response model.

Fig. 3.1.3 : Request-Response Communication Model

Publish-Subscribe

- Publish-Subscribe is a communication model that involves publishers, brokers and consumers. Publishers are the source of data. Publishers send the info to the topics which are managed by the broker.
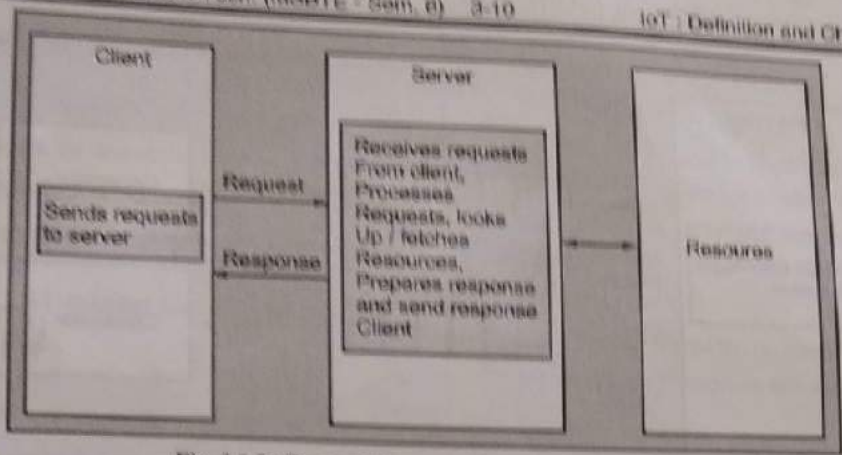
- Publishers are not aware of the consumers. Consumers subscribe to the topics which are managed by the broker. When the broker receives data for a subject from the publisher.

- It sends the data to all the subscribed consumers. Fig. 3.1.4 shows the publisher-broker-consumer interactions in the publish-subscribe model.
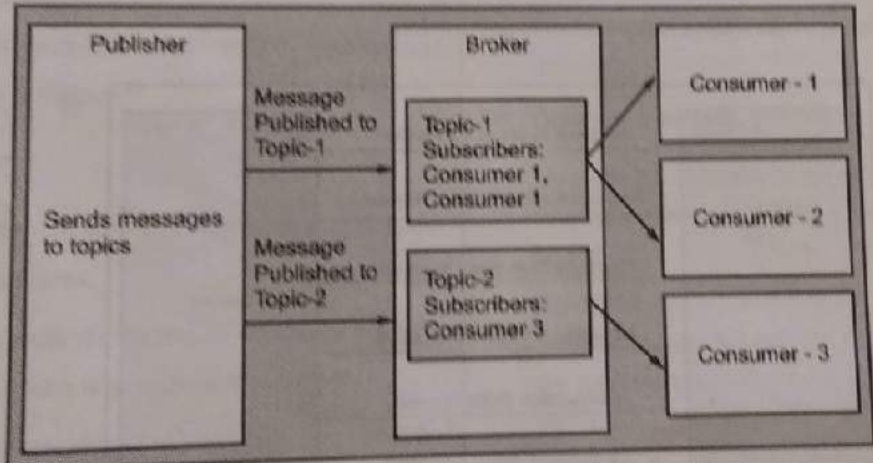
Fig. 3.1.4 : Publish-Subscribe communication model

Push-Pull

- Push-Pull is a communication model in which the data producers push the data to queues and the consumers pull the data from the queues.

- Producers do not need to be aware of the consumers. Queues help in decoupling the messaging in between the producers and consumers.

- Queues also acting as a buffer which helps in situations when there is a mismatch between the rate at which the producers push data and the rate at which the consumers pull data. Fig. 3.1.5 shows the publisher-queue-consumer interactions in the push-pull model.
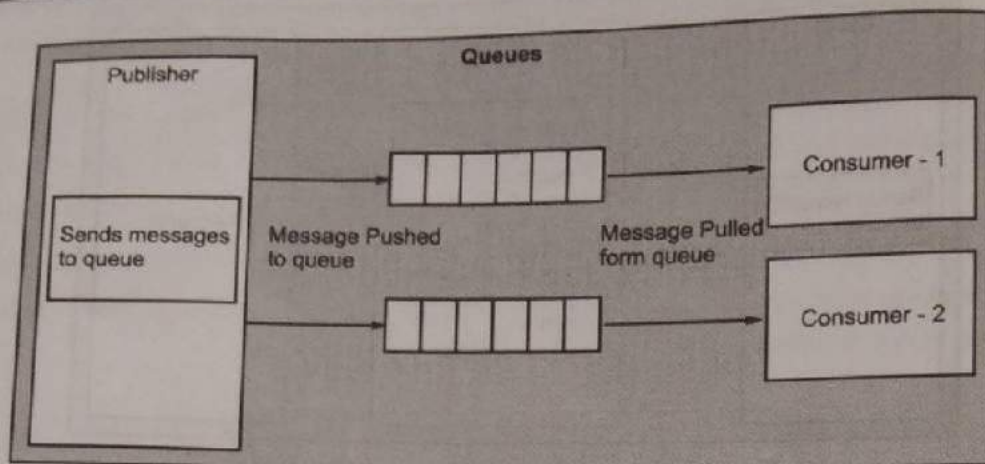
Fig. 3.1.5 : Push-Pull communication model

☞ **Exclusive Pair**

- Exclusive Pair is a bi-directional, fully duplex communication model that uses a persistent connection between the client and server.

- Once the connection is setup it always remains open till the client sends a request to close the connection. Client and server can send messages to each other after completion of connection setup.

- Exclusive pair is a stateful communication model and the server is aware of all the open connections. Figure 3.1. shows the client-server interactions in the exclusive pair model.
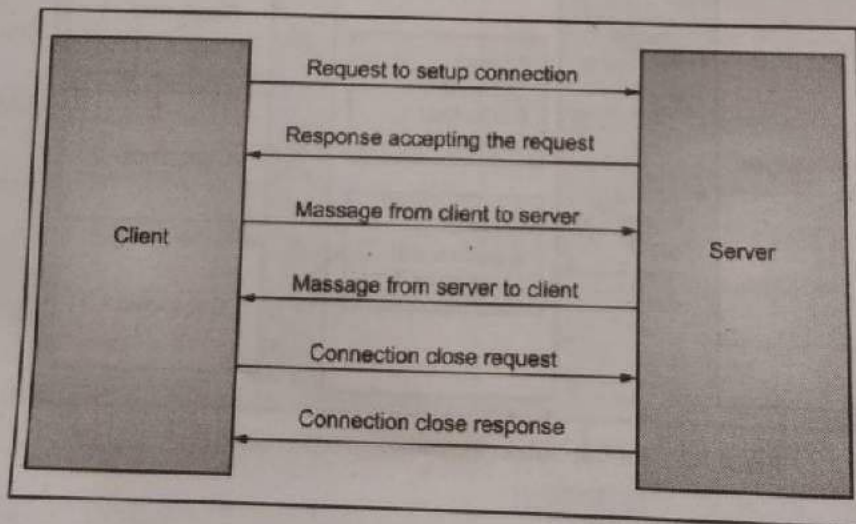
Fig. 3.1.6 : Exclusive Pair communication model

3.1.4.3 IoT Communication APIs

In the previous section you learned about various communication models. In this section you will learn about two specific communication APIs which are used in the examples in this book.

3.1.4.3.1 REST-based Communication APIs

- Representational State Transfer (REST) is a set of architectural principles by which you can design web services and web APIs that focus on a system's resources and how resource states are addressed and transferred.

- REST APIs follow the request-response communication model described in previous section.

- The REST architectural elements apply to the components, connectors and data elements, inside a distributed hypermedia. The REST architectural constraints are as follows :

Client-Server

- The principle behind the client-server constraint is the separation of concerns.

- Par example, clients should not be concerned with the storage of data which is a concern of the server.

- Similarly, the server should not be concerned about the user interface which is a concern of the client. Separation allows client and server to be independently developed and updated.

Stateless

Every request from client to server must have all the important info to understand the request and cannot take superiority of any stored content on the server. The session state is kept completely on the client.

Cache-able

- Cache constraint requires that the data within a response to a request be implicitly or explicitly labelled as cache-able or non-cache-able.

- If a response is cache-able, then a client cache is given the proper to reuse that response data for later equivalent requests.

- Caching can partially or completely eliminate some interactions and improve efficiency and scalability.

Layered System

- Layered system constraint, constrains the behaviour of components such that each component cannot see beyond the immediate layer with which they are interacting.

- For example a client cannot tell whether it's connected on to the top server or to an intermediary along the way.

- System scalability can be improved by allowing intermediaries to respond to requests instead of the end server without the client having to do anything different.

Uniform Interface

- Uniform Interface constraint requires that the method of communication between a client and a server must be uniform.

- Resources are identified in the requests (by URIs in web based systems) and are themselves separate from the representations of the resources that are returned to the client.

- When o client holds a representation of a resource it has all the information required to update or delete the resource (provided the client has required permissions).

- Each message includes enough information to explain the way to process the message.

Cade on demand

Servers can provide executable code or scripts for clients to execute in their context. This constraint is the only one that is optional.
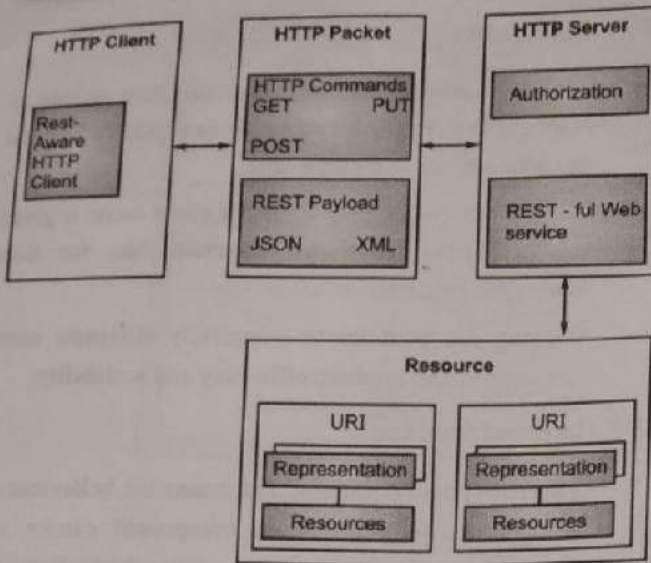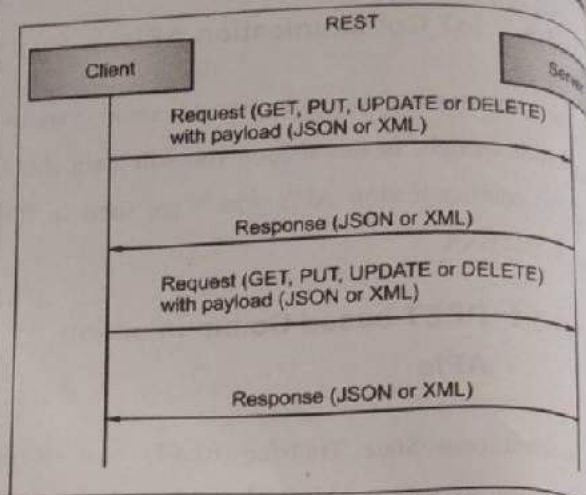
Fig. 3.1.7 : Communication with REST APIs

- A RESTful web service is a "web API" implemented with the help of HTTP and REST principles. Fig. 3.1.7 shows the communication in between client and server with the help of REST APIs.

- Fig. 3.1.8 how's the interactions in the request-response model used by REST.

- Restful web service is a collection of resources which are represented by URIs. RESTful web API has a base URI (e.g. http://example.com/api/tasks/).

- The clients send requests to these URIs using the methods defined by the HTTP protocol (e.g., GET, PUT, POST or DELETE).

- A RESTful web service can support various Internet media types (EON being the most popular media type for RESTful web services).

- IP for Smart Objects Alliance (IPSO Alliance) has published an Application Framework that defines a RESTful design for use in IP smart object systems.

Fig. 3.1.8 : Request-response model by REST

3.1.4.3.2 WebSocket-based Communication APIs

- WebSocket APIs allow bi-directional, full duplex communication between clients and servers. WebSocket APIs follows the exclusive communication model described in previous section and as shown in Fig. 3.1.8 Unlike request-response APIs such as REST.

- The WebSocket APIs allow full duplex communication and do not require a new connection to be setup for each message to be sent. WebSocket communication begins with a connection setup request sent by the client to the server.

- This request (called a WebSocket handshake) is sent over HTTP and the server interprets it as an upgrade request. If the server supports WebSocket protocol.

- The server responds to the WebSocket handshake response. After the connection is setup. The client and server can send data/messages to each other in full duplex mode.

- WebSocket APIs reduces the network traffic and latency as there's no overhead for connection setup and termination requests for every message.

- WebSocket is suitable for IoT applications that have low latency or high throughput requirements.

3.1.5 IoT Enabling Technologies

- IoT is enabled by several technologies including wireless sensor networks, cloud computing, big data analytics, embedded systems, security protocols and architectures, communication protocols, web services, mobile Internet, and semantic search engines.

- This section provides an overview of some of these technologies which play a key-role in IoT.

3.1.5.1 Wireless Sensor Networks

- A Wireless Sensor Network (WSN) comprises of distributed devices with sensors which are used to monitor the environmental and physical conditions.

- A WSN contains variety of end-nodes and routers and a coordinator. End nodes have several sensors attached to them. End nodes can also act as routers. Routers are responsible for routing the data packets from end-nodes to the coordinator.

- The coordinator collects the data from all the nodes. Coordinator also acts as a gateway that connects the WSN to the Internet. Some examples of WSNs used in IoT systems are described as follows:

- Weather monitoring systems use WSNs in which the nodes collect temperature, humidity and other data, which is aggregated and analyzed.

- Indoor air quality monitoring systems use WSNs to collect data on the indoor air quality and concentration of various gases.

- Soil moisture monitoring systems use WSNs to monitor soil moisture at various locations.

- Surveillance systems use WSNs for collecting surveillance data (such as motion detection data)

- Smart grids use WSNs for monitoring the grid at various points.

- Structural health monitoring systems use WSNs to watch the health of structures (buildings, bridges) by collecting vibration data from sensor nodes deployed at various points within the structure.

- WSNs are enabled by wireless communication protocols like IEEE 802.15.4. ZigBee is one among the foremost popular wireless technologies employed by WSNs.

- ZigBee specifications are supported IEEE 802.15.4. ZigBee operates at 2.4 GHz frequency and offers data rates upto 250 KB/s and range from 10 to 100 meters counting on the facility output and environmental conditions.

- The facility of WSNs lies in their ability to deploy sizable amount of low-cost and low-power sensing nodes for continuous monitoring of environmental and physical conditions. WSNs are self-organizing networks.

- Since WSNs have sizable amount of nodes, manual configuration for every node isn't possible.

- The self-organizing capability of WSN makes the network robust. Within the event of failure of some nodes or addition of latest nodes to the network, the network can reconfigure itself

3.1.5.2 Cloud Computing

- Cloud computing may be a transformative computing paradigm that involves delivering applications and services over the web.

- Cloud computing involves provisioning of computing, networking and storage resources on demand and providing these resources as metered services to the users, during a "pay as you go" model.

- Cloud computing resources are often provisioned on-demand by the users, without requiring interactions with the cloud service provider.

- The method of provisioning resources is automated.

- Cloud computing resources are often accessed over the network using standard access mechanisms that provide platform-independent access through the utilization of heterogeneous client platforms like workstations, laptops, tablets and smart-phones.

- The storage memory resources provided by cloud service providers are pooled to multiple users using multi-tenancy. Multi-tenant aspects of the cloud allow multiple users to be served by an equivalent physical hardware.

- Users are assigned virtual resources that execute on top of the physical resources. Cloud computing services are offered to users in different forms:

☞ Infrastructure-as-a-Service (Iaas)

- Iaas provides the users the ability to provision computing and storage resources.

- These resources are provided to the users as virtual machine instances and virtual memory. Users can Malt stop, configure and manage the virtual machine instances and virtual memory.

- Users can deploy operating systems and applications of their choice on the virtual resources provisioned in the cloud.

- The cloud service provider manages the underlying infrastructure. Virtual resources provisioned by the users are billed based on a pay-per-um paradigm.

☞ Platform-as-a-Service (PaaS)

- PaaS provides the users the ability to develop and deploy application in the cloud using the development tools, application programming interfaces (APIs), software libraries and services are provided by the cloud service provider.

- The cloud service provider manages the fundamental cloud infrastructure which includes servers, network, operating systems and storage.

- The user, themselves are responsible for developing, deploying, configuring and managing applications over the cloud infrastructure.

☞ Software-as-a-Service (SaaS)

- SaaS provides the users a complete software application or the user interface to the application itself.

- The cloud service provider manages the underlying cloud infrastructure including servers, network, operating systems, storage and application software and the user is unaware of the underlying architecture of the cloud.

- Applications are provided to the user through a skinny client interface (e.g.. a browser).

- Sat AS applications are platform independent and can be accessed from various client devices such as workstations, laptop, tablet and smart-phones running

different operating systems. Since the cloud provider manages both the appliance and data the are able to access the applications from anywhere

☒ 3.1.5.3 Big Data Analytic

Big data is defined as collections of data sets volume, velocity (in terms of its temporal variation variety is so huge that it is difficult to store, manage, and analyze the info using traditional databases processing tools. Big data analytic, involves several starting from data cleansing, data munging (or wrang data processing and visualization. Some examples of data generated by IoT systems are described as follows

- Sensor data generated by IoT systems such as wea monitoring stations.

- Machine sensor data collected from sensors embed in industrial and energy systems for monitoring health and detecting failures.

- Health and fitness data generated by IoT devices s as wearable fitness bands.

- Data generated by IoT systems for location tracking of vehicles.

- Data generated by retail inventory monitoring system

- The underlying characteristics of big data include:

☞ Volume

- Though there is no fixed threshold for the volume data to he considered as big data, however, typical the term big data is used for massive scale data that difficult to store, manage and process using tradition databases and data processing architectures.

- The volumes of data generated by modern industrial, and health-care systems, for example, growing exponentially driven by the lowering costs data storage and processing architectures and the ne to extract valuable insights from the data to improv business processes, efficiency and service consumers.

☞ Velocity

Velocity is another important characteristic of big data and the primary reason for exponential growth of data. Velocity of data refers to how fast the data is generated and how frequently it varies. Modern IT, industrial and other systems are generating data at increasingly higher speeds.

☞ Variety

Variety refers to the forms of the data. Big data comes in different forms such as structured or unstructured data, including text data, image, audio, video and sensor data.

3.1.5.4 Communication Protocols

- Communication protocols form the heart of IoT systems and enable network connectivity and coupling to applications.

- Communication protocols allow devices to interchange data over the network. These protocols define the data exchange formats, data encoding, addressing schemes for devices and routing of packets from source to destination.

- Other functions of the protocols include sequence control (that helps in ordering packets determining lost packets), flow control (that helps in controlling the rate at which the sender is sending the data so that the receiver or the network is not overwhelmed) and retransmission of lost packets.

3.1.5.5 Embedded Systems

- An Embedded System is a computer system that has computer hardware and software embedded to perform specific tasks.

- In contrast to general purpose computers or personal computers (PCs) which can perform various types of tasks, embedded systems are designed to perform a specific set of tasks.

- Key components of an embedded system include microprocessor or microcontroller, memory (RAM, ROM, and cache), networking units (Ethernet, Wi-Fi adapters), input/output units (display, keyboard, etc.) and storage (such as flash memory).

- Some embedded systems have specialized processors such as digital signal processors (DSPs), graphics processors and application specific processors.

- Embedded systems run embedded operating systems such as real-time operating systems (RTOS).

- Embedded systems range from low-cost miniaturized devices such as digital watches to devices such as digital cameras, point of sale terminals, vending machines, appliances (such as washing machines), etc. In the next chapter we describe how such devices form an integral part of IoT systems.

3.1.6 IoT Levels and Deployment Templates

In this section we define various levels of IoT systems with increasing completely. An IoT system comprises of the following components :

☞ Device

An IoT device allows identification, remote sensing, actuating and remote monitoring capabilities.

☞ Resource

Resources are software elements on the IoT device for accessing, processing, and storing sensor info, or controlling actuators joined to the device. Resources also include the software elements that enable network access for the device.

☞ Controller Service

Controller service may be a native service that runs on the device and interacts with the online services. Controller service sends data from the device to the online service and receives commands from the appliance (via web services) for controlling the device.

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   3-17

IoT : Definition and Characteristics

☞ Database

Database can be either local or in the cloud and stores the data generated by the IoT device.

☞ Web Service

Web services serve as a link between the IoT device, application, database and analysis components. Web services are often either implemented using HTTP and REST principles (REST service) or using WebSocket protocol (WebSocket service). A comparison of REST and WebSocket is provided below:

☞ Stateless/Stateful

- REST services are stateless in nature. Each request contains all the knowledge needed to process it.
- Requests are independent of each other.
- WebSocket on the other hand is stateful in nature where the server maintains the state and is aware of all the open connections.

☞ Uni-directional/Bi-directional

- REST services operate over HTTP and are uni-directional.
- Request is always sent by a client and the server responds to the requests.
- On the other hand, WebSocket is a bi-directional protocol and allows both client and server to send messages to each other.

☞ Request-Response/Full Duplex

- REST services follow a request-response communication model where the client sends requests and the server responds to the requests.
- WebSocket on the oilier hand allow full-duplex communication between the client and server, i.e., both client and server can send messages to each other independently.

☞ TCP Connections

- For REST services, each HTTP request involves setting up a new TCP connection.
- WebSocket on the other hand involves a single connection over which the client and server communicate in a full-duplex mode.

☞ Header Overhead

- REST services operate over HTTP, and each request independent of others. Thus each request carries HTTP header which is an overhead.
- Due the overhead of HTTP headers, REST is suitable for real-time applications.
- WebSocket on the other hand does not involve overhead of headers. After the initial handshake (which happens over HTTP), the client and server exchange messages with minimal frame information. The WebSocket is suitable for real-time applications.

☞ Scalability

Scalability is easier in the case of REST services requests are independent and no state information needs be maintained by the server. Thus both horizontal (scaling out) and vertical scaling (scaling-up) solutions are possible for REST services. For WebSockets, horizontal scaling can be cumbersome due to the stateful nature of the communication. Since the server maintains the state of connection, vertical scaling is easier for WebSockets than horizontal scaling.

☞ Analysis Component

The Analysis Component is responsible for analyzing the IoT data and generates results in a form which are easy for the user to understand. Analysis of IoT data can be performed either locally or in the cloud. Analyzed results are stored in the local or cloud databases.

☞ Application

IoT applications provide an interface that the users can use to manage and monitor various aspects of the IoT system. Applications also allow users to look at the system status and consider the processed data.

➲ 3.1.6.1   IoT Level-1

– A level-I MT system has a single node/device that performs sensing and/or actuation, stores data, performs analysis and hosts the application as shown in Fig. 3.1.9.

– Level-1 IoT systems are compatible for modelling low-cost and low-complexity solutions where the info involved isn't big and therefore the analysis requirements aren't computationally intensive.

– Let us now consider an example of a level-1 IoT system for home automation.

– The system consists of one node that permits controlling the lights and appliances during a home remotely.

– The device used in this system interfaces with the lights and appliances using electronic relay switches.

– The status information of each light or appliance is maintained in a local database.

– REST services deployed locally allow retrieving and updating the state of each light or appliance in the status database.

– The controller service continuously monitors the state of each light or appliance (by retrieving state from the database) and triggers the relay switches accordingly.

– The application which is deployed locally has a user interface for controlling the lights or appliances. Since the device is connected to the Internet, the application can be accessed remotely as well.
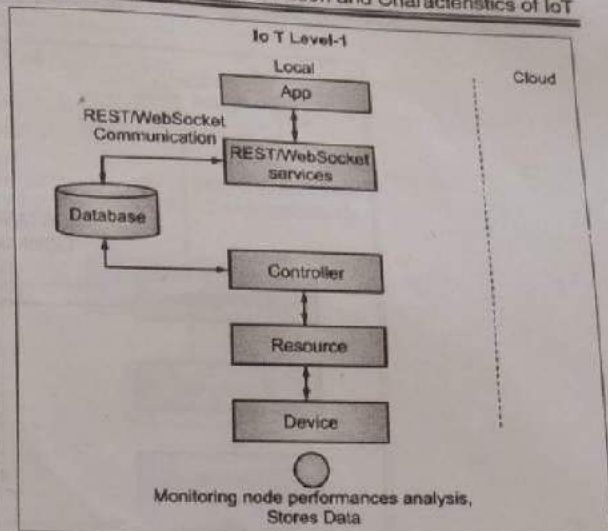
Fig. 3.1.9 : IoT Level-1

➲ 3.1.6.2   IoT Level-2

– A level-2 IoT system has a single node that performs sensing and/or actuation and local analysis as shown in Fig. 3.1.10.

– Data is stored within the cloud and application is typically cloud-based. Level-2 IoT systems are compatible for solutions where the data involved is big, however, the primary analysis need isn't computationally intensive and should be done locally by itself. Let us consider an example of a level-2 IoT system for smart irrigation.

– The system consists of one node that monitors the soil moisture level and controls the irrigation system.

– The device utilized in this technique collects soil moisture data from sensors.

– The controller service continuously monitors the moisture levels.

– If the moisture level gets below a threshold, the irrigation system is turned on.

– For controlling the irrigation system actuators such as solenoid valves can be used.

– The controller also sends the moisture data to the computing cloud.

– A cloud-based REST web service is used for storing and retrieving moisture data which is stored in the cloud database.

– A cloud-based application is used for visualizing the moisture levels over a period of time, which can help in making decisions about irrigation schedules.
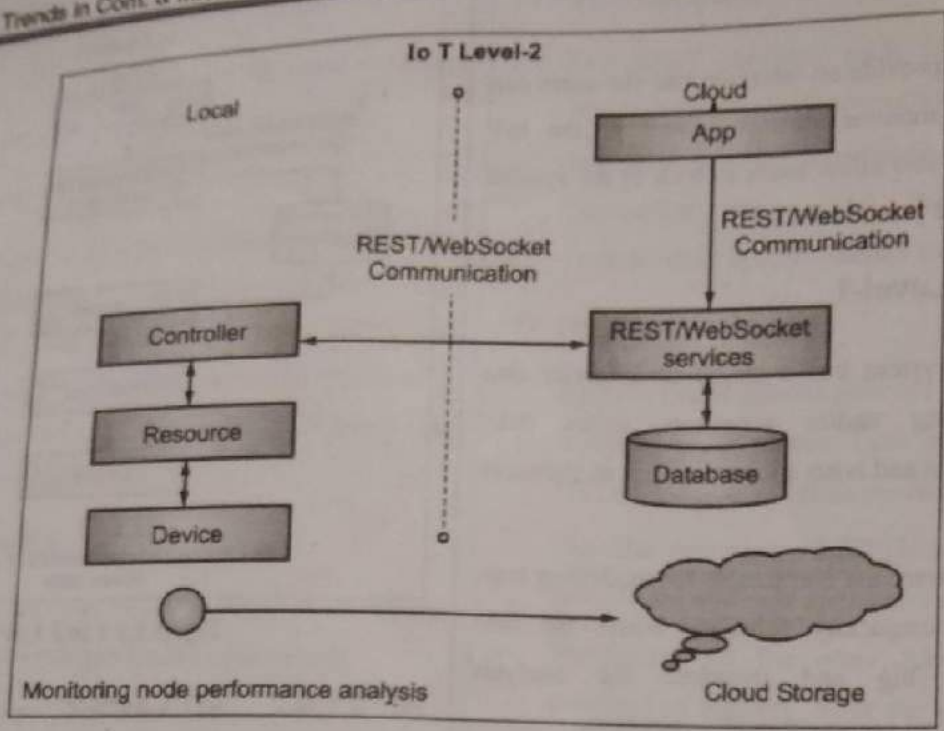
Fig. 3.1.10 : IoT Level-2

3.1.6.3 IoT Level-3

- A level-3 IoT system has a single node. Data is stored and analyzed in the cloud and application is cloud-based shown in Fig. 3.1.11. Level-3 IoT systems are suitable for solutions where the info involved is big and therefore the analysis requirements are computationally intensive.

- Let us consider an example of a level-2 IoT system for tracking package handling.

- The system consists of one node (for a package) that monitors the vibration levels for a package being shipped.

- The device during this system uses accelerometer and gyroscope sensors for monitoring vibration levels.

- The controller service sends the sensor data to the cloud in real-time using a WebSocket service. The data is stored the cloud and also visualized using a cloud-based application.

- The analysis components in the cloud can trigger alerts if the vibration levels become greater than a threshold.

- The benefit of using WebSocket service instead of REST service in this example is that, the sensor data can be sent real time to the cloud.

- Moreover, cloud based applications can subscribe to the sensor data feeds for viewing the real-time data.
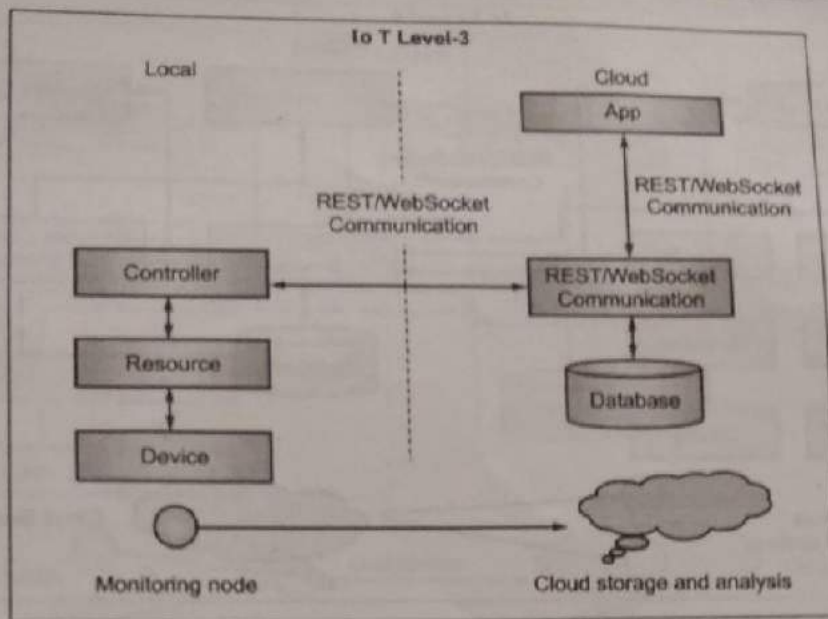
Fig. 3.1.11 : IoT Level-3

⚄ 3.1.6.4   IoT Level-4

- A level-4 IoT system has multiple nodes that perform local analysis. Data is stored in the cloud and application is cloud-based as shown in Fig. 3.1.12.

- Level-4 contains local and cloud-based observer nodes which can subscribe to and receive information collected in the cloud from IoT devices. Observer nodes can process info and use that info for various applications; however, observer nodes don't perform any of the control functions.

- Level-4 IoT systems are compatible for solutions where multiple nodes are needed, the info involved is big and therefore the analysis requirements are computationally intensive. Let us consider an example of a level-4 IoT system for noise analysis.

- The system consists of multiple nodes placed in different locations for monitoring noise levels in an area.

- The nodes in this example are equipped with sound sensors. Nodes are independent of each other. Each node runs its own controller service that sends the data to the cloud.

- The data is stored in a cloud database. The analysis of data collected from a number of nodes is done in the cloud. A cloud-based application is used for visualizing the aggregated data.
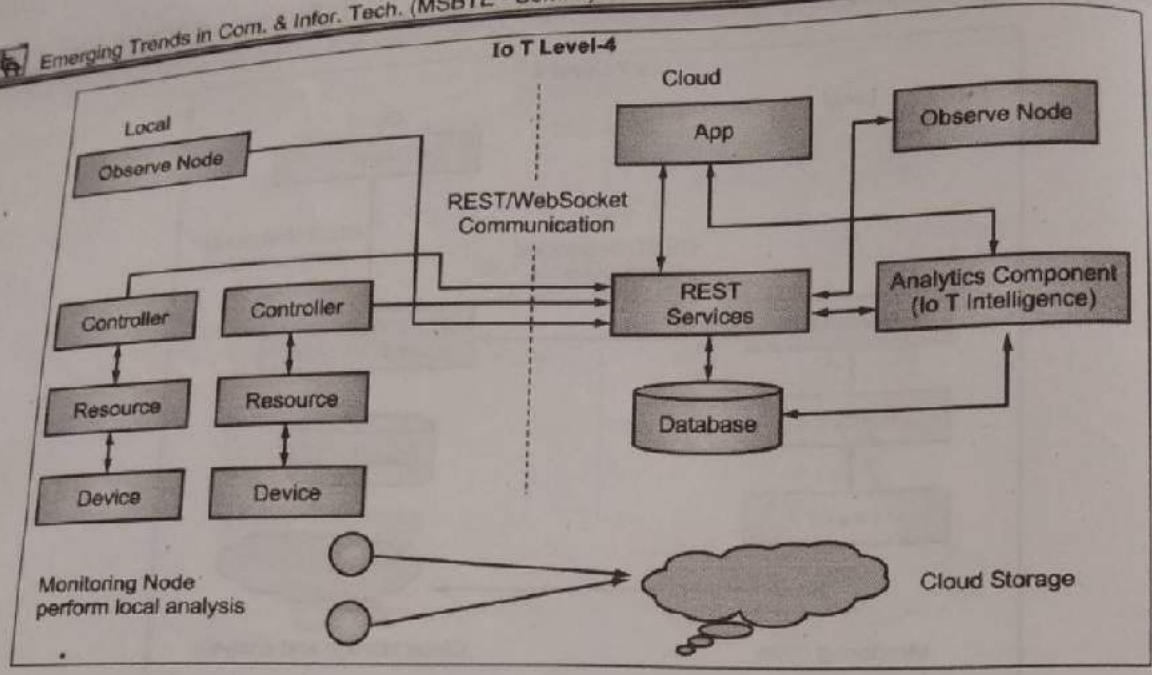
Fig. 3.1.12 : IoT Level-4

3.1.6.5   IoT Level-5

- A level-5 LIT system has multiple end nodes and one coordinator node as shown in Figure 3.1.13. The end nodes that perform sensing and/or actuation.

- Coordinator node collects data from the end nodes and sends to the cloud. Data is stored and analyzed within the cloud and application is cloud-based. Level-5 IoT systems are suitable for solutions based on wireless sensor networks, in which the data involved is big and the analysis requirements are computationally intensive. Let us consider an example of a level-3 for system for forest fire detection.

- The system consists of multiple nodes placed indifferent locations for monitoring temperature, humidity and carbon dioxide (CO_2) levels in a Coast.

- The end nodes in this example are equipped with various sensors (such as temperature, humidity and CO_2). The coordinator node collects the data from the end nodes and acts as a gateway that provides Internet connectivity to the IoT system.

- The controller service on the coordinator device sends the collected data to the cloud-The data is stored in a cloud database.

- The analysis of data is done in the computing cloud to aggregate the data and make predictions. A cloud-based application is used for visualizing the data.
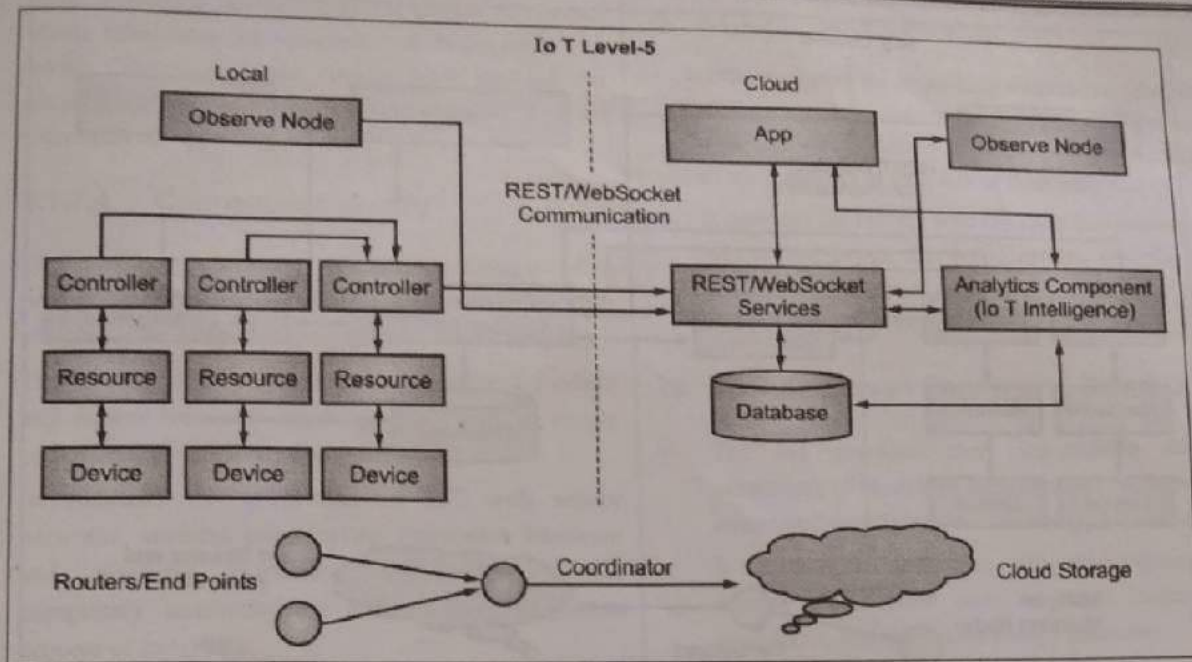
Fig. 3.1.13 : IoT Level-5

3.1.6.6 IoT Level-6

– A level-6 IoT system has multiple independent end nodes that perform sensing and/or actuation and send data to the cloud. Data is stored in the cloud and application is cloud-based as shown in Fig. 3.1.14.

– The analytics component analyzes the info and stores the leads to the cloud database. The results are visualized with the cloud-based application.

– The centralized controller is aware of the status of all the cad nodes and sends control commands to the nodes. Let us consider an example of a level-6 IoT system for weather monitoring.

– The system consists of multiple nodes placed in several locations for monitoring temperature, humidity and pressure in an area.

– The end nodes art equipped with various season (such as temperature, pressure and humidity), the end nodes send the data to the cloud in real-time using a WebSocket service. The data is stored in a cloud database.

– The analysis of data is done in the cloud to aggregate the data and make predictions. A cloud-based application is used for visualizing the data.

IoT : Definition and Characteris

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   3-23

Emerging Trends in
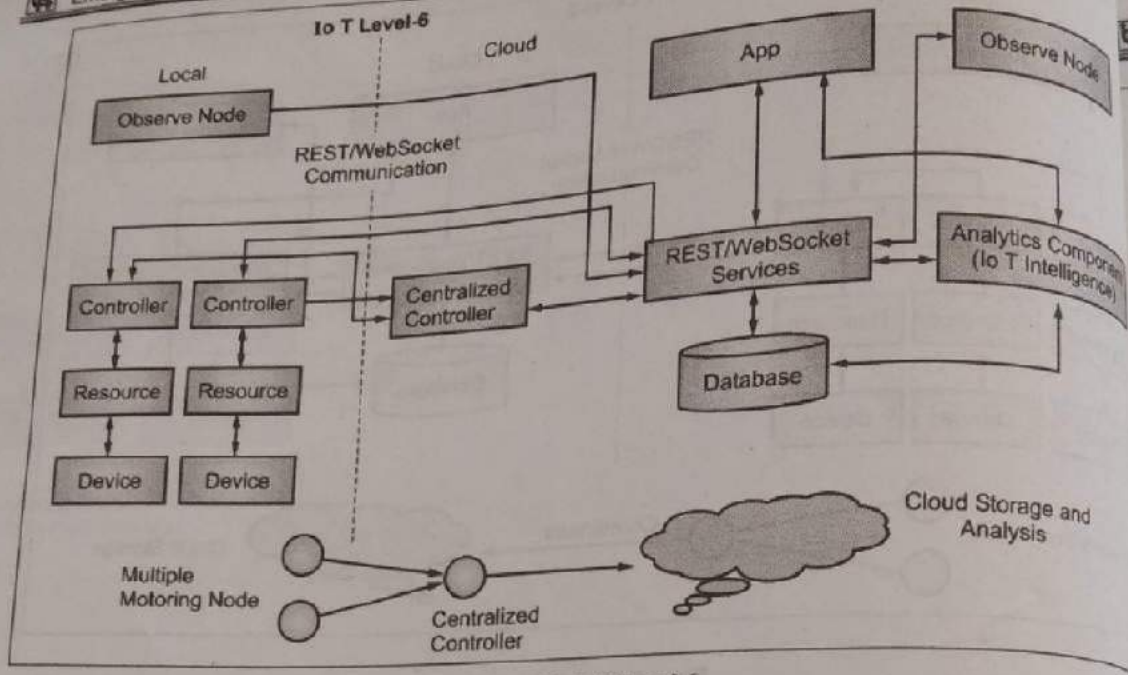
Fig. 3.1.14 : IoT Level-6

3.1.7 IoT challenges, Applications

The IoT has the potential to attach everyday objects. It has introduced many numbers of applications and smart services, which have affected users' day today lives.

3.1.7.1 Healthcare

- The IoT has brought many benefits and opportunities to the field of healthcare. It helps to develop and improve healthcare services and keep the sector innovative.

- For instance, intelligent drug/medicine control and hospital management. In addition, the IoT merge more benefits by monitoring the everyone's health in real-time.

- Also, ambulances can be immediately dispatched to accident scenes and patients can be monitored at their homes just as effectively as in hospitals. For example, a doctor can immediately be informed if the patient suffers a heart attack.

3.1.7.2 Smart City

- The concept of the smart city is used to descri better use of public resources, increasing the qu service presented to the citizens, and at the sam reducing operational costs of public administratio

- The IoT provides many numbers of benefits wi management and tuning of public services transport and parking, lighting, surveillance maintenance of public areas, preservation of ar heritage, and garbage collection.

- Furthermore, the availability of different types collected by IoT devices can be used to enhance awareness of people about the status of their cit stimulate the active participation of the citizens i management of public administration.

3.1.7.3 Smart Home

- People always attempt to find new approache extend their luxury. Currently, people can install s appliances inside their homes to regulate many house tasks.

These intelligent de
which eliminates
device. Therefore,
automation of hom
embedded devices

3.1.7.4 Con

- The connected
producing envir
communicate w

- The connected
and control vi
operational pro

- In addition,
networks, wir
and machin
completely t
process of in

3.1.7.5

- For retailers
extend supp
and reshape

- For instanc
inventory,
retailers,
improve t

3.1.7.6

- Connecte
can shar
to a wi
vehicles
functior
in futur

- The cc
minimi
remote
errors

- These
just s
the s
2040
of ca

- These intelligent devices have the choice of remote, which eliminates the necessity of being near the device. Therefore, these devices have enabled the automation of home activities by the adoption of varied embedded devices.

3.1.7.4   Connected Industry

- The connected industry is that the vision of a producing environment where every machine can communicate with all other machines across the plant.

- The connected industry with IoT will connect, monitor and control virtually anything, anywhere to supply operational productivity and profitability.

- In addition, the integration of IoT with sensor networks, wireless connectivity, innovative hardware and machine to-machine communication will completely transform the conventional automation process of industries.

3.1.7.5   Smart Retail

- For retailers, the IoT offers unlimited opportunities to extend supply chain efficiencies, develop new services, and reshape the customer experiences.

- For instance, applications for tracking goods, real-time inventory, information exchange among suppliers and retailers, and automated delivery capabilities will improve the retail sector.

3.1.7.6   Connected Car

- Connected cars are equipped with Internet access and can share their access with others, just like connecting to a wireless network in a home or office. More vehicles are starting to come equipped with this functionality, so be prepared to see more apps included in future cars.

- The connected car is considered as the best way to minimize accidents such that a pilot can operate the car remotely to minimize car accidents and reduce human errors.

- These driverless cars can provide functions more than just safety such as they can save valuable time, reduce the stress of driving etc. Some studies reveal that by 2040, driverless cars will account for up to 75 percent of cars on the road worldwide.

3.1.7.7   Smart Parking

- In recent time, smart parking sensors are attached in parking space to detect the arrival and departure of vehicles. It provides an efficient management solution to assist drivers to save lots of time and fuel.

- It provides the drivers with the right info about parking spaces and keeps the traffic system smooth. It also enables the power of deployment to book parking lot directly from the vehicle.

3.1.7.8   Smart Energy and Smart Grid

- The IoT provides more information about the behaviours of electricity suppliers and consumers in an automated way to improve the energy efficiency.

- It also provides consumers with smart management of energy consumption such as smart meters, smart appliances, and renewable energy resources.

3.1.7.9   Environmental Monitoring

- The key element of the IoT system is sensors which collect information about the encompassing environment. Therefore, with the IoT, a high-speed data system is often provided.

- This allows the entity that monitors wide-area environments and sensors deployed in the area to convey a huge amount of data easily such as pollution source monitoring, water quality monitoring, air quality monitoring .

3.1.7.10   Smart Agriculture

- With the presence of sensors in everywhere, farmers can use the large collected information to yield a far better return on investment. Sensing for soil moisture and nutrients, controlling water use for plant growth and finding custom fertilizer are some simple uses of IoT within the agriculture.

- In addition, many wireless technologies were used in the agriculture such as remote sensing, global positioning system and geographical information system. This successively will replace human labour with automatic machinery which can increase the productivity.

3.1.7.11 Wearable

- Watches are no longer just for telling time. Smart watches have turned our wrists into a Smartphone by enabling text messaging, phone calls, and more.

- Many other devices are used to give us more information about our workouts such as fit bit, Jawbone and others.

3.1.8 Challenges of the IoT

There are many challenges that stand in the way of the successful deployment of IoT applications. These challenges include:

3.1.8.1 Big Data

- As said earlier, the IoT system involves billions of devices which generate an enormous amount of knowledge. This data is variable in term of structure and often arrive in real-time.

- The volume, velocity and variety make the storing and analytics process, which is employed to get meaningful information, a really complex task.

- It is obvious that the IoT is one of the main sources of big data. Using the Cloud computing can facilitate storing this data for a long period of time.

- However, handling this massive amount of data is a substantial issue, as the whole performance of different applications is heavily reliant on the properties of this data management service.

- Moreover, one of the important factors that related to big data is the data integrity. This is because it affects the quality of service and its security and privacy aspects.

3.1.8.2 Networking

- IoT networking protocols can be divided into smart device networks and traditional networks, which is used to increase data rates.

- Smart networking protocols are expected to adopt the protocols already established in WSNs and Machine-to-Machine (M2M) communications. Building a networking protocol isn't a simple task because it

should satisfy the wants of ease-of-use, cost performance of the entire system.

- In addition, choosing the acceptable topology for protocol is another issue. However, the mesh topology is the most suitable choice for wireless communication in smart environments. Therefore, different communication protocols and different network topologies create a big challenge that must be handled.

3.1.8.3 Heterogeneity

- The IoT interconnects large numbers of devices/objects to supply new applications that improve our quality of life. However, one of the important challenges faced by the IoT system is the wide heterogencity of devices, platforms, operating systems, and services that exist and might be used to create new applications.

- As the IoT continues to grow, the necessity for services that employment with multiple IoT application will still increase to understand the promised efficiency gain of the IoT.

- In addition, the IoT system uses a good sort of devices with different features which make the connectivity and coordination process very difficult task.

3.1.8.4 Interoperability

- The IoT provides a standard network that connects almost every object in our surroundings. The inter connectivity between IoT devices helps to increases system production by generating new applications and services.

- This inter connectivity comes at a price, because the popularity increases, and therefore the number of devices and networks increase, the shortage of interoperability between them becomes a critical issue.

- Although there are many suggested solutions to unravel the interoperability issue like data-over-sound technology which encodes data into several tones to supply a sonic barcode, which may then be transmitted and decoded by IoT devices, the interoperability is still a big issue for the IoT system.

3.1.8.5   Scalability

-   The number of IoT devices grows rapidly. Predictions are made that by 2020; the amount of IoT devices will reach or maybe exceed 50 billion. Scalability means that the system is able to handle the specific needs as they arise.

-   The main purpose of creating the IoT system scalable is to satisfy the changing demands because the interest of individuals changes with time also because the environmental conditions.

-   In addition, scalability helps the system to work efficiently without any performance issues that may arise due to system expansion.

3.1.8.6   Security and Privacy

-   One of the most difficult issues that face most of the new technologies is the security and privacy. As the IoT system relies on sensors that installed in our environment. These sensors collect environment data as well as our habits, financial records and other sensitive information.

-   Therefore, providing a secure IoT system may be a compulsory task to continue its successful deployments in our surroundings.

-   The IoT is intrinsically vulnerable to most of the wireless common attacks because of most IoT devices are connected through wireless networks that are hard to protect against different attacks such as man-in-the middle attack and other attacks.

3.1.8.7   Maintenance

-   Maintenance may be a serious challenge to acknowledge as billions of latest devices flood the web. These devices may belong to different vendors who have already gone out of business, and their devices may be full of bugs that nobody will ever be able to fix.

-   In addition, many vendors do not care about upgrading their devices to the latest platforms and fix security and other problems in their devices which create a big challenge not only in overall performance but also it's considered as a liability which will be attacked easily and affect the entire IoT network.

3.1.9   IoT Devices and Its Features

3.1.9.2   Arduino

-   Arduino may be a microcontroller, which may be a a part of the pc. It runs only one program again and again. Arduino can be powered using a battery pack.It is very normal and simple to interface sensors and other electronic components to Arduino.

-   It is accessible for low cost. Arduino requires external hardware to attach to the web and this hardware is addressed properly using code. Arduino can provide onboard storage. Arduino has just one USB port to attach to the pc. Processor used in Arduino is from AVR family Atmega328P.

-   This is a just plug and play device. If power is connected it starts to run the program and if disconnected it gets stops. Arduino uses Arduino, C/C++.

3.1.9.2   Raspberry Pie

-   Raspberry pie is a mini computer with Raspbian OS. It can run multiple programs at a time. It is difficult to power employing a battery pack. It needs complex tasks like installing library files and software for interfacing sensors and other elements.

-   It is expensive. Raspberry Pi are often easily connected to the web using Ethernet port and USB Wi-Fi dongles. Raspberry Pi did not have storage on board. It provides an SD card port. Raspberry Pi has 4 USB ports to attach different devices.

-   The processor used is from ARM family. This should be properly shutdown otherwise there's a risk of files corruption and software problems. The Recommended programing language is python but C, C++, Python, ruby are pre-installed.

3.1.9.3   Node Microcontroller Unit

-   The Node MicroController Unit is an open source i.e. free software and hardware development environment that's built around an inexpensive System-on-a-Chip (SoC) called the ESP8266.

-   The ESP8266 contains all crucial elements of the fashionable computer: CPU, RAM, networking (wifi), and even a contemporary OS and SDK.

-   When purchased at bulk, the ESP8266 chip costs only $2 USD a bit. That makes it a superb choice for IoT projects of all types.

3.2 Multiple Choice Question for Online Exam

Q. 1 How many types of arduinos do we have?

a) 5   b) 6
c) 8   d) 6

Ans. : (c)

Q. 2 What is the microcontroller used in Arduino UNO?

a) ATmega328p   b) ATmega2560
c) ATmega32114   d) AT91SAM3x8E

Ans. : (a)

Q. 3 What does p refer to in ATmega328p?

a) Production
b) Pico-Power
c) Power-Pico
d) Programmable on chip

Ans. : (b)

Q. 4 Arduino shields are also called as _____

a) Extra peripherals
b) Add on modules
c) Connectivity modules
d) Another Arduinos

Ans. : (b)

Q. 5 What is the default bootloader of the Arduino UNO?

a) Optiboot bootloader   b) AIR-boot
c) Bare box
d) GAG

Ans. : (a)

Q. 6 Does the level shifter converts the voltage levels between RS-232 and transistor-transistor logic.

a) True   b) False

Ans. : (a)

Q. 7 Which is the software or a programming language used for controlling of Arduino?

a) Assembly Language
b) C Languages
c) JAVA
d) Any Language

Ans. : (d)

Q. 8 Do Arduino provides IDE Environment?

a) True   b) False

Ans. : (a)

Q. 9 Does Raspberry Pi need external hardware?

a) True   b) False

Ans. : (b)

Q. 10 Does RPi have an internal memory?

a) True   b) False

Ans. : (a)

Q. 11 What do we use to connect TV to RPi?

a) Male HDMI
b) Female HDMI
c) Male HDMI and Adapter
d) Female HDMI and Adapter

Ans. : (c)

Q. 12 How power supply is done to RPi?

a) USB connection
b) Internal battery
c) Charger
d) Adapter

Ans. : (a)

Q. 13 What is the Ethernet/LAN cable used in RPi?

a) Cat5   b) Cat5e
c) Cat6   d) RJ45

Ans. : (d)

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   3-28

IoT : Definition and Characteristics of IoT

Q. 14 What is the default user in Debain on Raspberry Pi?

a) Default   b) User

c) Pi   d) Root

Ans. : (c)

Q. 15 What bit processor is used in Pi 3?

a) 64-bit   b) 32-bit

c) 128-bit   d) Both 64 and 32 bit

Ans. : (a)

Q. 16 Which characteristics involve the facility the thing to respond in an intelligent way to a particular situation?

a) Intelligence   b) Connectivity

c) Dynamic Nature   d) Enormous Scale

Ans. : (a)

Q. 17 _____ empowers IoT by bringing together everyday objects.

a) Intelligence

b) Connectivity

c) Dynamic Nature

d) Enormous Scale

Ans. : (b)

Q. 18 The collection of data is achieved with _____ changes.

a) Intelligence

b) Connectivity

c) Dynamic Nature

d) Enormous Scale

Ans. : (c)

Q. 19 _____ Provide the means to create capability that reflects true awareness of the physical world and people.

a) Sensors

b) Heterogeneity

c) Security

d) Connectivity

Ans. : (a)

Q. 20 IoT devices are naturally vulnerable to _____ threats.

a) Sensors   b) Heterogeneity

c) Security   d) Connectivity

Ans. : (c)

Q. 21 Which challenge comes under IoT devices, reliable bidirectional signaling.

a) Signaling

b) Security

c) Presence detection

d) Power consumption

Ans. : (a)

Q. 22 Which challenge comes under securing the information?

a) Signaling

b) Security

c) Presence detection

d) Power consumption

Ans. : (b)

Q. 23 _____ gives an exact, up to the second state of all devices on a network.

a) Signaling

b) Security

c) Presence detection

d) Power consumption

Ans. : (c)

Q. 24 IIoT stands for _____

a) Industrial Internet of Things

b) Internet Internet of Things

c) Intelligence Internet of Things

d) Internal Internet of Things

Ans. : (a)

Q.25 What does design provide?

a) Technology

b) Ecosystem

c) Technology and ecosystem

d) Digital revolution

Ans. : (c)

Q.26 Which possibility automatically communicates with other vehicles?

a) Transportation and logistics

b) Energy and utilities

c) Automotive

d) Connected supply chain

Ans. : (c)

Q.27 Which possibility provides inter connectivity between shop floor and top floor?

a) Transportation and logistics

b) Energy and utilities

c) Plant control flow operation

d) Connected supply chain

Ans. : (c)

Q.28 Which possibility is the highest contributor to cost overhead for manufacturing facilities?

a) Transportation and logistics

b) Energy and utilities

c) Plant control flow operation

d) Energy management and optimization

Ans. : (d)

Q.29 BAN stands for _____

a) Body Area Network

b) Brain Area Network

c) Body Android Network

d) Brain Android Network

Ans. : (a)

Q.30 NFC stands for _____

a) Near Fast Communication

b) Near Field Communication

c) Near Field Customer

d) Near Field Connection

Ans. : (b)

Chapter End

□□

CH

4.1

4.2

4.3

CHAPTER 4

Digital Forensics

▶ 4.1 Introduction to Digital Forensic

- The Digital devices like cell phones, tablets, gaming consoles, laptop and also desktop computers have become indispensable part of the modern society. With the proliferation of these devices in our everyday lives, there is the tendency to use information derived from them for criminal activities.

- A Crimes like fraud, drug trafficking, homicide, hacking, forgery, and also terrorism often involve computers.

- To fight computer crimes, digital forensics (DF) originated in law enforcement, computer security, and also national defense.

- The Law enforcement agencies, financial institutions, and the investment firms are incorporating digital forensics into their infrastructure.

- The Digital forensics is used to help investigate cybercrime or to identify direct evidence of a computer-assisted crime.

- The concept of the digital forensics dates back to late 1990s and early 2000s when it was considered as computer forensics.

- The legal profession, law enforcement, policy makers, the business community, education, and government all have a vested interest in DF.

- The Digital forensics is often used in both criminal law and private investigation. It has been traditionally associated with criminal law. It requires rigorous standards to stand up to cross examination in court.

☞ Advantages of Digital forensics

- Here, are pros/benefits of Digital forensics

- To ensure the integrity of the computer system.

- To produce evidence in the court, which can lead to the punishment of the culprit.

- It helps the companies to capture important information if their computer systems or networks are compromised.

- Efficiently tracks down cybercriminals from anywhere in the world.

- Helps to protect the organization's money and valuable time.

- Allows to extract, process, and interpret the factual evidence, so it proves the cybercriminal action's in the court.

☞ Disadvantages of Digital Forensics

- Here, are major cons / drawbacks of using Digital Forensic

- Digital evidence accepted into court. However, it is must be proved that there is no tampering

- Producing electronic records and storing them is an extremely costly affair

- Legal practitioners must have extensive computer knowledge

- Need to produce authentic and convincing evidence

- If the tool used for digital forensic is not according to specified standards, then in the court of law, the evidence can be disapproved by justice.

- Lack of technical knowledge by the investigating officer might not offer the desired result

✎ 4.1.1 History of Forensic

Forensic science was established as a separate scientific domain during the 1800s and early 1900s. The contributions of this new area of science dramatically changed the effectiveness of law enforcement. A comprehensive overview of the contributions is available in Saferstein (2007), but some notable innovators and milestones are :

- Mathieu Orfila (1787-1853), considered the father of forensic toxicology, published the first scientific text on forensic toxicology in 1814.

- Alphonse Bertillon (1853-1914) developed a method for identification through body measurements and published a system on personal identification in 1879.

- Francis Galton (1822-1911) studied fingerprints as a means of identification and published the book *Finger Prints* in 1892.

Hans Gross (1847-1915) established the principles for the application of science in investigations in several publications, the first one in 1893.

- Alberts S. Osborn (1858-1946) established scientific principles for document examination and published the book *Questioned Documents* in 1910.

- Leone Lattes (1887-1954) studied characteristics of blood types for identification and created a method for the analysis of blood groups in blood stains in 1915.

- Edmond Locard's (1877-1966), recognized worldwide for promoting the scientific method in criminal investigation, established a police laboratory in Lyon in 1910.

4.1.2 Rules of Digital Forensic

The Computer equipment there are some key "rules" to be followed :

- **Rule 1 :** An examination must never be performed on original media.

- **Rule 2 :** A copy is made onto forensically sterile media. The New media must always be used if available.

- **Rule 3 :** The copy of evidence should be an exact, bit-by-bit copy.

- **Rule 4 :** The computer and the data on it must be protected during the acquisition of the media to ensure that the data is not modified.

- **Rule 5 :** The examination must be conducted in such a way as to prevent any modification of the evidence.

- **Rule 6 :** The chain of the custody of all evidence must be clearly maintained to provide an audit log of whom might have accessed the evidence and at what time.

4.1.3 Definition of Digital Forensic

Digital forensics refers to forensic science applied to digital information, whereas a *digital investigation* refers to investigations in the digital domain. We will use the definition from the first Digital Forensics Research Workshop (Digital Forensics Research Workshop, 2001), as defined in Definition 1.6.

☐ **Definition :** Digital Forensics The scientifically derived and proven toward the preservation, collection, identification, analysis, interpr documentation, and presentation of evidence derived from digital sources for purpose of facilitating or furthering reconstruction of events found to be crimin helping to anticipate unauthorized shown to be disruptive to planned operation

- **Other terms, such** as network forensics, forensics, and *Internet forensics*, are often used to specialized fields within digital forensics information technology has become an integral all aspects of society, digital forensics is growing importance. Most legal cases today have an aspe digital forensics, involving for example mobile credit card transactions, email systems, Internet and GPS systems. As many types of digital evid can be volatile and easily manipulated, the preservation of evidence through the use standardized forensic tools and methods has bee essential.

📝 Types of Digital Forensics

Three types of digital forensics are :

- **Disk Forensics :** It deals with extracting data storage media by searching active, modified, or del files.

- **Network Forensics :** It is a sub-branch of dig forensics. It is related to monitoring and analys computer network traffic to collect import information and legal evidence.

- **Wireless Forensics :** It is a division of netw forensics. The main aim of wireless forensics is offers the tools need to collect and analyze the from wireless network traffic.

- **Database Forensics :** It is a branch of digital foren relating to the study and examination of databases their related metadata.

📖 Emerging

Malware
identific
viruses,

Email F
emails,
contacts

Memor
system
form an

Mobil
examin
retriev
and ou

📝 Chall

Here, are n

- The
acces

- Easy

- Lack

- The
mak

- Any
chan

📝 Exa

In r
digital fo

- Inte

- Ind

- Em

- Fra

- Ina
wo

- Fo

- Ba

- Is

Tech-Ne

- **Malware Forensics :** This branch deals with the identification of malicious code, to study their payload, viruses, worms, etc.

- **Email Forensics :** Deals with recovery and analysis of emails, including deleted emails, calendars, and contacts.

- **Memory Forensics :** It deals with collecting data from system memory (system registers, cache, RAM) in raw form and then carving the data from Raw dump.

- **Mobile Phone Forensics :** It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, videos, etc.

☞ Challenges faced by Digital Forensics

Here, are major challenges faced by the Digital Forensic:

- The increase of PC's and extensive use of internet access

- Easy availability of hacking tools

- Lack of physical evidence makes prosecution difficult.

- The large amount of storage space into Terabytes that makes this investigation job difficult.

- Any technological changes require an upgrade or changes to solutions.

☞ Example Uses of Digital Forensics

In recent time, commercial organizations have used digital forensics in following a type of cases :

- Intellectual Property theft

- Industrial espionage

- Employment disputes

- Fraud investigations

- Inappropriate use of the Internet and email in the workplace

- Forgeries related matters

- Bankruptcy investigations

- Issues concern with the regulatory compliance

☜ 4.1.4 Digital Forensics Investigation and its Goal

An investigation is a systematic examination, typically with the purpose of identifying or verifying facts. A key objective during investigations is to identify key facts related to a crime or incident, and a common methodology used in this textbook is referred to as 5WH defined in Definition

☐ **Definition : 5WH** defines the objectives of an investigation as who, where, what, when, why, and how.

The 5WH formula sets the following objectives (Stelfox, 2013) :

- **Who :** Persons involved in the investigation, including suspects, witnesses, and victims

- **Where :** The location of the crime and other relevant locations

- **What :** Description of the facts of the crime in question

- **When :** The time of the crime and other related events

- **Why :** The motivation for the crime and why it happened at a given time

- **How :** How the crime was committed.

☞ Goals

Here are the essential objectives of using Computer forensics :

- It helps to recover, analyze, and preserve computer and related materials in such a manner that it helps the investigation agency to present them as evidence in a court of law.

- It helps to postulate the motive behind the crime and identity of the main culprit.

- Designing procedures at a suspected crime scene which helps you to ensure that the digital evidence obtained is not corrupted.

- Data acquisition and duplication: Recovering deleted files and deleted partitions from digital media to extract the evidence and validate them.

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   4-6

Digital Forensic

- Helps you to identify the evidence quickly, and also allows you to estimate the potential impact of the malicious activity on the victim

- Producing a computer forensic report which offers a complete report on the investigation process.

- Preserving the evidence by following the chain of custody.

▶▶ 4.2   Models of Digital Forensic Investigation

There are a number of process models for digital forensics, which define how forensics examiners should proceed in their quest to gather and understand evidence. While these can vary, most processes follow four basic steps:

- **Collection**, in which digital evidence is acquired. This often involves seizing physical assets, like computers, phones or hard drives; care must be taken to ensure that no data is damaged or lost. Storage media may be copied or imaged at this stage in order to keep the original in a pristine state for reference.

- **Examination**, in which various methods are used to identify and extract data. This step can be divided into preparation, extraction and identification. Important decisions to make at this stage are whether to deal with a system that's *live* (for instance, to power up a seized laptop) or *dead* (for instance, connecting a seized hard drive to a lab computer). Identification means determining whether individual pieces of data are relevant to the case at hand - particularly when warrants are involved, the information examiners are allowed to learn may be limited.

- **Analysis**, in which the data that's been gathered is used to prove (or disprove!) the case being built by examiners. For each relevant data item, examiners will answer the basic questions about it who created it? who edited it? how was it created? when did this all happen? and attempt to determine how it relates to the case.

- **Reporting**, in which the data and analysis are synthesized into a format that can be understood by laypeople. Being able to create such reports is absolutely crucial skill for anyone interested in digital forensics.

☞ Process of Digital forensics

Digital forensics entails the following steps:

- Identification
- Preservation
- Analysis
- Documentation
- Presentation
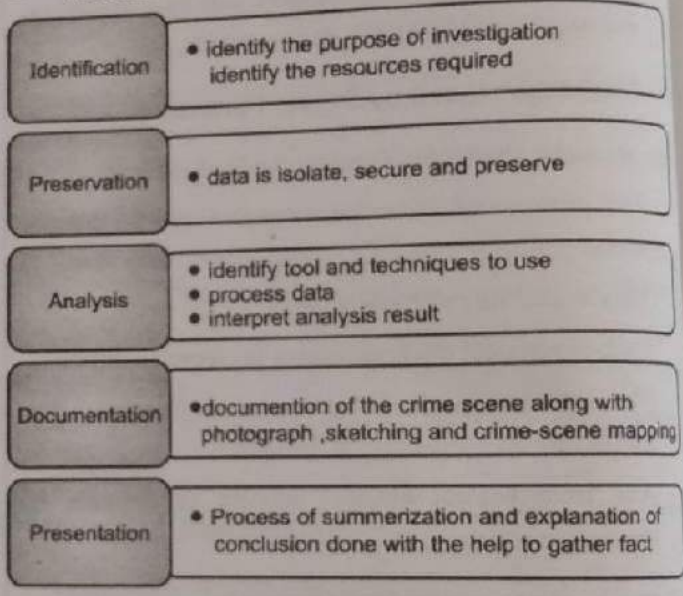
Fig. 4.2.1

Let's study each in detail,

☞ Identification

It is the first step in the forensic process. The identification process mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored (in which format).

Electronic storage media can be personal computers, Mobile phones, PDAs, etc.

☞ Preservation

In this phase, data is isolated, secured, and preserved. It includes preventing people from using the digital device so that digital evidence is not tampered with.

☞ Analysis

In this step, investigation agents reconstruct fragments of data and draw conclusions based on evidence found. However, it might take numerous iterations of examination to support a specific crime theory.

☞ Documentation

In this process, a record of all the visible data must be created. It helps in recreating the crime scene and reviewing it. It Involves proper documentation of the crime scene along with photographing, sketching, and crime-scene mapping.

☞ Presentation

In this last step, the process of summarization and explanation of conclusions is done.

However, it should be written in a layperson's terms using abstracted terminologies. All abstracted terminologies should reference the specific details.

✎ 4.2.1 Digital Forensic Research Workshop Group (DFRWS) Investigative

☞ Model

The research roadmap from Digital Research Workshops proposed in 2001 a general purpose digital forensic framework composed of six main phases:
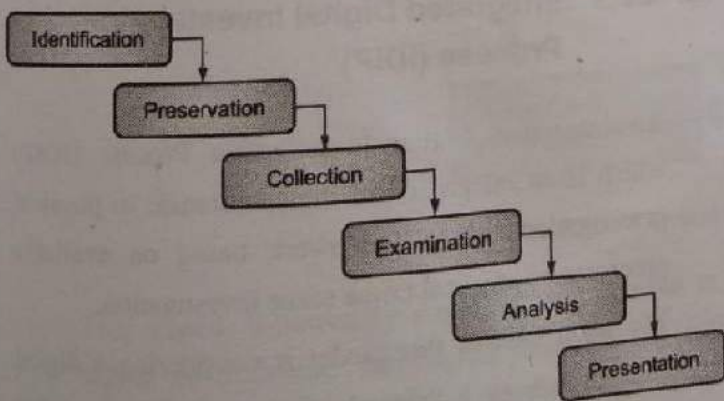
Fig. 4.2.2 : DFRWS Investigative Model

- This model was the base fundament of further enhancement since it was very consistent and

standardized, the phases namely : Identification, Preservation, Collection, Examination, Analysis and Presentation (then a pseudo additional step: Decision). Each phase consists of some candidate techniques or methods.

- The first is Identification and comprises event or crime detection, resolving signature, anomalous detection, system monitoring, audit analysis, etc. Followed by Preservation step in which a proper case management is set, imaging technologies are used, and all measurement are taken to ensure an accurate and acceptable chain of custody, preservation is a guarded principle across all forensic phases.

- Collection comes directly after in which relevant data is collected based on approved methods, software, and hardware; in this step, we make use also of different recovery techniques and lossless compression.

- Following this step are two interesting and very crucial phases, Examination and Analysis, whereby evidence traceability, pattern matching are guaranteed, then hidden data must be discovered and extracted, at this point data mining and timeline are performed. The latest phase of this model is Presentation.

- Tasks related to this step are documentation, clarification, mission impact statement, recommendation and countermeasures are taken and experts testimony.

✎ 4.2.2 Abstract Digital Forensics Model (ADFM)

- As seen DFRWS Investigative Model was meant to be a generic "technology-independent" model, and in 2002 Mark Reith, Clint Carr, and Gregg Gunsch was inspired from DFRWS and presented the Abstract Digital Forensic Model an enhanced model composed of nine phases:

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   4-8
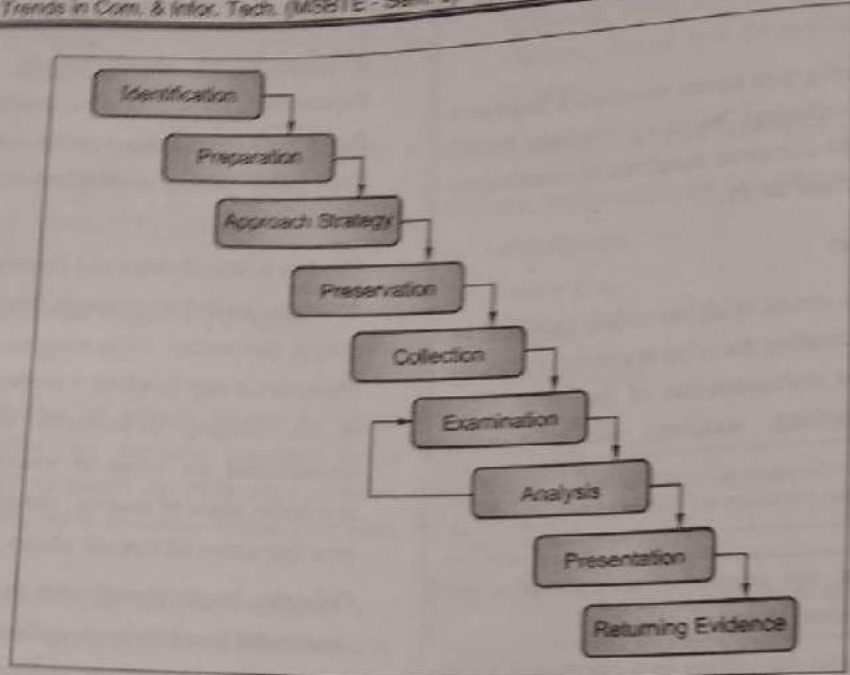
Digital Forensics

Fig. 4.2.3 : Abstract Digital Forensics Model (ADFM)

- As, by this model, the Identification phase assumes that the incident type is well recognized and determined, this is an important step since all upcoming steps depend on it.

- Preparation step, this is the first introduced step where tools, techniques, search warrants, monitoring authorization and management support are prepared, this step is followed by the second introduced step Approach Strategy, this step is meant to maximize the collection of the evidence while minimizing the impact on the victim by formulating different approaches and procedures to follow. In the following phase, Preservation, all acquired data must be isolated and secured to keep them in their actual state.

- All acquired digital evidence is duplicated, and the physical scene is recorded, based on standardized procedures, these tasks are performed under the Collection phase.

- The next phase is Examination whereby an in-depth systemic analysis is conducted to search the evidence relating to the current case. The probative value of the examined evidence is determined in Analysis phase.

- The following step is Presentation where a summary of the process is developed, then comes the third introduced step : Returning Evidence that closes the investigation process by returning physical and digital evidence to the proper owner.

- The most important value that added this model (in contrast with DFRWS Investigative Model) consists of a comprehensive pre and post investigation procedures.

4.2.3 Integrated Digital Investigation Process (IDIP)

- An Integrated Digital Investigation Process (IDIP) which is an integration of digital forensic to physical investigation, it's a framework based on available processes of physical crime scene investigation.

- The main idea of this model is considering a digital crime scene as a "virtual crime scene" and applies adapted crime scene investigation techniques. This model is macroscopically composed of 5 stages consisting microscopically in 17 stages.

- The Fig. 4.2.4 bellow shows the 5 macroscopic stage of IDIP model :
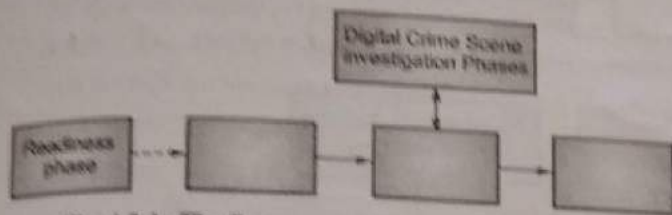
Fig. 4.2.4 : The five macroscopic stage of IDIP model

Physical and Digital crime scenes are processed together and digital forensics are fed into physical investigation.

- The Readiness Phases ensure that human competences and technical infrastructures are able to fully carry the whole investigation process; this stage is subdivided to two phases:

- **Operation Readiness** : involves the preparation of adequate training and equipment for the personnel that will investigate the crime scene.

- **Infrastructure Readiness** : this phase aims to ensure data stability and integrity as long as investigation process takes, this phase may include for example hashing files, securely storing evidence and maintaining a change management database

- The first stage is followed by Deployment phases, the goal of this stage is to provide a mechanism to detect and confirm an incident, and this stage is also subdivided to two phases:

- **Detection and notification:** concretely, this phase triggers the start of the investigation process where incident is detected and appropriate people are notified.

- **Confirmation and Authorization** : once a crime or incident is confirmed, at this phase authorization must be received to fully investigate the-digital- crime scene.

- Physical Crime Scene Investigation phases which come after are when the investigation itself begins with the goal of collecting and analyzing the physical evidence to reconstruct actions that firstly took place. This stage is subdivided to 6 phases that are typical to real cases post-physical crime investigation process and described in the figure below :
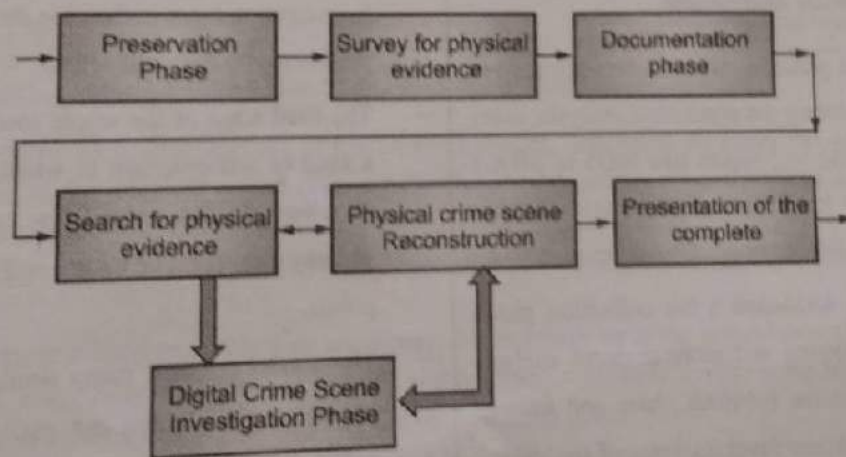
Fig. 4.2.5 : Physical Crime Scene Investigation

- This stage is followed by a quite similar one but in a digital context focusing on digital evidence within a "virtual" digital environment, the Digital Crime Scene Investigation Phases follow the same previously presented path considering any smartphone (or other digital device) a separate crime scene :
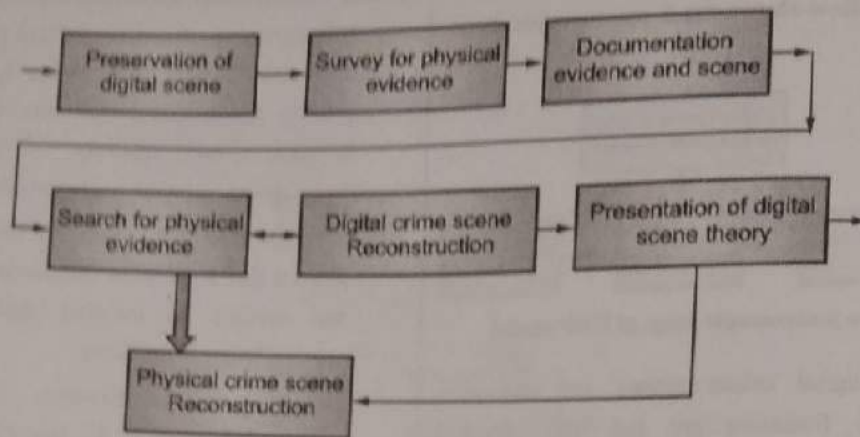
Fig. 4.2.6 : Digital Crime Scene Investigation

Preservation : at this phase, the investigator must pay intention to keeping data integrity, meaning at this level, the digital scene must be secured in order to avoid any external interference that could alter evidence.

Survey for Digital Evidence

Depending on the case being investigated this phase aims to collect the obvious evidence related to that case, and should be occur in a controlled environment (Forensic Lab for instance) using a replica of the original crime scene.

Document Evidence and Scene

- The documentation phase involves documenting every acquired evidence during the conducted analysis, using cryptographic hashing techniques like MD5 or SHA-1 Is recommended to keep trace of evidence integrity. This phase does not substitute the final forensic report.

- **Search for Digital Evidence :** the collection phase involves a deeper digging and more in-depth analysis of what was found in the previous phase and focuses on more specific and low-level analysis of the digital device activities. Deleted file recovering, file carving, reverse engineering and encrypted file analysis are some examples of techniques that could be applied at this stage.

- **Digital Crime Scene Reconstruction :** all digital evidences acquired are put together in order to define

at what point we can trust or reject collected evidence and to determine if further analysis is required and Search for Digital Evidence should be resumed in the case of missing parts of the hole puzzle.

- **Presentation of Digital Scene Theory :** this phase documents and presents the findings to the physical investigation team in the case the investigation was not performed by the same team.

- The final stage of the whole model is Review Phase is a kind of self-criticism in which the whole process is reviewed to determine how well the investigation process went right or wrong and to detect improvement points.

- This model presents many similarities with previously presented models and can easily be considered as an enhanced model of the both, nevertheless IDIP model is way too abstract and the interaction between physical and digital investigations may be in many cases not applicable.

4.2.4 End to End Digital Investigation Process (EEDIP)

By the same year, that is, 2003, Peter Stephenson (Stephenson, P. (2003). A Comprehensive Approach to Digital Incident Investigation.) reviews the DFRWS framework and translated it into a "more" practical investigative process dubbed End-To-End Digital Investigation process (EEDI) by extending the existing process into nine stages; End-to-end because Stephenson in his model considers that "every digital crime has a source point, a destination point and a path between those two points".

The model itself is schematized as follow :
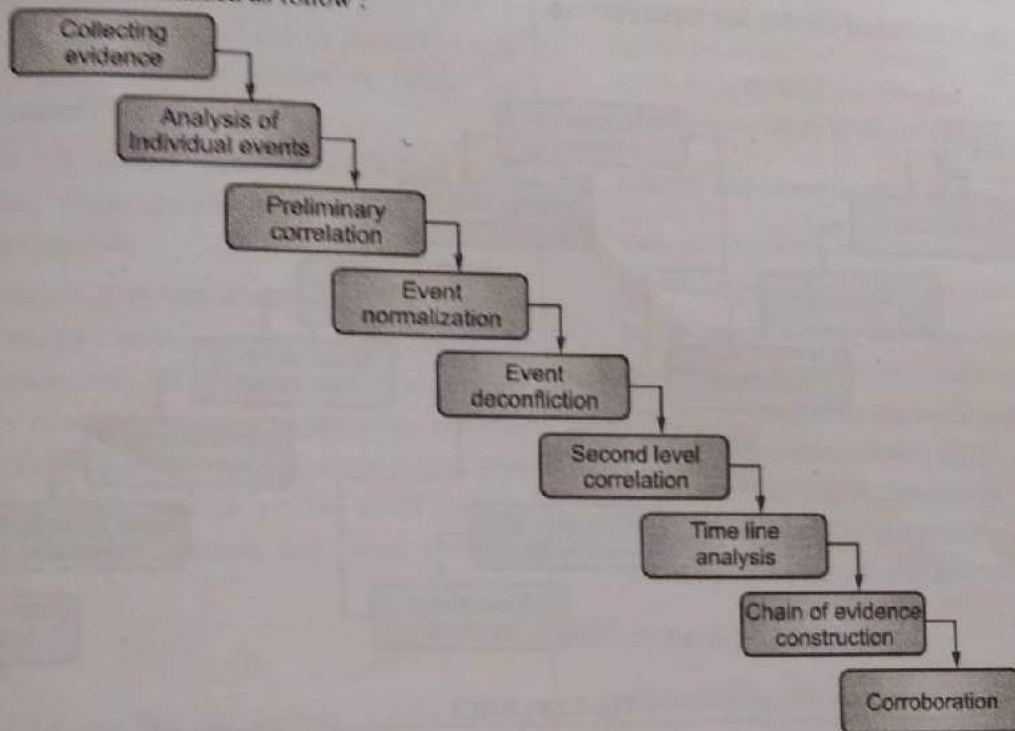
Fig. 4.2.7 : The basic End-to-End Digital Investigation process

- EEDI can be considered as a layer applied to the DFRWS model, depending on cases the whole EEDI process is applied to each class of the DRFWS model (Fig. 4.2.7). This model defines critical steps to do in order to correctly preserve, collect and analyze digital evidence.

- In the phase Collection of Evidence, primary and secondary evidences are collected and taken in their respective contexts.

- The context here is more related to events time sensitivity, which brings us to the second step of this process, Analysis of Individual events, each individual event is isolated and analyzed separately to determine how it can tie with other events and the potential value it can add or they can add to the overall investigation.

- This is followed by Preliminary Correlation step in which individual events are linked with each other to determinate a primary chain of evidence in order to determine what happened, when, and which devices was involved.

- Event Normalization is a step that mainly aims to remove redundancy in evidentiary data assuming that the same events could be reported separately from different sources using multiple vocabularies.

- As an extension to the normalization, whatever how and from where they was reported, the same evidentiary events are combined into one evidentiary event in the Event Deconfliction step; at this stage all events and evidentiary events are refined and a Second-Level Correlation can be performed.

- The previously outlined steps result in timeline which is defined in the Timeline Analysis step, the timeline analysis is an iterative task which lasts as the investigation lasts.

- The Construction of a Chain of Evidence can begin based on the result of timeline of events, theoretically, a coherent chain is developed when each evident will lead to the other and this is what is meant to be done in this step.
- The last phase of this model is Corroboration, where digital investigator support, strengthen and confirm each evidence within the chain of evidence previously developed, with other independent or traditional events and evidence collected in the case of conducted digital forensic investigation is in support of a group of investigators outside the digital forensic unit.

4.2.5 An Extended Model for Cybercrime
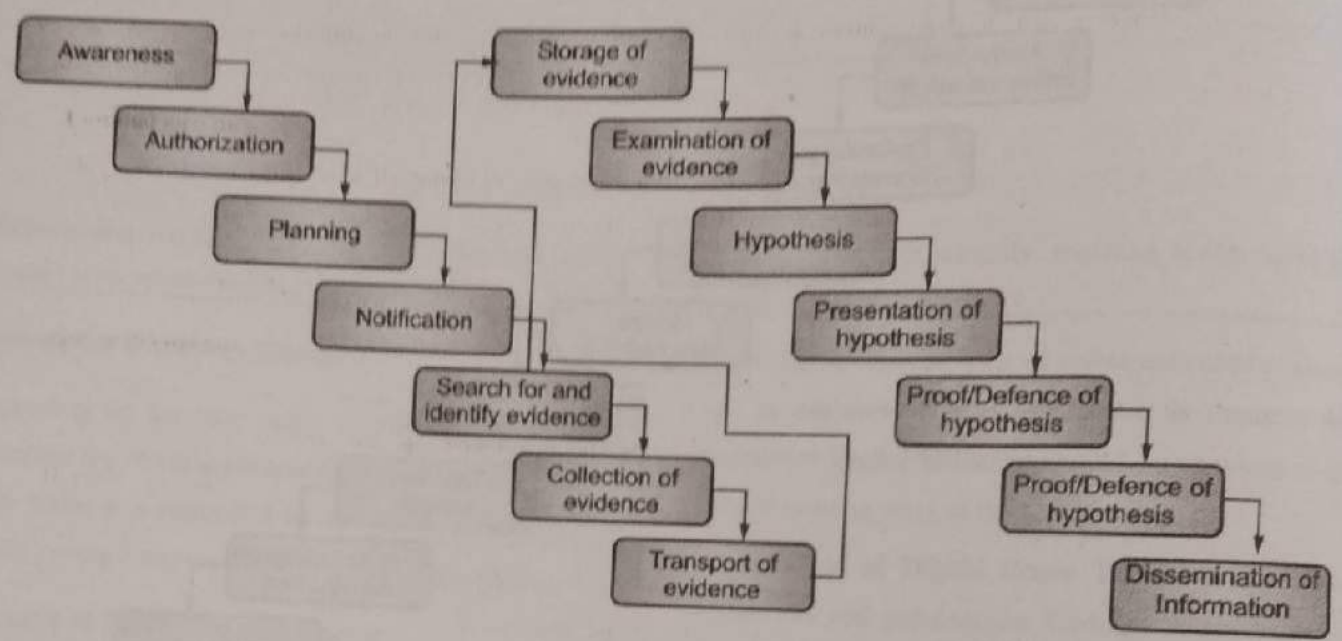
Fig. 4.2.8 : EMCI

- The major information flows during the investigation are also shown in Fig. 4.2.8. Information about the investigation flows from one activity to the next all the way through the investigation process.
- For example, the chain of custody is formed by the list of those who have handled a piece of evidence and must pass from one stage to the next with names being added at each step. There are also flows to/from other parts of the organisation, and to/from external entities.
- The information flows are discussed in more detail below.

Awareness

- The first step in an investigation is the creation of an awareness that investigation is needed. This awareness is typically created by events external to the organisation which will carry out the investigation,

e.g. a crime is reported to the police or an auditor is requested to perform an audit.

- It may also result from internal events, e.g. an intrusion detection system alerts a system administrator that a system's security has been compromised.
- The awareness activity is made explicit in this model because it allows the relationship with the events requiring investigation to be made clear.
- Most earlier models do not explicitly show this activity and so do not include a visible relationship to the causative events.
- This is a weakness of such models because the events causing the investigation may significantly influence the type of investigation required, e.g. an auditor can expect cooperation from a client, whereas a police investigator may not receive cooperation from suspects in an investigation.

It is vital to take into account such differences to ensure that the correct approach is taken to an investigation in a particular context.

Authorisation

- After the need for an investigation is identified, the next activity is to obtain authorisation to carry it out.

- This may be very complex and require interaction with both external and internal entities to obtain the necessary authorisation.

- The level of formal structure associated with authorisation varies considerably, depending on the type of investigation.

- At one extreme, a system administrator may require only a simple verbal approval from company management to carry out a detailed investigation of the company's computer systems; at the other extreme, law enforcement agencies usually require formal legal authorisation setting out in precise detail what is permitted in an investigation (e.g. court orders or warrants).

Planning

- The planning activity is strongly influenced by information from both inside and outside the investigating organisation.

- From outside, the plans will be influenced by regulations and legislation which set the general context of the investigation and which are not under the control of the investigators. There will also be information collected by the investigators from other external sources.

- From within the organisation, there will be the organisation's own strategies, policies, and information about previous investigations.

- The planning activity may give rise to a need to backtrack and obtain further authorisation, for example when the scope of the investigation is found to be larger than the original information showed.

Notification

- Notification in this model refers to informing the subject of an investigation or other concerned parties that the investigation is taking place.

- This activity may not be appropriate in some investigations, e.g. where surprise is needed to prevent destruction of evidence. However, in other types it may be required, or there may be other organisations which must be made aware of the investigation.

Search and Identification of Evidence

- This activity deals with locating the evidence and identifying what it is for the next activity.

- In the simplest case, this may involve finding the computer used by a suspect and confirming that it is the one of interest to the investigators. However, in more complex environments this activity may not be straightforward; e.g. it may require tracing computers through multiple ISPs and possibly in other countries based on knowledge of an IP address.

Collection

- Collection is the activity in which the investigating organisation takes possession of the evidence in a form which can be preserved and analysed, e.g. imaging of hard disks or seizure of entire computers.

- This activity is the focus of most discussion in the literature because of its importance for the rest of the investigation.

- Errors or poor practices at this stage may render the evidence useless, particularly in investigations which are subject to strict legal requirements.

Transport

- Following collection, evidence must be transported to a suitable location for later examination.

- This could be simply the physical transfer of seized computers to a safe location; however, it could also be the transmission of data through networks.

- It is important to ensure during transport that the evidence remains valid for later use, i.e. that the means

Digital Forensics

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   4-14

of transport used does not affect the integrity of the evidence.

☞ Storage

- The collected evidence will in most cases need to be stored because examination cannot take place immediately.

- Storage must take into account the need to preserve the integrity of the evidence.

☞ Examination

- Examination of the evidence will involve the use of a potentially large number of techniques to find and interpret significant data.

- It may require repair of damaged data in ways which preserve its integrity. Depending on the outcomes of the search/identification and collection activities, there may be very large volumes of data to be examined so automated techniques to support the investigator are required.

☞ Hypothesis

- Based on the examination of the evidence, the investigators must construct a hypothesis of what occurred.

- The degree of formality of this hypothesis depends on the type of investigation.

- For example, a police investigation will result in the preparation of a detailed hypothesis with carefully documented supporting material from the examination, suitable for use in court.

- An internal investigation by a company's systems administrator will result in a less formal report to management.

- Backtracking from this activity to the examination activity is to be expected, as the investigators develop a greater understanding of the events which led to the investigation in the first place.

- Presentation The hypothesis must be presented to persons other than the investigators.

- For a police investigation the hypothesis will be placed before a jury, while an internal company investigation will place the hypothesis before management for a decision on action to be taken.

☞ Proof/Defence

- In general the hypothesis will not go unchallenged; a contrary hypothesis and supporting evidence will be placed before a jury, for example.

- The investigators will have to prove the validity of their hypothesis and defend it against criticism and challenge.

- Successful challenges will probably result in backtracking to the earlier stages to obtain and examine more evidence, and construct a better hypothesis.

☞ Dissemination

- The final activity in the model is the dissemination of information from the investigation. Some information may be made available only within the investigating organisation, while other information may be more widely disseminated.

- Policies and procedures will normally be in place which determine the details.

- The information will influence future investigations and may also influence the policies and procedures.

- The collection and maintenance of this information is, therefore, a key aspect of supporting the work of investigators and is likely to be a fruitful area for the development of advanced applications incorporating techniques such as data mining and expert systems.

- An example of the dissemination activity is described by Hauck et al. (2002). They describe a system called Coplink which provides real-time support for law enforcement investigators in the form of an analysis tool based on a large collection of information from previous investigations.

- A further example is described by Harrison et al. (2002). Their prototype system is not real-time, but instead provides an archival function for the experience and knowledge of investigators.

4.2.6 UML Modeling of Digital Forensic process Model (UMDFPM)

4.2.6.1 UML Modelling

- For the purposes of this paper we will be modelling the Kruse and USDOJ DFPMs.

- The two different types of behavioural UML models that are used will be the Activity and Use Case Diagrams. Only a high-level system depiction will be presented in all diagrams.

1 Kruse

- The Kruse model of computer forensics consists of three main processes or phases.

- The first is acquire the evidence while ensuring that the integrity of the data is maintained. Secondly, authenticate the acquired data, while checking the integrity of the extracted data against the original data.

- Authentication in digital forensics is usually done by comparing data of the original MD5 hash with the copied MD5 hash [10].

- Thirdly, analyse the data without tainting the integrity of the data. This process involves the most intense part of the investigation into the Kruse model.

- It is also worth mentioning that the Kruse DFPM is designed specifically for computer-related crimes [3].

- UML Activity Diagram The Kruse DFPM Activity diagram is represented in Figure .
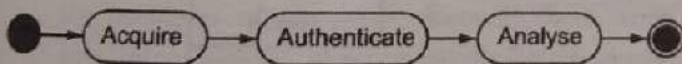
Fig. 4.2.9 : Kruse Activity diagram

- The three processes follow one after the other : Acquire, Authenticate and then Analyse. These processes commence with a starting state and end with a finishing state.

- UML Use Case Diagram The Kruse DFPM Use Case is represented in Figure . This figure also depicts the different role players.

Digital Forensics

- The three main role players that interact with the system are the Investigator, the Prosecution and the Defence.

- The Investigator can be specialised to a First Responder, which can be any one of the following: Emergency Response Team or System Administrator.

- The Prosecution and the Defence will be role players in a criminal matter only. The system consists of three :
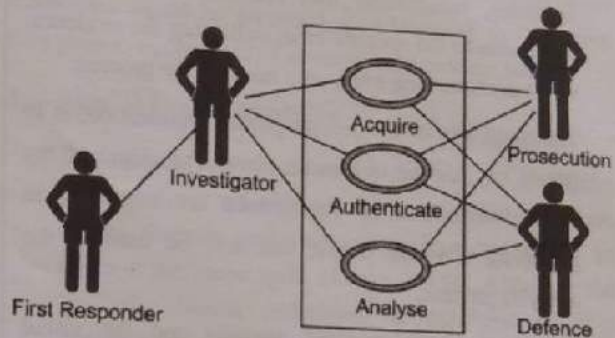
Fig. 4.2.10 : Kruse Use Case Diagram

- Use Cases : Acquire, Authenticate and Analyse. The system boundary is depicted by the large rectangle containing the three use cases.

- 3 Comments on Kruse DFPM It should be noted that this is truly an over simplification of the Kruse DFPM. Each of the use cases in Figure and the activity diagram in above Figure will be expanded to include sub process.

- The activity diagram is clear and it is obvious to see that an investigation starts, runs its course and stops. The main concern is that no real evidence document or report is generated during the investigation.

- The Kruse DFPM however states in its specification that documentation and chain-of-custody reports should be maintained during each of the processes.

- The use case clearly indicates that the investigator will interact with each one of the processes. Kruse states that in many instances the investigator will not be the same person.

- The 'Acquire' activity is always encountered by the First Responder and the other two use cases can be performed in a laboratory environment.

- The court is mentioned throughout the specification, but there is no clear interaction with the system.

4.2.6.2   United States Department of Justice (USDOJ)

- The USDOJ [4] model accounts for four phases namely collection, examination, analysis and report. The collection phase involves searching for the evidence, recognising that the evidence would be applicable to the specific case, collecting the evidence, while documenting every step taken in the process.

- The main aim of the second phase, examination, is to reveal any hidden or obscure data. The origin of the original data and its significance are important in providing a visual output that will be used in the analysis process.

- The third phase involves analysis and the visual product of the examination process is the input to this analysis. Here a case will be built and evidence will be constructed to prove the particular crime. Baryamureeba [?] states that the analysis phase will also determine the probative value, which would actually be the function of the courts.

- The outcome of this phase would be to produce evidence that would serve to prove the elements of a specific crime. Every step is also documented throughout. The final phase in the USDOJ model is the report phase. During this phase a complete report will be compiled to document the process followed from the beginning of the investigation. The product will be the final evidence report presented in court.

- Contained in this document is the chain-of-custody report, complete investigation documentation and presentable evidence. One of the design principles in the USDOJ DFPM is to abstract the process from any specific technology [4].

1.   UML Activity Diagram UML

- Activity Diagram The Activity Diagram of the USDOJ DFPM is given in Fig. 4.2.11.
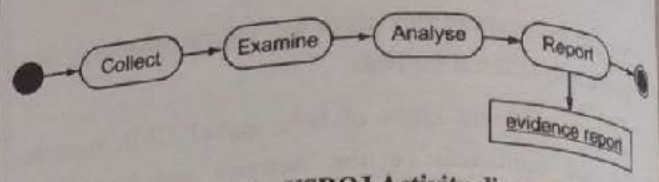
Fig. 4.2.11 : USDOJ Activity diagram

- The process commences with a starting state. The data is collected from the digital device, after which it is examined and then analysed. During the report phase, an evidence report is created as an object output. After the completion of the evidence report, the process stops.

2.   UML Use Case Diagram

- The Use Case diagram of the USDOJ DFPM can be seen in Fig. 4.2.12.
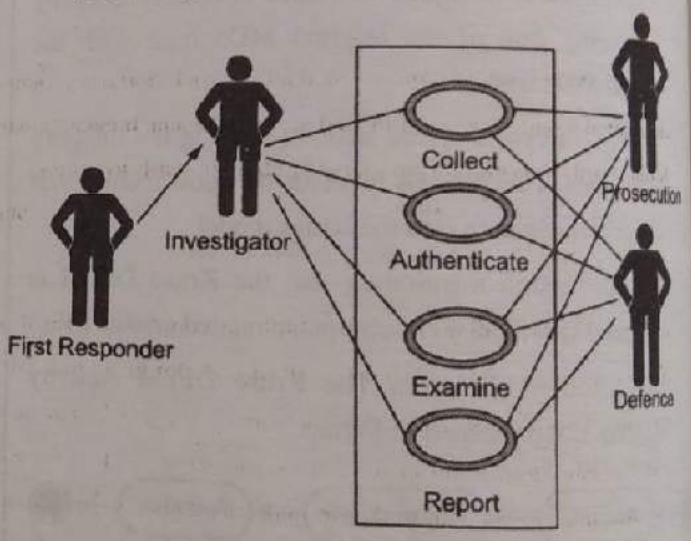
Fig. 4.2.12 : USDOJ Use Case Diagram

- In Fig. 4.2.12 there are three actors: the Investigator, the Prosecution and the Defence. The First Responder is a specialisation of Investigator. An Investigator can be any one of the following : police officer, manager or a forensic investigator.

- The DFPM is specifically set up for First Responders. There are four use cases in the system, namely, Collection, Examination, Analysis and Reporting.

3. Comments on the USDOJ DFPM

In the USDOJ Activity diagram, the processes are executed one after the other. There is one apparent difference, which involves the fact that during the Reporting process an evidence report is generated as an output. This will ultimately be used in a matter before the court.

The evidence report will contain all the evidence collected during the investigation, including the chain-of-custody document and presentable evidence. It should be noted that the current paper will not consider what a court considers to be presentable evidence.

The Use Case diagram in Figure does not show the court as a role player that interacts with the system.

In the USDOJ specification the court is often mentioned, but no emphasis is placed on the fact that the court ultimately will evaluate the presented evidence report in its finding. There is also no clear indication as to how and when the court must evaluate the document. Nevertheless, an important contribution by the USDOJ DFPM is the fact that an evidence report document is in fact produced.

4. Comparison between the two Dfpms

- Similarities between the Kruse and USDOJ DFPMs are apparent: Firstly, although the models use different terminology ('Acquire' and 'Collect') to describe the first phase, the processes are actually the same.

- For our purposes we will refer to both as 'Collect' in the remainder of the paper. Secondly, both models have an 'Analysis' phase, resulting in an Analyse process.

- There are however also a number of significant difference that cannot be ignored.

- These include the fact that Kruse's DFPM explicitly validates the integrity of the data in an authentication process, while the USDOJ DFPM includes an examination process.

- The latter might not always be needed, as data is often hidden and obscured from an investigator.

This process will also compromise the integrity of the data. Finally, the DFPM of the USDOJ includes the compilation of a report process, while the Kruse DFPM does not.

▶▶ 4.3 Ethical Issues in Digital Forensic

Current issues arising from the development and implementation of digital forensic systems that are unaddressed are highlighted, with the expectation that future researches would be focussed on addressing the concerns they pose to the welfare of an automated modern society.

1. Fear of Unpredictability

- Due to the complexities in the nature of digital artefacts from which evidences are gathered, various digital forensic tools exploit various techniques to perform the same tasks (Casey, 2009). Although the use of different techniques is adjudged to help investigators to keep up with containing new ways of misusing information systems efficiently (Volonino et al., 2007), it becomes confusing to users which computing behaviours are deemed inappropriate by which digital forensic tools.

- The resultant fear tends to influence the computing activities of users, as they become conservative rather than expressive (Kubitschke, 2009).

- This can affect the quality of feedbacks being supplied by the users to the system, and the accuracy of the system in detecting trends of computer usage is impaired.

2. Breach of Privacy

- The recommendation that disk manufacturers should provide backdoors to aid investigators to bypass lockouts and ensure effective digital forensic analyses has gained proponents who has argued for its commercial implementation (Balogun & Zhu, 2013).

- In the same vein, digital forensic systems employ backdoor entry techniques to user devices for collection of potential evidential data.

- The potential access these techniques grant to a certain group – supposedly law enforcement – to individual / organization's non-public information poses a serious moral concern.

- In addition to that, there is a genuine possibility that such techniques would find their way into the wrong hands, who would breach the confidentialities attached in infringing and embarrassing manners.

3. Exploitation of Tools

- The functionality of digital forensic systems are unique and straightforward. However, experienced computer users with certain skill sets can reverse engineer or extend modules of a digital forensic system - especially open source systems that grant such permissions - for personal use (Fitzgerald, 2006); (Ridder, 2009).

- These tools are even used to frustrate their own effectiveness in anti-forensic moves, thus discrediting the information they produce as results.

- Thus, questions arise about how open source digital forensic systems can be prevented from being exploited for unethical use, and how their exploited implementation instances could be detected.

- Other concerns arise about the open licence nature of some digital forensic systems, and whether it is more secure to make all digital forensic systems proprietary to inhibit immoral exploitations.

4. Commercial and Market Share Motives

- The digital forensic system market is not as competitive as the typical information system market. Unlike the latter, the earliest developers in the former market have acquired and still retain the majority of the market share.

- This could be attributed to the relative immaturity of the digital forensics discipline, and the fact that such developer reputations earned from the legal systems serve as precedents that do not change very often (Casey, 2009). Yet, digital forensic system developers show virtually no proof to the claims about the accuracy and reliability of their systems.

- Investigators take these claims at face value, and tend to prefer the earliest developers due to their reputations. However, the possibility that these revered developers hype their systems more than their actual

capabilities, in the bid to retain or acquire larger share of the market, exists (Balogun & Zuva, 2017).

- It also hinders the market share index and implementation of more efficient digital forensic systems and discourages better digital forensic investigation process in the long run.

5. Standardization of Practices

- The difference in the nature of practice, in which information system practices are more straightforward than the practices in the digital forensic domain, is a persistent issue worth mentioning.

- Users of digital forensic systems always rely on experience and creativity in setting up procedures to complete tasks, whereas typical information system users use clearly set out procedures (Casey, 2009).

- Though standardization of digital forensic system implementation has been attempted and revisited often, its actualization has been elusive (Garfinkel, 2010).

- Thus, it remains unclear how to determine whether all procedural variations of digital forensic system practices are effective, or which among them is the most efficient for recommendation as a standard.

6. Inconsistent Educational/Training Outcomes

- As mentioned in the previous section, the use of digital forensic systems require prerequisite specialized skills.

- These skills are not acquirable from general computing education which are usually enough to use typical information systems.

- They are imparted through specific education or training over a period of time by academic universities and professional organizations, in formal and informal modes.

🔲 4.3.1 General Ethical Norms For Investigators

No single organization offers a definitive code of ethics for forensics examiners. To form their ethical standards, the organizations look at the standards of other organizations. The ethical guidelines of organizations can have a great impact on expert's testimony.

☞ International Society of Forensics Computer Examiners (ISFCE)

The ISFCE's professional responsibility and code of ethics provides its members solid guidelines on how they should perform their duties as computer forensics analysts. As responsible investigators, computer forensics analysts must adhere to the guidelines that include particular instructions on how they should maintain their professional standing. The instructions in ISFCE's code of ethics include:

- In all forensic examinations, the investigator should maintain the greatest objectivity and present accurate findings.

- All matters should be testified to truthfully before the court.

- The examiner shouldn't take any action that would appear to be a conflict of interest later on.

- Examinations must be based on well-established and validated principles.

- The examiner is forbidden to reveal any confidential information without the client's permission or a court order.

- The investigator is not allowed to misrepresent credentials or associated memberships.

In addition, ISFCE encourages members to report violations by other members. ISFCE also offers a certified computer examiner (CCE) certification. The CCE-certified must comply with the ISFCE's ethical principles.

☞ High Technology Crime Investigation Association (HTCIA)

For its members, the HTCIA provides ethical standards, namely, its "Code of Ethics of Professional Standards Conduct." The HTCIA's core principles related to testifying include:

- HTCIA members use specialized techniques and advanced technologies to uncover the "truth" so as to avoid wrongful conviction.

- The HTCIA values its members' integrity and the truth they reveal through computer forensics best practices, involving effective techniques used to collect digital evidence.

☞ International Association of Computer Investigative Specialists (IACIS)

The IACIS provides a clear guide for ethical behavior of computer forensics investigators. In fact, these guidelines follow the principles defined by other professional organizations. The guidelines for IACIS's members that apply to testifying include:

- Members should maintain the utmost objectivity in all forensics investigations and present the facts accurately.

- The evidence should be examined and analyzed thoroughly.

- Only unbiased opinions should be given.

- Members must not conceal any findings that would cause the facts of a case to be distorted or misrepresented.

☜ 4.3.2 Unethical Norms for Investigation

Unethical practices manifest in investigation depending on the types of investigation.

(i) In an investigation on behalf of an individual or a firm proposing to buy a business, the accountant could collude with the vendor to manipulate records, inflate asset values, depress liabilities and inflate revenues in the years during which the proposed sale is contemplated.

Also stock may be overstate by double counting of certain items, over valuation and inflation due to manipulation of cut-off procedures. A case in point in Nigeria was the Sadiq Petroleum Limited in the African Petroleum deal. Sadiq Petroleum limited had emerged as the core investor in the privatization of the Federal government investment in the African Petroleum Limited. On taking over African Petroleum after regulations and purchase. It was discovered that AP had over N20 billion debt over hand which was creatively concealed and unreported by the investigating accountants who carried out the diligence on the company.

(ii) In the investigation on behalf of a bank for the purpose of credit, the bank requires more detailed information

and an accountant is called to carry out investigations for this purpose. Bankers are interested in knowing the reason for the required loan as they are careful to see that in such cases, the money is usually employed. Furthermore, they wish to know the extent to which the customer is liquid.

The accountant's investigation will therefore centre, on the verification of assets and liabilities, ascertaining the financial strength of the business, if the client who is seeking the loan does not prepare a regular budget, the investigating accountant will be well advised to offer assistance to the client in preparing a cash forecast showing how the loan is expected to be repaid. In the course of carrying out his duties, the investigating accountant engages to unethical practices by window dressing the financial statements of the client to be presented to the banker. For example, the cash flow statements of the client to be presented to the banker. For example, the cash flow statement can be window-dressed in order for the client to appear financially healthy before the banker.

(iii) When the information obtained in the course of the investigating assignment is used for personal gain by the professional accountants or the privileged information is disclosed to third parties without proper and specific authority. iv. Presenting a report that contains information that is materially false or misleading and prepared without proper care or consideration for its accuracy. v. When the professional accountant fails to write and agree with the content of the engagement letter with the client before commencing the assignment. vi. Where the professional fees is based on the value of the discovery in the course of the investigating assignment.

(iv) When the professional accountant accepts gift, goods and services from the management of the client or one of the client's staff is a close relative of the professional accountant.

☞ Causes of Unethical Practices in Investigation

The various forms of unethical practices that the investigating accountant perpetuates amount to corruption.

Corruption can be defined as all those improper actions or transaction aimed at changing the normal causes of events, a judgment and position of trust. sees corruption as any act undertaken with the deliberate intent of deriving or extracting monetary or other benefits by encouraging or conniving at illegal benefits. Various reasons have been adduced for corrupt practices which invariably can be linked to why professional accountants engage in unethical practices. They include the following among other.

i. **Greed :** People get involved in corruption because they are just never satisfied with what they have. The rich want to get richer Unethical Practices in Investigation: The Need for Reinforcement of Ethical Codes and Values.

ii. **Poverty :** Another reason people get involved in corruption is poverty. Nigeria which is a developing economy is faced with the problem of poverty. No one wants to be poor and so everyone struggles to get out of poverty either by hook or crook, even if it means getting involved in corruption.

iii. **Most people especially the youth today lack patience :** they want to get rich as quickly as possible. Most youth also lack hard work, always depending on their father's wealth. People want to make ends meet, but are not willing to do it the right way. This leads them to get involved in corruption such as stealing, accepting of bribes, falsification of records, documents and so on.

iv. **Weak law enforcement system :** The weak law enforcement system has encouraged a lot of people including the accountants to involve themselves in corruption, hoping to get the law on their side by paying for it or working for people who can buy the law and rescue them.

v. Lack of standards to control investigation quality

vi. Failure to offer education relating to ethics in the accounting curricula

▶▶ 4.4 Multiple Choice Questions for Online Exam

☞ Section 4.1

Q. 1 The Digital forensics is often used in both _____.

a. criminal law and private investigation.

b. cyber law and private investigation

c. public law and public investigation

d. none of the above

Ans. : (a)

Q. 2 A(n) _____ is a document that lets you know what questions to expect when you are testifying.

a. written report

b. affidavit

c. examination plan

d. subpoena

Ans. : (c)

Q. 3 _____ refers to forensic science applied to digital information

a. cyber forensics

b. Digital forensics

c. multimedia forensics

d. network forensics

Ans. : (b)

Q. 4 It is a sub-branch of digital forensics. It is related to monitoring and analysis of computer network traffic to collect important information and legal evidence.

a. Network Forensics b. Wireless Forensics

c. Malware Forensics d. Database Forensics

Ans. : (a)

Q. 5 It mainly deals with the examination and analysis of mobile devices. It helps to retrieve phone and SIM contacts, call logs, incoming, and outgoing SMS/MMS, Audio, Videos, etc.

a. Network Forensics

b. Wireless Forensics

c. Mobile Phone Forensics

d. Database Forensics

Ans. : c

Q. 6 An investigation is a _____, typically with the purpose of identifying or verifying facts.

a. information examination.

b. systematic examination

c. network examination

d. data examination

Ans. : (b)

☞ Section 4.2

Q. 7 _____ in which digital evidence is acquired.

a. Collection, b. Examination

c. Analysis d. reporting

Ans. : a

Q. 8 _____, in which various methods are used to identify and extract data.

a. Collection, b. Examination

c. Analysis d. reporting

Ans. : (b)

Q. 9 _____ in which the data and analysis are synthesized into a format that can be understood by laypeople.

a. Collection, b. Examination

c. Analysis d. reporting

Ans. : (b)

Digital Forensics

🔲 Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   4-22

Q. 10 The _____ mainly includes things like what evidence is present, where it is stored, and lastly, how it is stored

   a. identification process

   b. Preservation process

   c. documentation process

   d. analysis

  Ans. : (a)

Q. 11 _____ the process of summarization and explanation of conclusions is done.

   a. presentation

   b. Preservation process

   c. documentation process

   d. analysis

  Ans. : (a)

Q. 12 _____ Investigative Model was meant to be a generic "technology-independent" model.

   a. ADFM

   b. IDIP

   c. DFRWS

  Ans. : (c)

Q. 13 _____ involves the preparation of adequate training and equipment for the personnel that will investigate the crime scene.

   a. Operation Readiness

   b. Infrastructure Readiness

   c. Detection and notification

   d. Confirmation and Authorization

  Ans. : (a)

Q. 14 _____ concretely, this phase triggers the start of the investigation process where incident is detected and appropriate people are notified.

   a. Operation Readiness

   b. Infrastructure Readiness

   c. Detection and notification

   d. Confirmation and Authorization

  Ans. : (c)

Q. 15 _____ at this phase, the investigator must pay intention to keeping data integrity.

   a. preservation:

   b. survey for digital evidence

   c. digital crime scene reconstruction

   d. none of the above

  Ans. : (a)

Q. 16 In the phase _____, primary and secondary evidences are collected and taken in their respective contexts

   a. Analysis of Individual events

   b. Preliminary Correlation

   c. Event Normalization

   d. Collection of Evidence

  Ans. : (d)

Q. 17 _____ step; at this stage all events and evidentiary events are refined.

   a. Event Deconfliction

   b. Timeline analysis

   c. Event normalization

   d. Corroboration

  Ans. : (a)

Q. 18 The first step in an investigation is the creation of _____ that investigation is needed.

a. causing

b. an awareness

c. identification

d. none of the above

Ans. : (b)

Q. 19 _____ is the activity in which the investigating organisation takes possession of the evidence in a form which can be preserved and analysed, e.g. imaging of hard disks or seizure of entire computers.

a. Collection   b. Transport

c. Notification   d. None of the above

Ans. : (a)

Q. 20 The _____ accounts for four phases namely collection, examination, analysis and report.

a. USDOJ model   b. Kruse model

c. DFPM model   d. none

Ans. : (a)

Q. 21 ISFCE stands for

a. Interconnected Society of Forensics Computer Examiners

b. Intercommunicated Society of Forensics Computer Examiners

c. International Society of Forensics Computer Examiners

d. Investigation Society of Forensics Computer Examiners

Ans. : (c)

Q. 22 HTCIA for stands for   Digital Forensics

a. High Terminal Crime Investigation Association

b. High Technology Crime Investigation Association

c. High-Tech Crime Investigation Association

d. High Testify Crime Investigation Association

Ans. : (b)

Q. 23 IACIS stands for

a. International Access of Computer Investigative Specialists

b. International Analysis of Computer Investigative Specialists

c. International Association of Computer Investigative Specialists

d. International Accountant of Computer Investigative Specialists

Ans. : (c)

Q. 24 The guidelines for IACIS's members that apply to testifying include : find out the wrong one :

a. Members should maintain the utmost objectivity in all forensics investigations and present the facts accurately.

b. The evidence should be examined and analyzed thoroughly.

c. Only unbiased opinions should be given.

d. All are correct

Ans. : (d)

Chapter Ends...

□□□

CHAPTER 5

Digital Evidence

☞ 5.7 Multiple Choice Questions for Online Exam

• Chapter Ends...

Digital Evidence

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6) 5-3

▶▶ 5.1   Digital Evidences

- The field of computer security includes events that provide a successful forensic experience, which is worthwhile and satisfying.

- Investigations into computer security incidents can lead to legal proceedings, such as court proceedings, in which digital evidence and documents obtained are likely to be used as evidence in trials.

- It is a science of finding evidence from digital media like a computer, mobile phone, server, or network.

- It provides the forensic team with the best techniques and tools to solve complicated digital-related cases.

- Digital Forensics helps the forensic team to analyses, inspect, identifies, and preserve the digital evidence residing on various types of electronic devices.

- In the past few years, a new category of crime scenes has become more common, that is, crimes committed in the electronic or digital domain, especially in cyberspace.

- Criminal justice agencies around the world increasingly need to investigate some or all crimes committed through the Internet or other electronic media.

- Resources and procedures are needed to effectively search, find and save all types of electronic evidence.

- The evidence ranges from child pornography to encrypted data used to further various criminal activities.

- Even in investigations that are not primarily electronic in nature, computer files or data may be found at some point in the investigation and require further analysis.

- Digital evidence can be used in a wide range of criminal investigations, including homicides, sexual crimes, missing persons, child abuse, drug dealing, fraud and theft of personal information.

- In addition, civil cases can rely on digital evidence, and electronic discovery is becoming a routine part of civil disputes.

- Computer records can help determine when the incident occurred, where the victims and suspects were located, and with whom they communicated, and even show the criminal intentions of the suspects.

- Digital data is ubiquitous and should be collected regularly in any survey.

- People involved in crime are likely to operate computers, use mobile devices, or access the Internet.

- Therefore, every company survey should consider relevant information stored on computer systems used by employees at work and at home.

- Each search warrant should include digital evidence to avoid the need for a second search warrant and related lost opportunities.

- Even though digital data cannot establish a link between crime and crime victims or crime and crime offenders, they can play a role in investigations.

- Digital evidence can reveal criminal behaviour, provide investigative clues, oppose or support witness testimony, and identify possible criminal suspects.

📖 5.1.1   Definition of Digital Evidence

- In any court case, the parties must produce evidence in support of their case whether that is the claimant/prosecution or the defence.

- Without supporting evidence, the claim/prosecution or defence is highly likely to fail.

- Digital evidence is defined as any data that is stored or transmitted using a computer, supports or disproves the theory of how a crime occurred, or addresses key elements of crime (such as proof of intent or absence).

- The use of digital evidence has increased in the past few decades as courts have allowed the use of e-mails, digital photographs,

- ATM transaction logs, word processing documents, instant message histories, files saved from accounting programs, spreadsheets, internet browser histories, databases, the contents of computer memory, computer backups, computer printouts, Global Positioning

System tracks, logs from a hotel's electronic door locks, and digital video or audio files.

5.1.2 Best Evidence Rule

The best evidence rule, which had been established to deter any alteration of evidence, either intentionally or unintentionally, states that the court prefers the original evidence at the trial rather than a copy, but will accept a duplicate under these conditions :

- The original was lost or destroyed by fire, flood, or other acts of God. This has included such things as careless employees or cleaning staff.

- The original was destroyed in the normal course of business.

- The original is in possession of a third party who is beyond the court's subpoena power.

- This rule has been relaxed to allow duplicates unless there is a genuine question as to the original's authenticity, or admission of the duplicate would, under the circumstances, be unfair.

5.1.3 Original Evidence

- Evidence of a statement made by someone other than a witness to prove that the statement was actually made, not its authenticity.

- Therefore, if a witness testified in a defamation lawsuit that he heard the defendant defame the claimant, his testimony is the original evidence.

- Occasionally, procedures or situations are used to put the situation outside the control of the client / victim.

- We also assume that cases with due diligence or those with long-term efforts will eventually be dealt with through judicial procedures and we will deal with the evidence accordingly.

- Where criminal or civil litigation is possible, we usually constantly urge the client or victim to let us hand over all of the original evidence because we have a phased process of evidence processing.

5.2 Rules of Digital Evidence

In both civil and criminal cases, five general rules are used to weigh the value of evidence. These five rules are :

- **Admissible**
  o Evidence must have been preserved and gathered in such a way that it can be used in court.
  o Many different errors can be made that could cause a judge to rule a piece of evidence as inadmissible.
  o These can include failure to obtain a proper warrant, breaking the chain of evidence, and mishandling or even destroying the evidence.

- **Authentic**
  o The evidence must be relevant to the case, and the forensic examiner must be able to account for the origin of the evidence.
  o For example, intercepting an email transmission is not enough to prove that the alleged sender was responsible for the message.
  o A relationship must be established between the message and the computer it was sent from.
  o It will also need to be established, beyond reasonable doubt, that there was a relationship between the computer, the message, and the person who sent the message.

- **Complete**
  o When evidence is presented, it must tell the whole story. A clear and complete picture must be presented that can account for how the evidence came to be.
  o If unchecked, incomplete evidence may go unnoticed, which can be even more dangerous than no evidence at all.
  o As a recent example, consider the case of a man who was charged with possession of child pornography.

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6) 5-5

Digital Evidence

o The evidence presented showed that the images had been downloaded onto the man's work computer, but it wasn't until much later in the case that the defense revealed that the images had been downloaded by a virus on the machine, and not by the defendant.

o An innocent man was almost convicted and put in prison because the prosecution's examiner did not present complete evidence and a jury is not technically savvy enough to see this.

o With all of the different processes running on a computer, it's critical to be able to tie a piece of evidence to its origins and tell the whole story.

- **Reliable**

o Any evidence collected must be reliable. This depends on the methodology and science used.

o The techniques used must be credible and generally accepted in the field.

o If the examiner made any errors or used questionable techniques, this could cast reasonable doubt on a case.

- **Understandable and believable**

o A forensic examiner must be able to explain, with clarity and conciseness, what processes he used and how the integrity of the evidence was preserved.

o If the examiner does not appear to understand his own work, a jury may reject it as well.

o The evidence must be easily explainable and believable.

▶▶ 5.3 Characteristics of Digital Evidence

Following are essential characteristics of a digital evidence:

Admissibility : It must be in conformity with common law and legislative rules. There must be relationship between the evidence and the fact being proved. Digital evidence is often ruled inadmissible by courts because it was obtained without authorization.

In most jurisdictions a warrant is required to seize and investigate digital devices. In a digital investigation this can present problems where, for example, evidence of other crimes are identified while investigating another.

- **Reliability** : The evidence must be from indisputed origin.

- **Completeness** : The evidence should prove the culprit's actions and help to reach a conclusion.

- **Convincing to Judges** : The evidence must be convincing and understandable by the judges.

- **Authentication** : The evidence must be real and related to the incident. Courts largely concerned themselves with the reliability of such digital evidence. The investigator must be able to prove to the authenticity of the digital evidence by explaining: o the reliability of the computer equipment.

o The manner in which the basic data was initially entered.

o The measures taken to ensure the accuracy of the data as entered. o the method of storing the data and the precautions taken to prevent its loss.

o The reliability of the computer programs used to process the data, and o the measures taken to verify the accuracy of the program.

⌖ 5.3.1 Locard's Exchange Principle

- The value of trace (or contact) forensic evidence was first recognized by Edmund Locard's in 1910. He was the director of the very first crime laboratory in existence, located in Lyon, France.

- The Locard's Exchange Principle states that "with contact between two items, there will be an exchange".

- For example, burglars will leave traces of their presence behind and will also take traces with them.

- They may leave hairs from their body or fibers from their clothing behind and they may take carpet fibers away with them.

- Paul L. Kirk expressed the principle as follows : "Wherever a criminal steps, whatever he touches,

whatever he leaves, even unconsciously, will serve as a silent witness against him.

Not only his fingerprints or his footprints, but his hair, the fibers from his clothes, the glass he breaks, the tool mark he leaves, the paint he scratches, the blood or semen he deposits or collects.

All of these and more, bear mute witness against him. This is evidence that does not forget. It is not confused by the excitement of the moment.

It is not absent because human witnesses are. It is factual evidence. Physical evidence cannot be wrong, it cannot perjure itself, it cannot be wholly absent. Only human failure to find it, study and understand it, can diminish its value."

- Digital evidence is usually not in a format that is directly readable by human.

- Therefore it requires some additional steps to convert it into a human readable form in the form of writing. Digital evidences must follow the requirements of the Best Evidence Rule.

5.3.2 Digital Stream of Bits

- Fred Cohen mentioned that digital evidence is the only sequence of bits that can be arranged in an array to display information.

- The focus will be on the bits, not the media that contains, transmits or processes them, or the basic physical characteristics of the media.

- Consecutive bits of information are rarely meaningful, and tools are needed to logically display these structures for readability.

- Finding digital evidence also helps inspectors conduct inspections during inspections. Metadata is used to describe data more specifically and to help determine the context of digital evidence.

- A bit-stream image is a sector-by-sector / bit-by-bit copy of a hard drive.

- A bit-stream image is actually a set of files that can be used to create an exact copy of a hard drive, preserving all latent data in addition to the files and directory structures.

Digital Evidence

- A bit-stream image can be read by the majority of the tools used by the Computer Forensics Examiner to analyse the hard drive such as Encase, FTK, ProDiscover and many others.

- By utilizing the bit-stream image, the Computer Forensics Examiner takes no risk of contaminating the original evidence.

- The Computer Forensics Examiner creates the bit-stream image by attaching the original computer media to a write protection device that ensures no writes can take place to the original media while the bit-stream image is created.

▶▶ 5.4 Type of Evidence

- Evidence comes in many forms, and even if it's not admissible in court it can still be relevant to a case and provide valuable insight during an investigation.

- Some of the major types of evidence are as follows:

1. Illustrative evidence
2. Electronic evidence
3. Documented evidence
4. Explainable evidence
5. Substantial evidence
6. Testimonial evidence

5.4.1 Illustrative or Demonstrative Evidence

- Illustrative evidence is also called as demonstrative evidence.

- Demonstrative evidence is evidence in the form of a representation of an object.

- This is, as opposed to, real evidence, testimony, or other forms of evidence used at trial.

- An object or document is considered to be demonstrative evidence when it directly demonstrates a fact. It's a common and reliable kind of evidence.

- Examples of demonstrative evidence include photos, x-rays, videotapes, movies, sound recordings, diagrams, forensic animation, maps, drawings, graphs, animation, simulations, and models.

- In a workplace investigation, this could be an audio recording of someone's harassing behaviour or a photograph of offensive graffiti.

- It is useful for assisting a finder of fact (fact-finder) in establishing context among the facts presented in a case.

- In addition to the foregoing sets of tactical and technical issues, illustrative evidence may present additional considerations, such as:

- Which presentation medium or combination of media will be most persuasive?

- Whether to present animation in a fixed form that cannot be altered to accommodate changed assumptions or in a form that can be modified.

- Whether such evidence will need to be disclosed pre-trial.

5.4.2 Electronics Evidence

- Electronic evidence is information and data of investigative value that are stored in or transmitted by an electronic device.

- Electronics evidence is nothing but digital evidence. Digital evidence means information stored or transmitted in binary form that may be relied on in court.

- Digital evidence can be any sort of digital file from an electronic source.

- This includes email, text messages, instant messages, files and documents extracted from hard drives, electronic financial transactions, audio files, video files.

- Digital evidence can be found on any server or device that stores data, including some lesser-known sources such as home video game consoles, GPS sport watches and internet-enabled devices used in home automation.

- Digital evidence is often found through internet searches using open source intelligence (OSINT).

- Collecting digital evidence requires a skill set not always needed for physical evidence.

- There are many methods for extracting digital evidence from different devices and these methods, as well as the devices on which evidence is stored, change rapidly.

- Investigators need to either develop specific technical expertise or rely on experts to do the extraction for them.

- Preserving digital evidence is also challenging because unlike physical evidence, it can be altered or deleted remotely.

- Investigators need to be able to authenticate the evidence, and also provide documentation to prove its integrity.

5.4.3 Documented Evidence

- Documented evidence is any evidence that is, or can be, introduced at a trial in the form of documents, as distinguished from oral testimony.

- Documentary evidence is most widely understood to refer to writings on paper (such as an invoice, a contract or a will), but the term can also apply to any media by which information can be preserved, such as photographs; a medium that needs a mechanical device to be viewed, such as a tape recording or film; and a printed form of digital evidence, such as emails or spreadsheets.

- Normally, before documentary evidence is admissible as evidence, it must be proved by other evidence from a witness that the document is genuine, called "laying a foundation".

- Documentary evidence is subject to specific forms of authentication, usually through the testimony of an eyewitness to the execution of the document, or to the testimony of a witness able to identify the handwriting of the purported author.

- Documentary evidence is also subject to the best evidence rule, which requires that the original document be produced unless there is a good reason not to do so.

5.4.4 Explainable Evidence

Explainable evidence which is also knows Exculpatory evidence is evidence favourable to the defendant in a criminal trial that exonerates or tends to exonerate the defendant of guilt.

This type of evidence can exonerate a defendant in a – usually criminal – case. Prosecutors and police are required to disclose to the defendant any exculpatory evidence they find or risk having the case dismissed.

5.4.5 Substantial Evidence

Substantial evidence is a legal concept that an individual piece of evidence is so sufficient that a reasonable person of sound mind could convict or acquit based on that one piece of evidence alone.

It is also called as physical evidence. Physical evidence is any material object that plays some role in the matter that gave rise to the litigation, introduced as evidence in a judicial proceeding (such as a trial) to prove a fact in issue based on the object's physical characteristics.

Examples of Substantial evidence

1. Where the accused of a murder is caught by the police with a knife in his hand having blood stains at near the dead body.

2. Where the accused is in possession of a gun having fired a shot on the dead person.

- The presentation of substantive evidence raises tactical and technical considerations.

- Tactical considerations
  o Should e-mail messages and other digital evidence be presented in hard copy or on screen?
  o Will the jury be able to review hard copies of digital evidence in the jury room?
  o Should all relevant files or only specific examples be offered ? If all are to be offered, should all of them or only specific examples be discussed? How should sample files (e.g., files in a child pornography case) be selected?
  o Digital evidence may include voluminous records for which summaries may be appropriate.

Digital Evidence

- Technical considerations
  - Addressing technical glitches during trial (e.g., arrange for technical support, provide backup or hard copies).
  - Preparing the courtroom for presentation of digital evidence.
  o Ensure the computers are functional.
  o Check that adequate and appropriate equipment is available and in working order, and that wiring and functional outlets are in place.
  o Notify court security that special equipment will be in the courtroom.
  o Notify the court reporter if audio will be presented.
  o Consider the placement of monitors and lighting issues.

- Presenting the evidence.
  o Have clean copies of exhibits.
  o Ensure adequate setup time.
  o Ensure that standby mode, start-up screen, sound (if applicable), and screen savers are deactivated.
  o Remember where presentation ended at the last break (i.e., cueing).
  o Create an adequate court record by fully describing referenced exhibits. Consider asking the court to allow non-traditional means of recording the presentation of evidence (e.g., videotape of computer presentations, printouts of screen captures, CD-ROMs).
  o Provide jury notebooks or exhibit books.
  o Consider whether to request jury note taking.

5.4.6 Testimonial Evidence

- In the law, testimony is a form of evidence that is obtained from a witness who makes a solemn statement or declaration of fact.

- Testimony may be oral or written, and it is usually made by oath or affirmation under penalty of perjury.

- To be admissible in court and for maximum reliability and validity, written testimony is usually witnessed by

one or more persons who swear or affirm its authenticity also under penalty of perjury.

- Unless a witness is testifying as an expert witness, testimony in the form of opinions or inferences is generally limited to those opinions or inferences that are rationally based on the perceptions of the witness and are helpful to a clear understanding of the witness' testimony.

▶▶ 5.5 Challenges in Evidence Handling

- Properly retrieved evidence requires a paper trail.

- Properly collecting evidence is a big challenge. It must be authenticated at a judicial proceedings and chain of custody for the evidence must be maintained.

- After detention, it is necessary to ensure that the traditional chain of custody remains intact, but is not enough to determine the authenticity of the data or evidence obtained from forensic examinations.

- In addition to traditional chains of custody, the handling of digital evidence may require complementary precautionary measures.

- However, care should be taken to avoid unexpected agency relationships between law enforcement and private employees who have or are considering processing potential digital evidence.

- The image used to explain the testimony of the witness is easy to verify.

- Usually only the testimony of the witness is required.

- According to personal knowledge, the image can fairly and accurately depict the content it represents.

- Digital photos provided as pictures of a crime scene should generally be certified like traditional photos, unless there is a real focus on the change.

- For example, enhancing digital images may raise authentication issues.

- Re-creations and simulations that accompany expert testimony may require the same foundation as the expert testimony itself (see section III.E, below) to support the assumptions on which such evidence rests.

Testimony that the input and output parameters were correct may also be needed.

For example, simulations are commonly used, in civil cases to portray airline disasters and automotive crashes.

- Authentication issues in such cases focus on the extent to which input data correspond to actual events (in terms of accuracy and completeness) and the scientific validity of the mathematical model underlying the simulation.

- For example, enhancing digital images can cause authentication issues.

- The reconstruction and simulation accompanying the expert testimony may require the same basis as the expert testimony itself to support the assumptions on which such evidence is based.

- Testimony that the input and output parameters were correct may also be needed. For example, simulation are often used in civil cases to depict airline disasters and car crashes.

- In this case, the authentication problem focuses on the degree to which the input data corresponds to the actual event (in terms of accuracy and completeness) and the scientific validity of the underlying mathematical model.

- Whether computer-generated evidence to be used in trials can cause hearsay problems depends on the purpose of the introduction and the nature of the evidence.

- In some cases, complete or apparently sufficient explanations cannot be found for specific anomalies in the evidence.

- In other cases, the cost of interpreting the exception (for example, a computer programmer or an electrical engineer) would be prohibitively high in practice.

- As computers and operating systems become more complex, most network administrators and computer maintainers limit their problem resolution to the most frequent ones.

- Computer experts accept unexplained "errors" or "faults" without questioning the validity of its information stored or processed by the computer.

Failure to adequately document the response to a computer security incident.

5.5.1 Authentication of Evidence

- In the law of evidence, authentication is the process of proving that documentary evidence and other physical evidence are real, not counterfeit.

- Generally, authentication can be displayed in one of two ways.

- First, witnesses can testify on the chain of custody through the passage of evidence from discovery to trial.

- Second, the evidence can be authenticated through the opinions of an expert witness, who will examine the evidence to determine if it has all the characteristics expected if it is true.

- For handwritten documents, anyone who has been familiar with the alleged author's handwriting before the cause of action in the lawsuit can prove that there is a file in the handwriting.

- There are several documents that are generally considered self-certification documents.

- These include commercial labels, newspapers and other periodicals, as well as official publications from government agencies.

- A special category of evidence called an ancient document will be deemed authentic if it can be shown to be more than twenty years old, and found in a place and condition that a document of that age would likely be found.

5.5.2 Chain of Custody

- A chain of custody is a document that is borrowed from law enforcement that tracks evidence from the time the Computer Forensics Examiner gains possession of the item until it is released back to the owner.

- This document contains the basic information about the client and law firm, billing party, details about the media such as brand, type, serial number and other basic information.

The form also tracks each person who has touched the media for such items as collection, imaging, and return of property.

- The form has a line every time each item is removed from secure storage.

- There is need to establish a policy for secure storage and handling of potential evidence.

- The objective of this step is to secure the evidence for the longer term once it has been collected and to facilitate its retrieval if required.

- It concerns the long-term or off-line storage of information that might be required for evidence at a later date.

- A policy for secure storage and handling of potential evidence comprises security measures to ensure the authenticity of the data and also procedures to demonstrate that the evidence integrity is preserved whenever it is used, moved or combined with new evidence.

- In the parlance of investigation this is known as chain of custody.

- The continuity of evidence also includes records of who held, and who had access to, the evidence (for example from swipe control door logs).

- A significant contribution to the legal collection of evidence is given by the code of practice on the legal admissibility and weight of information stored electronically, published by the British Standards Institution. This document originated from a perceived need for evidence collection in the paperless office.

- The problem it addressed is if all paper documents are scanned, can the paper sources be thrown away without loss of evidential usability?

- The current edition broadens the scope to all information management systems. All too opportunistic searches, without justification, for potentially incriminating activities or communication such as those where information is transmitted over networks such as email systems for example, hardware and even the

- It points out that methods of storage, access control, and even the reliability, operation and access control.

programs and source code, may be investigated in order to determine admissibility.

- A closely related international standard is being developed as ISO 15801.

- The required output of this step is a secure evidence policy.

- It should document the security measures, the legal advice and the procedural measures used to ensure the evidence requirement is met.

- Upon this document rests the likely admissibility and weight of any evidence gathered.

- Preservation of the chain of custody is accomplished by having verifiable documentation that indicates who handled the evidence, when they handled it, and the locations, dates, and times of where the evidence was stored.

- Secure storage of evidence is necessary, or custody cannot be verified.

- When evidence is collected and ready for analysis, it is important to store and archive the evidence in a way that ensures its safety and integrity.

- Clearly document the chain of custody of the evidence.

- Create a check-in / check-out list that includes information such as the name of the person examining the evidence, the exact date and time they check out the evidence, and the exact date and time they return it.

- The investigator must thoroughly examine the situation and if deemed essential, a further search warrant any be required to search third party data carriers like ISP.

- After acquisition, the chain of custody, which the record of history of the custody of the evidence is prepared and recorded.

- After bringing the digital media to the forensics lab, proper chain of custody should be maintain and these evidences should be stored in a physically safe location with access control facility.

- Also enough duplicate copies of the media should be made to carry out the investigation.

NEVER USE ORIGINAL MEDIA FOR CARRYING OUT INVESTIGATION.

5.5.3 Evidence Validation

- The challenge is to make sure that the data you collect or obtain is the same as the data provided or presented to the court.

- Many years pass between the collection of evidence, and the production of evidence during court proceedings. This is quite common.

- To meet the challenge of authentication, it is important to ensure that the original media will match the forensic duplication using the MD5 hash.

- The MD5 engine does a remarkably good job of generating a cascade effect on all the bits in the hash value even when just a single bit in the input file is changed.

- The forensics community can still rely upon MD5 to do an excellent job at identifying even the smallest change in electronic data.

- The computer forensics community will want to embrace the new hash technology once it has been thoroughly tested by the cryptographic community.

- Until then, computer forensics examiners should feel comfortable in their continued, albeit short, term use of MD5.

- When possible, hashing electronic evidence with both MD5 and a second hash function such as SHA-1 or SHA-256 is always a good idea.

- The forensics software needs to support multiple hash functions, however, for this to be feasible.

- Unless new information emerges showing a further weakness in the MD5 hash algorithm, we should continue to use MD5.

- Forensics examiners should work with the manufacturers of forensic software so that new releases, when possible, will start implementing stronger hash functions, such as SHA-1 or SHA-256 into the forensics process.

5.6 Volatile Evidence

- Some evidence appears only when the computer or server is running and is lost when the computer is turned off.

- Evidence that exists only when the computer is running is called volatile evidence and must be collected using real-time forensics.

- This includes evidence in system RAM (random access memory), such as programs that exist only in computer memory.

- These programs are considered TSR or "terminate and stay" programs.

- Many types of malware (such as Trojan horse programs, viruses, and worms) are designed as memory-only programs that appear in the computer's memory when the computer is running, and disappear when the computer is turned off, in many cases will not leave any traces.

- There are many other kinds of volatile evidence that are only available when the computer is running, including certain temporary files, log files, cached files, and passwords.

- Powering off the computer clears the RAM and all existing data is lost.

- This can be a crucial step if you suspect that any type of data encryption is enabled to prevent viewing of the hard drive or parts of the hard drive.

- In many cases, the only way to recover the password needed to remove encryption on your hard drive is to collect "live memory" before shutting down your computer.

- Similarly, if the computer is running, you can access the encrypted portion of the data store, but only before the computer is turned off, so the hard drive must be copied while the computer is still on.

- There are tools to make copies of RAM and hard drives on running computers and line-of-business servers that cannot be shut down, and still ensure that these copies can be heard properly in court.

Digital Evidence

- Order of volatility : It is a good idea to process the evidence to be collected.

- Generally, we want to start with the most volatile evidence first. In computer forensics, this is known as the order of volatility.

- This descending list works from the most volatile (RAM) to the least volatile (archived data).

The order of volatility is:

1. CPU, cache, and register content

2. Routing table, ARP cache, process table, kernel statistics

3. Memory

4. Temporary file system/swap space

5. Data on hard disk

6. Remotely logged data

7. Data contained on archival media

▶ 5.7 Multiple Choice Questions for Online Exam

Section 5.1

Q. 1 _____ is defined as any data that is stored or transmitted using a computer.

a. Digital evidence

b. digital photographs

c. computer memory

d. none of the above

Ans. : (a)

Q. 2 _____ is Evidence must have been preserved and gathered in such a way that it can be used in court.

a. Admissible

b. Complete

c. Reliable

d. Understandable and believable

Ans. : (a)

Digital Evidence

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem 6) 5-13

Q. 3 _____ Any evidence collected must be reliable. This depends on the methodology and science used.

a. Admissible
b. Complete
c. Reliable
d. Understandable and believable

Ans. : (c)

Section 5.2

Q. 4 _____ it must be in conformity with common law and legislative rules.

a. Admissibility
b. Authentication
c. Completeness
d. None of the above

Ans. : (a)

Q. 5 The value of trace (or contact) forensic evidence was first recognized by _____

a. burglars
b. Edmund Locard
c. Paul L. Kirk
d. None of the above

Ans. : (b)

Q. 6 Digital evidence is usually not in a format that is directly readable by _____

a. Human
b. Computer
c. Machine
d. None of the above

Ans. : (a)

Q. 7 Digital evidences must follow the requirements of the _____

a. Best Evidence Rule
b. Best digital Rule
c. Best computer Rule
d. All of the above

Ans. : (a)

Q. 8 _____ evidence is information and data of investigative value that are stored on or transmitted by an electronic device.

a. Manual
b. Electronic
c. Document
d. None of the above

Ans. : (b)

Q. 9 _____ evidence is any evidence that is, or can be, introduced at a trial in the form of documents, as distinguished from oral testimony.

a. Manual
b. Electronic
c. Document
d. None of the above

Ans. : (c)

Q. 10 _____ which is also knows Exculpatory evidence is evidence favorable to the defendant in a criminal trial that exonerates or tends to exonerate the defendant of guilt.

a. Explainable evidence
b. Substantial Evidence
c. Document evidence
d. None of the above

Ans. : (a)

Section 5.5

Q. 11 _____ is the process of proving that documentary evidence and other physical evidence are real, not counterfeit.

a. Chain of Custody
b. Authentication evidence
c. Evidence Validation
d. none of the above

Ans. : (b)

Q.12 A _____ is a document that is borrowed from law enforcement that tracks evidence from the time the Computer Forensics Examiner gains possession of the item until it is released back to the owner.

a. Chain of custody
b. Authentication evidence
c. Evidence Validation
d. none of the above

Ans. : (a)

Q.13 _____ evidence appears only when the computer or server is running and is lost when the computer is turned off.

a. Volatile
b. Document
c. electronic
d. none of the above

Ans. : (a)

Q.14 Evidence that exists only when the computer is running is called _____

a. volatile evidence
b. Document
c. Chain of custody
d. None of the above

Ans. : (a)

Q.15 Implementing stronger hash functions, such as _____

a. SHA-1 or SHA-256
b. SHA-1 or SHA-255
c. SHA-II or SHA-266
d. None of the above

Ans. : (a)

Section 5.4

Q.16 _____ is a form of evidence that is obtained from a witness who makes a solemn statement or declaration of fact.

a. Testimonial Evidence
b. Substantial Evidence
c. Explainable Evidence
d. Documented evidence

Ans. : (a)

Q.17 _____ is a legal concept that an individual piece of evidence is so sufficient that a reasonable person of sound mind could convict or acquit based on that one piece of evidence alone.

a. Testimonial Evidence
b. Substantial Evidence
c. Explainable Evidence
d. Documented evidence

Ans. : (b)

Q.18 _____ is evidence in the form of a representation of an object.

a. Testimonial Evidence
b. Substantial Evidence
c. Explainable Evidence
d. demonstrative evidence

Ans. : (d)

Section 4.3

Q.19 The _____ states that "with contact between two items, there will be an exchange."

a. Locard's Exchange Principle
b. Paul L. Kirk principle
c. Edmund Locard principle
d. None of the above

Ans. : (a)

Q.20 Digital evidence is often found through internet searches using _____

a. open source internet (OSINT)
b. open source intelligence (OSINT)
c. open source interaction (OSINT)
d. open source interface (OSINT)

Ans. : (b)

Q. 21 _____ need to either develop specific technical expertise or rely on experts to do the extraction for them.

a. Investigators   b. Digital evidence

c. documentation   d. none of the above

Ans. : (a)

Q. 22 Collecting digital evidence requires a skill set not always needed for _____ evidence

a. physical   b. public

c. private   d Virtual

Ans. : (a)

Q. 23 _____ mentioned that digital evidence is the only sequence of bits that can be arranged in an array to display information.

a. Fred Cohen

b. Locard's Exchange Principle

c. Paul L. Kirk principle

d. Edmund Locard's principle

Ans. : (a)

Q. 24 The evidence must me convincing and understandable by the _____.

a. Investigators

b. Digital evidence

c. documentation

d. Judges

Ans. : (a)

Q. 25 _____ it must be in conformity with common law and legislative rules. There must be relationship between the evidence and the fact being proved.

a. Admissibility

b. Reliability

c. Completeness

d. None of the above

Ans. : (d)

Chapter Ends...

❑❑❑

CHAPTER 6
Introduction of Ethical Hacking

Syllabus

6.1 Ethical Hacking
- How Hackers Beget Ethical Hackers
- Defining hacker, Malicious users

6.2 Understanding the need to hack your own systems

6.3 Understanding the dangers your systems face
- Nontechnical attacks
- Network-infrastructure attacks
- Operating-system attacks
- Application and other specialized attacks

6.4 Obeying the Ethical hacking Principles
- Working ethically
- Respecting privacy
- Not crashing your systems

6.5 The Ethical hacking Process
- Formulating your plan
- Selecting tools
- Executing the plan
- Evaluating results
- Moving on

6.6 Cracking the Hacker Mindset
- What You're Up Against?
- Who breaks in to computer systems?
- Why they do it?
- Planning and Performing Attacks
- Maintaining Anonymity

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   6-2

Introduction of Ethical Hacking

6.1 Introduction Ethical Hacking

Ethical hacking is to scan the vulnerabilities and to find potential threats on a computer or networks. An ethical hacker finds a weak points or the loopholes in computer, web applications or network and also reports them to the organization.

These are various types of hackers:

(1) White Hat Hackers (Cyber-Security Hacker)

(2) Black Hat Hackers (Cracker)

(3) Gray Hat Hackers (Both)

1. White Hat Hackers

Here, we need to check for bugs and ethically report it to organization. We are authorized as user to test for bugs in the website or the network and report it to them.

White hat hackers generally get all the needed information about application or the network to test for, from organization itself. They use their skills to test it before website goes live or it attacked by malicious hackers.

2. Black Hat Hackers

- In this the organization does not allow the user to test it. They unethically enter inside website and also steal data from admin panel or manipulate data.

- They only focus on themselves and advantages they will get from personal data for personal financial gain.

- They can cause major damage to company by altering the functions which lead to loss of the company at a much higher extent. This can even lead you to extreme consequences.

3. Grey Hat Hackers

- They sometimes access to data and the violates law. But never have same intention as Black hat hackers, they often operate for common good. The main difference is that they exploit vulnerability publicly whereas white hat hackers do it privately for company.

Ethical hacking also known as penetration testing or white-hat hacking - involves the same tools, tricks, and techniques that hackers use, but with one major difference :

- ○ Ethical hacking is legal.
- ○ Ethical hacking is performed with the target's permission.
- ○ The intent of ethical hacking is to discover vulnerabilities from a hacker's viewpoint so systems can be better secured. It is part of an overall information risk management program that allows for ongoing security improvements.
- ○ Ethical hacking can also ensure that vendors' claims about the security of their products are legitimate

6.1.1 How Hackers Beget Ethical Hackers

- All are heard of hackers. Many of us have even suffered the consequences of hacker actions. Information which we need to know is :

  - ○ Who are these hackers ?
  - ○ Why is it important to know about them?

6.1.2 Defining Hacker, Malicious users

Hacker is a word that has two meanings :

- Normally, a hacker is someone who likes to tinker with software or electronic systems. Hackers enjoy exploring and learning how computer systems operate. They love discovering new ways to work electronically.

- Recently, hacker has taken on a new meaning - someone who maliciously breaks into systems for personal gain. Technically, these criminals are crackers (criminal hackers). Crackers break into (crack) systems with malicious intent. They are out for personal gain: fame, profit, and even revenge. They modify, delete, and steal critical information, often making other people miserable.

- The good-guy (white-hat) hackers do not like being in the same category as the bad-guy (black-hat) hackers.

Introduction of Ethical Hacking

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   6-4

(These terms come from Western movies where the good guys wore white cowboy hats and the bad guys wore black cowboy hats.) Whatever the case, most people give hacker a negative connotation.

- Many malicious hackers claim that they do not cause damage but instead are altruistically helping others. Yeah, right. Many malicious hackers are electronic thieves

▸▸ 6.2 Understanding the Need to Hack Your Own Systems

- The law of averages works against security. With the increased numbers and expanding knowledge of hackers combined with the growing number of system vulnerabilities and other unknowns, the time will come when all computer systems are hacked or compromised in some way.

- Protecting your systems from the bad guys and not just the generic vulnerabilities that everyone knows about is absolutely critical. When you know hacker tricks, you can check how vulnerable your systems are.

- Hacking preys on weak security practices and undisclosed vulnerabilities. Firewalls, encryption, and virtual private networks (VPNs) can create a false feeling of safety.

- These security systems often focus on high-level vulnerabilities, such as viruses and traffic through a firewall, without affecting how hackers work. Attacking your own systems to discover vulnerabilities is a step to making them more secure.

- This is the only proven method of greatly hardening your systems from attack. If you do not identify weaknesses, it is a matter of time before the vulnerabilities are exploited.

- As hackers expand their knowledge, so should you. You must think like them to protect your systems from them. You, as the ethical hacker, must know activities hackers carry out and how to stop their efforts. You should know what to look for and how to use that information to thwart hackers' efforts.

- You do not have to protect your systems from everything. You can't. The only protection against everything is to unplug your computer systems and lock them away so no one can touch them not even you. That's not the best approach to information security. What's important is to protect your systems from known vulnerabilities and common hacker attacks.

- It is impossible to buttress all possible vulnerabilities on all your systems. You can't plan for all possible attacks especially the ones that are currently unknown. However, the more combinations you try the more you test whole systems instead of individual units the better your chances of discovering vulnerabilities that affect everything as a whole.

- Do not take ethical hacking too far, though. It makes little sense to harden your systems from unlikely attacks. For instance, if you do not have a lot of foot traffic in your office and no internal Web server running, you may not have as much to worry about as an Internet hosting provider would have. However, do not forget about insider threats from malicious employees!

- Your overall goals as an ethical hacker should be as follows:

  o Hack your systems in a non destructive fashion.

  o Enumerate vulnerabilities and, if necessary, prove to upper management that vulnerabilities exist.

  o Apply results to remove vulnerabilities and better secure your systems.

▸▸ 6.3 Understanding the Dangers your Systems Face

- It is one thing to know that your systems generally are under fire from hackers around the world. It is another to understand specific attacks against your systems that are possible. This section offers some well-known attacks but is by no means a comprehensive listing. That requires its own book : Hack Attacks Encyclopaedia, by John Chirillo (Wiley Publishing, Inc.).

Many information-security vulnerabilities are not critical by themselves. However, exploiting several vulnerabilities at the same time can take its toll.

For example, a default Windows OS configuration, a weak SQL Server administrator password, and a server hosted on a wireless network may not be major security concerns separately.

But exploiting all three of these vulnerabilities at the same time can be a serious issue

6.3.1 Nontechnical Attacks

Exploits that involve manipulating people end users and even yourself are the greatest vulnerability within any computer or network infrastructure.

- Humans are trusting by nature, which can lead to social-engineering exploits. Social engineering is defined as the exploitation of the trusting nature of human beings to gain information for malicious purposes.

- Other common and effective attacks against information systems are physical. Hackers break into buildings, computer rooms, or other areas containing critical information or property.

- Physical attacks can include dumpster diving (rummaging through trash cans and dumpsters for intellectual property, passwords, network diagrams, and other information).

6.3.2 Network-Infrastructure Attacks

Hacker attacks against network infrastructures can be easy, because many networks can be reached from anywhere in the world via the Internet.

Here are some examples of network-infrastructure attacks:

- Connecting into a network through a rogue modem attached to a computer behind a firewall.

- Exploiting weaknesses in network transport mechanisms, such as TCP/IP and NetBIOS Flooding a network with too many requests, creating a denial of service (DoS) for legitimate requests.

- Installing a network analyzer on a network and capturing every packet that travels across it, revealing confidential information in clear text.

- Piggybacking onto a network through an insecure 802.11b wireless configuration

6.3.3 Operating-system attacks

- Hacking operating systems (OSs) is a preferred method of the bad guys.

- OSs comprise a large portion of hacker attacks simply because every computer has one and so many well-known exploits can be used against them.

- Occasionally, some operating systems that are more secure out of the box such as Novell NetWare and the flavours of BSD UNIX are attacked, and vulnerabilities turn up.

- But hackers prefer attacking operating systems like Windows and Linux because they are widely used and better known for their vulnerabilities.

- Here are some examples of attacks on operating systems :

  o   Exploiting specific protocol implementations.

  o   Attacking built-in authentication systems.

  o   Breaking file-system security.

  o   Cracking passwords and encryption mechanisms

6.3.4 Application and other Specialized Attacks

- Applications take a lot of hits by hackers. Programs such as e-mail server software and Web applications often are beaten down :

  o   Hypertext Transfer Protocol (HTTP) and Simple Mail Transfer Protocol (SMTP) applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.

  o   Malicious software (malware) includes viruses, worms, Trojan horses, and spyware. Malware clogs networks and takes down systems.

Introduction of Ethical Hacking

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6) 6-6

- o Spam (junk e-mail) is wreaking havoc on system availability and storage space. And it can carry malware.

- Ethical hacking helps reveal such attacks against your computer systems.

- Parts II through V of this book cover these attacks in detail, along with specific countermeasures you can implement against attacks on your systems.

▶▶ 6.4 Obeying the Ethical Hacking Principles

Every ethical hacker must abide by a few basic commandments. If not, bad things can happen. I've seen these commandments ignored or forgotten when planning or executing ethical hacking tests. The results weren't positive.

6.4.1 Working ethically

- The word ethical in this context can be defined as working with high professional morals and principles. Whether you are performing ethical hacking tests against your own systems or for someone who has hired you, everything you do as an ethical hacker must be aboveboard and must support the company's goals. No hidden agendas are allowed.

- Trustworthiness is the ultimate tenet. The misuse of information is absolutely forbidden. That's what the bad guys do.

6.4.2 Respecting privacy

- Treat the information you gather with the utmost respect. All information you obtain during your testing from Web-application log files to clear-text passwords must be kept private.

- Do not use this information to snoop into confidential corporate information or private lives.

- If you sense that someone should know there's a problem, consider sharing that information with the appropriate manager.

Involve others in your process. This is a "watch the watcher" system that can build trust and support your ethical hacking projects.

6.4.3 Not Crashing your Systems

- One of the biggest mistakes I've seen when people try to hack their own systems is inadvertently crashing their systems.

- The main reason for this is poor planning. These testers have not read the documentation or misunderstand the usage and power of the security tools and techniques.

- You can easily create DoS conditions on your systems when testing. Running too many tests too quickly on a system causes many system lockups.

- I know because I've done this! Do not rush things and assume that a network or specific host can handle the beating that network scanners and vulnerability assessment tools can dish out.

- Many security-assessment tools can control how many tests are performed on a system at the same time.

- These tools are especially handy if you need to run the tests on production systems during regular business hours.

- You can even create an account or system lockout condition by social engineering someone into changing a password, not realizing that doing so might create a system lockout condition.

▶▶ 6.5 The Ethical Hacking Process

Like practically any IT or security project, ethical hacking needs to be planned in advance. Strategic and tactical issues in the ethical hacking process should be determined and agreed upon.

Planning is important for any amount of testing from a simple password-cracking test to an all-out penetration test on a Web application.

6.5.1 Formulating Your Plan

- Approval for ethical hacking is essential. Make what you are doing known and visible at least to the decision makers. Obtaining sponsorship of the project is the first step.

- This could be your manager, an executive, a customer, or even yourself if you are the boss.

You need someone to back you up and sign off on your plan. Otherwise, your testing may be called off unexpectedly if someone claims they never authorized you to perform the tests.

The authorization can be as simple as an internal memo from your boss if you are performing these tests on your own systems.

- If you are testing for a customer, have a signed contract in place, stating the customer's support and authorization.

Get written approval on this sponsorship as soon as possible to ensure that none of your time or effort is wasted.

- This documentation is your Get Out of Jail Free card if anyone questions what you are doing.

You need a detailed plan, but that does not mean you have to have volumes of testing procedures. One slip can crash your systems not necessarily what anyone wants. A well-defined scope includes the following information :

o Specific systems to be tested

o Risks that are involved

o When the tests are performed and your overall timeline

o How the tests are performed How much knowledge of the systems you have before you start testing

o What is done when a major vulnerability is discovered

- The specific deliverables this include security-assessment reports and a higher level report outlining the general vulnerabilities to be addressed, along with the countermeasures that must be implemented

- When selecting systems to test, start with most critical or the vulnerable systems.

- For instance, you can test computer passwords or attempt social engineering attack before drilling down into more detailed systems.

- It pays to have contingency plan for your ethical hacking process in case something goes awry.

- What if you are assessing your firewall or Web application, and you take it down?

- This can cause system unavailability, which can reduce system performance or employee productivity.

- Even worse, it could cause loss of data integrity, loss of data, and the bad publicity.

- Handle social engineering and the denial-of-service (DoS) attacks carefully. Determine how they can affect systems you are testing and also your entire organization.

- Determining when a tests are performed is something that you should think long and also hard about. Do you test during normal business hours?

- How about late at night or early in the morning so that production systems are not affected? Involve others to make sure they approve of your timing.

- The best approach is an unlimited attack, wherein any type of the test is possible.

- The bad guys are not hacking your systems within a limited scope, so why should you? Some exceptions to this approach are performing DoS, social engineering, and the physical-security tests.

- Do not stop with one security hole. This can lead to a false sense of security. Keep going to check what else you can discover

- One of your goals may be to perform tests without being detected.

- For example, you may be performing your tests on the remote systems or on a remote office, and you do not want the users to be aware of what you are doing. Otherwise, users may be on to you and be on their best behaviour.

- You do not required extensive knowledge of systems you are testing just a basic understanding. This will help you protect tested systems.

- Understanding a systems you are testing must not be difficult if you are hacking your own in-house systems. If you are hacking a customer's systems, you may have to dig deeper.

- Most people are scared of these assessments. Base the type of test you will perform on your organization's or customer's needs.

6.5.2 Selecting Tools

- As with any project, if you do not have right tools for ethical hacking, accomplishing a task effectively is difficult.

- Having said that, just because you use the right tools does not mean that you will discover all vulnerabilities.

- Know the personal and the technical limitations. Many security-assessment tools generate false positives and also negatives (incorrectly identifying vulnerabilities). Others may miss vulnerabilities.

- If you are performing tests like as social engineering or physical-security assessments, you may miss weaknesses.

- Many tools focus on specific tests, but no one tool can test for everything.

- For the same reason that you wouldn't drive in a nail with a screwdriver, you must not use a word processor to scan your network for open ports.

- This is why you need a set of specific tools that you can call on for the task at hand. The more tools you have, the easier your ethical hacking efforts are.

- Make sure you that you are using the right tool for the task :

  o To crack passwords, you need a cracking tool such as LC4, John the Ripper, or pwdump. A general port scanner, such as Super Scan, may not crack passwords.

  o For an in-depth analysis of a Web application, a Web-application assessment tool (such as Whisker or Web Inspect) is more appropriate than a network analyzer (such as Ethereal).

- When selecting the right security tool for the task, ask around. Get advice from your colleagues and from other people online. A simple Groups search on Google (www.google.com) or perusal of security portals, such as SecurityFocus.com,

SearchSecurity.com, and ITsecurity.com, often produces great feedback from other security experts.

- Hundreds, if not thousands, of tools can be used for the ethical hacking from your own words and the actions to software based vulnerability assessment programs to hardware based network analyzers. The following list runs down some commercial, freeware, and open-source security tools:

  o Nmap

  o EtherPeek

  o SuperScan

  o QualysGuard

  o WebInspect

  o LC4 (formerly called L0phtcrack)

  o LANguard Network Security Scanner

  o Network Stumbler

  o ToneLoc

- Here are some other popular tools :

  o Internet Scanner

  o Ethereal

  o Nessus

  o Nikto

  o Kismet

  o THC-Scan

- The capabilities of several security and the hacking tools are often misunderstood.

- This misunderstanding has shed negative light on some excellent tools, like as SATAN (Security Administrator Tool for Analyzing Networks) and Nmap (Network Mapper).

- Some of these tools are complex. Whichever tools you use, familiarize yourself with them before you start using them. Here are ways to do that:

  o Read the readme and/or online help files for your tools.

  o Study the user's guide for your commercial tools.

  o Consider formal classroom training from the security-tool vendor or another third-party training provider, if available.

Look for these characteristics in tools for the ethical hacking :

○ Adequate documentation.

○ Detailed reports on the discovered vulnerabilities, including how they may be exploited and fixed.

○ Updates and support when needed.

○ High-level reports that can be presented to managers or nontechnical types.

These features can save time and effort when you are writing the report.

6.5.3 Executing the Plan

- The Ethical hacking can take persistence. Time and also patience are important. Need to be careful when you are performing your ethical hacking tests.

- A hacker in your network or a seemingly benign employee looking over your shoulder may watch what's going on. This person could use this information against you.

- It is not practical to make sure that no hackers are on your systems before you start. Just make sure you keep everything as quiet and also private as possible.

- This is especially critical when transmitting and also storing your test results.

- If possible, encrypt these e-mails and a files using Pretty Good Privacy (PGP) or something similar. At a minimum, password-protect them.

- You are now on a reconnaissance mission. Harness as much information as possible about your organization and the systems, which is what malicious hackers do. Start with a broad view and narrow your focus :

1. Search the Internet for your organization's name, your computer and network system names, and your IP addresses. Google is a great place to start for this.

2. Narrow your scope, targeting the specific systems you are testing. Whether physical-security structures or Web applications, a casual assessment can turn up much information about your systems.

3. Further narrow your focus with a more critical eye. Perform actual scans and other detailed tests on your systems.

4. Perform the attacks, if that's what you choose to do.

6.5.4 Evaluating Results

- Assess your results to check what you uncovered, assuming that the vulnerabilities haven't been made obvious before now.

- This is where knowledge counts. Evaluating the results and correlating the specific vulnerabilities discovered is a skill that gets better with experience.

- You will end up knowing your systems as well as anyone else. This makes the evaluation process much simpler moving forward.

- Submit a formal report to upper management or to your customer, outlining your results.

- Keep these other parties in the loop to show that your efforts and their money are well spent.

6.5.5 Moving On

- When you will finished your ethical hacking tests, you still need to implement your analysis and recommendations to make sure your systems are secure.

- New security vulnerabilities continually appear. Information systems constantly change and become more complex.

- New hacker exploits and security vulnerabilities are regularly uncovered. Security tests are a snapshot of the security posture of your systems.

- At any time, everything can change, especially after software upgrades, adding computer systems, or applying patches. Plan to test regularly.

6.6 Cracking the Hacker Mindset

- Before you start assessing security of your own systems, you may want to know something about people you are up against.

A SACHIN SHAH Venture

- Many information security product vendors and other professionals claim that you should protect your systems from bad guys both internal and also external. But what does this mean? How do you know how these people think and work?

- Knowing what hackers and the malicious users want help you understand how they work. Understanding how they work helps you to look at your information systems in a whole new way.

6.6.1 What you are up Against?

- In the media, public perception of hacker has transformed from harmless tinkerer to malicious criminal.

- Nevertheless, hackers often state that public misunderstands them, which is mostly true. It is easy to prejudge what you do not understand.

- Unfortunately, many hacker stereotypes are based on misunderstanding rather than fact, misunderstanding that fuels a constant debate.

- Hackers can be classified by both their abilities and their underlying motivations. Some are skilled, and their motivations are benign; they're merely seeking more knowledge.

- At the other end of the spectrum, hackers with malicious intent seek some form of personal gain. Unfortunately, the negative aspects of hacking usually overshadow the positive aspects and promote the negative stereotypes.

- When they were growing up, hackers' rivals were monsters and the villains on video game screens. Now hackers check their electronic foes as only that electronic.

- Hackers who perform malicious acts do not really think about the fact that human beings are behind the firewalls, wireless networks, and Web applications they're attacking.

- They ignore that their actions often affect those human beings in negative ways, like as jeopardizing their job security.

- On the flip side, odds are you have at least a handful of employees, contractors, interns, or consultants who intend to compromise sensitive information on your network for malicious purposes.

- These people do not hack in the way people normally suppose. Instead, they root around in files on server shares, delving into databases they know they must not be in, sometimes stealing, modifying, and deleting sensitive information to which they have access.

- This behaviour is often very hard to detect especially given the widespread belief by management that users can and should be trusted to do the right things.

- This activity is perpetuated if these users passed their criminal background and credit checks before they were hired.

- Past behaviour is often the best predictor of future behaviour, but just because someone has a clean record and authorization to access sensitive systems does not mean he or she won't do anything bad. Criminals have to start somewhere!

- As negative as breaking into computer systems often can be, hackers and malicious users play key roles in the advancement of technology.

- In a world with-out hackers, odds are that the latest intrusion prevention technology, data leakage protection, or vulnerability scanning tools would not exist.

- Such a world may not be bad, but technology does keep us in our jobs and keeps our field moving forward.

- Unfortunately, the technical security solutions can't ward off all malicious attacks and unauthorized use because hackers and (sometimes) malicious users are usually a few steps ahead of technology.

- However you view the stereotypical hacker or malicious user, one thing is certain: Somebody will always try to take down your computer systems and compromise information by poking and prodding where he or she must not, by all-out hacking, or by creating and launching automated worms and other malware. You must take the appropriate steps to protect your systems against this kind of intrusion.

6.6.2 Who Breaks in to Computer Systems?

Computer hackers have been around for decades. Since the Internet became widely used in the late 1990s, the mainstream public has started to hear more and more about hacking.

- Only a few hackers, such as John Draper (also known as Captain Crunch), and Kevin Mitnick, are really well known. Many more unknown hackers are looking to make a name for themselves. They're the ones you have to look out for.

- In a world of black and white, describing typical hacker is easy. A general stereotype of a hacker is an antisocial, pimply faced, teenage boy.

- But world has many shades of gray and many types of hackers. Hackers are human and unique individuals, so an exact profile is hard to outline.

- The best broad description of hackers is that all hackers are not equal.

- Each hacker has his or her own unique motives, methods, and skills. Hacker skill levels fall into three general categories:

☞ Script kiddies

- These are computer novices who take advantage of the hacker tools, vulnerability scanners, and the documentation available free on Internet but do not have any knowledge of what is really going on behind the scenes.

- They know just enough to cause you headaches, but typically are very sloppy in their actions, leaving all sorts of digital fingerprints behind.

- Even though these guys are the stereotypical hackers that you hear about in the news media, they often need only minimal skills to carry out their attacks.

☞ Criminal hackers

- These are skilled criminal experts who also write some of hacking tools, including scripts and other programs that the script kiddies and the ethical hackers use.

- These folks also write such malware as viruses and worms.

- They can break into systems and cover their tracks. They can even make it look like someone else hacked their victims' systems.

☞ Security researchers

- These are highly technical and publicly known IT professionals who not only monitor and track computer, network, and application vulnerabilities but also write the tools and other code to exploit them.

- If these guys did not exist, we would not have much in the way of open source security testing tools.

- I follow many of these security researchers on a weekly basis via their blogs, message boards, and articles and you should, too. Following the progress of these security researchers helps you stay up to date on both vulnerabilities and the latest and greatest security tools.

- The Black Hat security conference that found that everyday IT professionals even engage in malicious and criminal activity against others.

- And people wonder why IT does not get the respect it deserves! Perhaps this group will evolve into a fourth general category of hackers in the coming years.

- Regardless of age and complexion, hackers possess curiosity, bravado, and often very sharp minds.

☞ Perhaps more important than a hacker's skill level is his or her motivation :

1. **Hacktivists** try to disseminate political or social messages through their work. A hacktivist wants to raise public awareness of an issue yet they want to remain anonymous. In many situations, these hackers will try to take you down if you express a view that's contrary to theirs. Examples of hacktivism are the websites that were defaced with the *Free Kevin* messages that promoted freeing Kevin Mitnick from prison for his famous hacking escapades. Others cases of hacktivism include messages about legalizing drugs, protests against the war, protests centered around

...A SACHIN SHAH Venture

Introduction of Ethical Hacking

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6) 6-12

wealth envy and big corporations, and just about any other social and political issue you can think of.

2. **Cyber terrorists** (both organized and unorganized, often backed by government agencies) attack corporate or government computers and public utility infrastructures, such as power grids and air-traffic control towers. They crash critical systems, steal classified data, or expose the personal information of government employees. Countries take the threats these cyber terrorists pose so seriously that many mandate information security controls in crucial industries, such as the power industry, to protect essential systems against these attacks.

3. **Hackers for hire** are part of organized crime on the Internet. Many of these hackers hire out themselves or their DoS creating botnet for money.

6.6.3 Why they do it?

- Hackers hack because they can. Period. Okay, it goes a little deeper than that.

- Hacking is a casual hobby for some hackers they hack just to check what they can and can't break into, usually testing only their own systems. These are not the folks.

- Focus on those hackers who are obsessive about gaining notoriety or defeating computer systems, and those who have criminal intentions.

- Many hackers get a kick out of outsmarting corporate and government IT and security administrators. They thrive on making headlines and being notorious.

- Defeating an entity or possessing knowledge that few other people have makes them feel better about themselves, building their self-esteem.

- Many of these hackers feed off the instant gratification of exploiting a computer system.

- They become obsessed with this feeling. Some hackers cannot resist the adrenaline rush they get from breaking into someone else's systems. Often, the more difficult the job is, the greater the thrill is for hackers.

- It is a bit ironic given their collective tendencies but hackers often promote individualism or at least the decentralization of information because many believe that all information should be free.

- They think their attacks are different from attacks in the real world.

- Hackers may easily ignore or misunderstand their victims and the consequences of hacking. They do not think long-term about the choices they are making today.

- Many hackers say they do not intend to harm or profit through their bad deeds, a belief that helps them justify their work.

- Many do not look for tangible payoffs. Just proving a point is often a sufficient reward for them. The word sociopath comes to mind.

- The knowledge that malicious attackers gain and the self-esteem boost that comes from successful hacking might become an addiction and a way of life. Some attackers want to make your life miserable, and others simply want to be seen or heard.

- Some common motives are revenge, basic bragging rights, curiosity, boredom, challenge, vandalism, theft for financial gain, sabotage, blackmail, extortion, corporate espionage, and just generally speaking out against "the man."

- Hackers regularly cite these motives to explain their behaviour, but these motivations tend to be cited more commonly during difficult economic conditions.

- Malicious users inside your network may be looking to gain information to help them with personal financial problems, to give them a leg up over a competitor, to seek revenge on their employers, to satisfy their curiosity, or to relieve boredom.

- Remember that hackers often hack simply because they can.

- Some hackers go for high-profile systems, but hacking into anyone's system helps them fit into hacker circles. Hackers exploit many people's false sense of security and go for almost any system they think they can compromise.

Electronic information can be in more than one place at the same time, so if hackers merely copy information from the systems they break into, it is tough to prove that hackers possess that information and it is impossible to get it back.

Similarly, hackers know that a simple defaced web page however easily attacked is not good for someone else's business.

It often takes a large-scale data breach; however, hacked sites can often persuade management and other nonbelievers to information threats and vulnerabilities.

Many recent studies have revealed that most security flaws are very basic in nature.

These nothing but the basic flaws the low-hanging fruit of the network just waiting to be exploited.

Computer breaches continue to get easier to execute yet harder to prevent for several reasons:

- Widespread use of networks and Internet connectivity

- Anonymity provided by computer systems working over the Internet and often on the internal network (because effective logging, monitoring, and alerting rarely takes place).

- Greater number and availability of hacking tools. Large number of open wireless networks that help hackers cover their tracks.

- Greater complexity of networks and the codebases in the applications and databases being developed today Computer-savvy children.

- Unlikeliness that attackers will be investigated or prosecuted if caught.

6.6.4 Planning and Performing Attacks

Attack styles vary widely

Some hackers prepare far in advance of a large attack. They gather small bits of information and methodically carry out their hacks. These hackers are the most difficult to track.

Other hackers usually the inexperienced script kiddies act before they think through the consequences.

- Such hackers may try, for example, to telnet directly into an organization's router without hiding their identities.

- Other hackers may try to launch a DoS attack against the Microsoft Exchange server without first determining the version of Exchange or the patches that are installed. These hackers usually are caught.

- Malicious users are all over the map. Some can be quite savvy based on their knowledge of network and of how IT operates inside the organization.

- Others go poking and the prodding around into systems they must not be in or must not have had access to in the first place and often do stupid things that lead security or network administrators back to them.

- Whatever approach they take, most malicious attackers' prey on ignorance. They know the following aspects of real-world security:

- **The majority of computer systems are not managed properly.** The computer systems are not properly patched, hardened, or monitored. Attackers can often fly below the radar of the average firewall or intrusion prevention system (IPS). This is especially true for malicious users whose actions are often not monitored at all while, at same time, they have full access to the very environment they can exploit.

- **Most network and security administrators simply can't keep up with the deluge of new vulnerabilities and attack methods.** These people often have too many tasks to stay on top of and too many other fires to put out. Network and the security administrators may also fail to notice or respond to security events because of poor time and goal management. I provide resources on time and goal management for IT and security professionals in the Appendix.

- **Information systems grow more complex every year.** This is yet another reason why overburdened administrators find it difficult to know what's happening across the wire and on the hard drives of all their systems. Virtualization, cloud services, and mobile devices such as laptops, tablets, and phones are making things exponentially worse. Time is an attacker's friend and it is almost always on his or her

Introduction of Ethical Hacking

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   6-14

side. By attacking through computers rather than in person, hackers have more control over the timing for their attacks :

○ Attacks can be carried out slowly, making them hard to detect.

○ Attacks are frequently carried out after typical business hours,

– Often in the middle of the night, and from home, in the case of malicious users.

– Defence are often weaker after hours with less physical security and less intrusion monitoring when the typical network administrator (or security guard) is sleeping.

6.6.5 Maintaining Anonymity

– Smart attackers need to remain as low key as possible. Covering their tracks is the priority, and also many times their success depends on them remaining unnoticed.

–. They want to avoid raising suspicion so they can come back and access systems in the future.

– Hackers often remain anonymous by using one of the following resources:

○ They Borrowed or stolen remote desktop and VPN accounts from friends or previous employers

○ Public computers at libraries, schools, or kiosks at local mall they use Open wireless networks

○ Internet proxy servers or anonymizer services Anonymous or disposable e-mail accounts from free e-mail services

○ Open e-mail relays

○ Infected computers also called zombies or hots at other organizations

○ Workstations or servers on the victim's own network

– If the hackers use enough stepping stones for their attacks, they are hard practically impossible to trace.

– Luckily, one of your biggest concerns the malicious user generally is not quite as savvy.

– That is, unless the user is an actual network or security administrator.

▸▸ 6.7 Multiple Choice Questions for Online Exam

Q. 1 What is the meaning of the statement double fun(int) ?

(a) The function fun takes an argument of type double & returns the int types value.

(b) The function fun takes an argument of type double & returns the double type value.

(c) The function fun is of type int.

(d) None of this

Ans. : (b)

Q. 2 Which of the following statements best describes a white-hat hacker?

a) Security professional

b) Former black hat

c) Former grey hat

d) Malicious hacker

Ans. : (A)

Explanation : A white-hat hacker is a "good" guy who uses his skills for defensive purposes.

Q. 3 Which type of hacker represents the highest risk to your network?

a) Disgruntled employees

b) Black-hat hackers

c) Grey-hat hackers

d) Script kiddies

Ans. : (A)

Explanation : Disgruntled employees have information which can allow them to launch a powerful attack.

Hackers who help in finding bugs and vulnerabilities in a system & don't intend to crack a system are termed as _____

a) Black Hat hackers

b) White Hat Hackers

c) Grey Hat Hackers

d) Red Hat Hackers

Ans : (B)

Explanation : White Hat Hackers are cyber security analyst and consultants who have the intent to help firms and Governments in the identification of loopholes as well as help to perform penetration tests for securing a system.

Q.5 Which is the legal form of hacking based on which jobs are provided in IT industries and firms?

a) Cracking

b) Non ethical Hacking

c) Ethical hacking

d) Hactivism

Ans. : C

Explanation: Ethical Hacking is an ethical form of hacking done by white-hat hackers for performing penetration tests and identifying potential threats in any organizations and firms. They are nefarious hackers, and their main motive is to gain financial profit by doing cyber crimes.

Q.6 Who are "they" referred to here ?

a) Gray Hat Hackers

b) White Hat Hackers

c) Hactivists

d) Black Hat Hackers

Ans. : (B)

Introduction of Ethical Hacking

Explanation: Black Hat hackers also termed as 'crackers' and are a major type of cyber criminals who take unauthorized access in user's account or system and steal sensitive data or inject malware into the system for their profit or to harm the organization.

Q.7 Which of the following tools are used for foot printing? (Choose 3 answers.)

a) Whois

b) Sam Spade

c) NMAP

d) SuperScan

e) Nslookup

Ans.: (A), (B), (E)

Explanation : Who is, Sam Spade, and nslookup are all used to passively gather information about a target. NMAP and SuperScan are host and network scanning tools.

Q.8 Performing a shoulder surfing in order to check other's password is _____ ethical practice.

a) a good

b) not so good

c) very good social engineering practice

d) a bad

Ans. : (D)

Explanation : Overlooking or peeping into someone's system when he/she is entering his/her password is a bad practice and is against the ethics of conduct for every individual. Shoulder surfing is a social engineering attack approach used by some cyber-criminals to know your password and gain access to your system later.

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   6-16

Introduction of Ethical Hacking

Q. 9 Leaking your company data to the outside network without prior permission of senior authority is a crime.

a) True   b) False

Ans. : (A)

Explanation : Without prior permission of the senior authority or any senior member, if you're leaking or taking our your company's data outside (and which is confidential), then it's against the code of corporate ethics.

Q. 10 _____ is the technique used in business organizations and firms to protect IT assets.

a) Ethical hacking

b) Unethical hacking

c) Fixing bugs

d) internal data-breach

Ans. : (A)

Explanation : Ethical hacking is a that used by business organizations and firms for exploiting vulnerabilities to secure the firm. Ethical hackers help in increasing the capabilities of any organization or firm in protecting their IT and information assets.

Q. 11 Before performing any penetration test, through legal procedure, which key points listed below is not mandatory?

a) Know the nature of the organization

b) Characteristics of work done in the firm

c) System and network

d) Type of broadband company used by the firm

Ans. : (D)

Explanation : Before performing any penetration test, through the legal procedure the key points that the penetration tester must keep in mind are :

i) Know the nature of the organization

ii) what type of work the organization do and

iii) the system and networks used in various departments and their confidential data that are sent and received over the network.

Q. 12 _____ is the branch of cyber security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong.

a) Social ethics

b) Ethics in cyber-security

c) Corporate ethics

d) Ethics in black hat hacking

Ans. : (D)

Explanation : Ethics in cyber-security is the branch of cyber security that deals with morality and provides different theories and principles' regarding the view-points about what is right and what need not to be done.

Q. 13 The full form of Malware is _____

a) Malfunctioned Software

b) Multipurpose Software

c) Malicious Software

d) malfunctioning of Security

Ans. : (C)

Explanation : Different types of harmful software and programs that can pose threats to a system, network or anything related to cyberspace are termed as Malware. Examples of some common malware are Virus, Trojans, Ransom ware, spyware, worms, rootkits etc.

Q.16 Which of the following statements best describes a white-hat hacker?

a) Security professional

b) Former black hat

c) Former grey hat

d) Malicious hacker

Ans. : (A)

Explanation : A white-hat hacker is a "good" guy who uses his skills for defensive purposes.

Q.17 Hacking for a cause is called _____

a) Active hacking   b) Hacktivism

c) Activism   d) Black-hat hacking

Ans. : (B)

Explanation : Hacktivism is performed by individual who claim to be hacking for a political or social cause.

Q.18 _____ is the branch of cyber security that deals with morality and provides different theories and a principle regarding the view-points about what is right and wrong.

a) Social ethics

b) Ethics in cyber-security

c) Corporate ethics

d) Ethics in black hat hacking

Ans. : (D)

Explanation : Ethics in cyber-security is the branch of cyber security that deals with morality and provides different theories and principles' regarding the view-points about what is right and what need not to be done.

Q.19 Connecting into a network through a rogue modem attached to a computer behind a _____.

a) firewall   b) operating System

c) DoS   d) None of the above

Ans. : (A)

Q.18 Exploiting weaknesses in _____ mechanisms.

a) Physical layer   b) network's transport

c) IP addressing   d) none of the above

Ans. : (B)

Q.19 Piggybacking onto a network through an insecure _____ wireless configuration.

a) 802.11a   b) 802.11b

c) both a and b   d) none of the above

Ans. : (B)

Q.20 Attacks on operating systems:

a) Exploiting specific protocol implementations.

b) Attacking built-in authentication systems.

c) Breaking file-system security.

d) all of the above

Ans. : (D)

Q.21 _____ applications are frequently attacked because most firewalls and other security mechanisms are configured to allow full access to these programs from the Internet.

a) HTTP and SMTP

b) ICMP and SMTP

c) TCP and HTTP

d) None of the above

Ans. : (A)

Q.22 _____ includes viruses, worms, Trojan horses, and spyware. Malware clogs networks and takes down systems.

a) Malicious software

b) file-system

c) down systems

d) none of the above

Ans. : (A)

Q. 23 ____is wreaking havoc on system availability and storage space. And it can carry malware.

a) Spam   b) Malware

c) SMTP   d) none of the above

Ans. : (A)

Q. 24 ____issues in the ethical hacking process should be determined and agreed upon.

a) Strategic and tactical

b) planning and strategic

c) ethical and strategic

d) none of the above

Ans. : (A)

Q. 25 Planning is important for any amount of testing from a simple ____test to an all-out penetration test on a Web application.

a) password – cracking

b) password – hacking

c) password – attacking

d) none of the above

Ans. : (A)

Q. 26 ____These are computer novices who take advantage of the hacker tools, vulnerability scanners, and the documentation available free on Internet.

a) Script kiddies

b) Criminal hackers

c) Security researchers

d) None of the above

Ans. : (A)

27 ____These are skilled criminal experts who also write some of hacking tools

a) Script kiddies

b) Criminal hackers

c) Security researchers

d) None of the above

Ans. : (B)

Q. 28 ____these are highly technical and publicly known IT professionals

a) Security researchers

b) network hackers.

c) Black Hat security

d) non of the above

Ans. : (A)

Q. 29 ____attack corporate or government computers and public utility infrastructures.

a) Cyber terrorists   b) DoS

c) Hackers   d) None of the above

Ans. : (A)

Q. 30 ____also called zombies or hots at other organizations

a) Public computers

b) Infected computers

c) dead computer

d) sleep computer

Ans. : (B)

Q. 31 Nmap is abbreviated as Network Mapper.

a) True   b) False

Ans. : (A)

Explanation : Network Mapper (Nmap) is a popular open-source tool used for discovering network as well as security auditing. It can be used for either a single host network or large networks.

Q. 32 ____ is a password recovery and auditing tool.

a) LC3   b) LC4

c) Network Stumbler   d) Maltego View

Ans. : (B)

Explanation : LC4 which was previously known as LOphtCrack is a password auditing and recovery tool; used for testing strength of a password and also helps in recovering lost Microsoft Windows passwords

Using pop-up windows to get a user to give out information is which type of social engineering attack?

a) Human-based   b) Computer-based
c) Nontechnical   d) Coercive

Ans. : (B)

Explanation : Pop-up windows are a method of getting information from a user utilizing a computer.

What is enumeration?

a) Identifying active systems on the network
b) Cracking passwords
c) Identifying users and machine names
d) Identifying routers and firewalls

Ans. : (C)

Explanation : Enumeration is the process of finding usernames, machine names, network shares, and services on the network.

an employee's credentials is called the _____ mode of ethical hacking.

a) Local networking
b) Social engineering
c) Physical entry
d) Remote networking

Ans. : (A)

Explanation : Local networking uses an employee's credentials, or access rights, to gain access to the network. Physical entry uses credentials to gain access to the physical IT infrastructure.

Q. 36 Attempting to gain access to a network using an employee's credentials is called the _____ mode of ethical hacking

a) Local networking
b) Social engineering
c) Physical entry
d) Remote networking

Ans. : (A)

Explanation : Local networking uses an employee's credentials, or access rights, to gain access to the network. Physical entry uses credentials to gain access to the physical IT infrastructure.

Q. 37 Which of the following is not a typical characteristic of an ethical hacker?

a) Excellent knowledge of Windows.
b) Understands the process of exploiting network vulnerabilities.
c) Patience, persistence and perseverance.
d) Has the highest level of security for the organization.

Ans. : (D)

Explanation : Each answer has validity as a characteristic of an ethical hacker. Though having the highest security clearance is ideal, it is not always the case in an organization.

Q. 38 What is the purpose of a Denial of Service attack ?

a) Exploit a weakness in the TCP/IP stack
b) To execute a Trojan on a system
c) To overload a system so it is no longer operational
d) To shutdown services by turning them off

Ans. : (C)

Explanation : DoS attacks force systems to stop responding by overloading the processing of the system.

Q. 39 Having individuals provide personal information to obtain a free offer provided through the Internet is considered what type of social engineering?

a) Web-based

b) Human-based

c) User-based

d) Computer-based

Ans. : (D)

Explanation : Whether using email, a fake website, or popup to entice the used, obtaining information from an individual over the Internet is a computer-based type of social engineering

Q. 40 When a hacker attempts to attack a host via the Internet it is known as what type of attack?

a) Local access

b) Remote attack

c) Internal attack

d) Physical access

Ans. : (B)

Explanation : An attack from the Internet is known as a remote attack.

Q. 41 What are the two basic types of attacks ?

a) Active   b) Passive   c) DoS   d) 1 & 2

Ans. : (D)

Explanation : Active & Passive are the two basic types of attacks.

Q. 42 What port number does HTTPS use?

a) 53   b) 443   c) 80   d) 21

Ans. : (B)

Explanation : HTTPS uses TCP port 443. This is a well-known port number and can be found in the Windows services file.

Chapter Ends....

□□□

l Hacking

host via

type of

ack

cess

ternet is

ks ?

& 2

the two

1

43.

l can be

r Ends...

□□□

CHAPTER 7

Network Hacking

UNIT VI

Syllabus

7.1 Network hacking

Network Infrastructure :

- Network Infrastructure Vulnerabilities
- Scanning-Ports
- Ping sweep
- Scanning SNMP
- Grabbing Banners
- Analysing Network Data and Network Analyzer
- MAC-daddy attack

Wireless LANs :

- Implications of Wireless Network Vulnerabilities,
- Wireless Network Attacks

7.2 Operating System Hacking

- Introduction of Windows and Linux Vulnerabilities

7.3 Applications Hacking

Messaging Systems :

- Vulnerabilities,
- E-Mail Attacks- E-Mail Bombs,
- Banners,
- Best practices for minimizing e-mail security risks

Web Applications :

- Web Vulnerabilities,
- Directories Traversal and Countermeasures,

Data base system :

- Database Vulnerabilities
- Best practices for minimizing database security risks

Network Hacking

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   7-2

7.1 Network Infrastructure

To have secure operating systems and applications, you need a secure network. Devices such as routers, firewalls, and even generic network hosts (including servers and workstations) must be assessed as part of the security testing process.

There are thousands of possible network vulnerabilities, equally as many tools, and even more testing techniques. You probably don't have the time or resources available to test your network infrastructure systems for all possible vulnerabilities, using every tool and method imaginable. Instead, you need to focus on tests that will produce a good overall assessment of your network and the tests I describe in this chapter produce exactly that.

You can eliminate many well-known, network-related vulnerabilities by simply patching your network hosts with the latest vendor software and firmware updates.

Because many network infrastructure systems aren't publicly accessible, odds are good that your network hosts will not be attacked from the outside. You can eliminate many other vulnerabilities by following some solid security practices on your network, as described in this chapter. The tests, tools, and techniques outlined in this chapter offer the most bang for your security assessment buck.

7.1.1 Network Infrastructure Vulnerabilities

Network infrastructure vulnerabilities are the foundation for most technical security issues in your information systems.

These lower-level vulnerabilities affect practically everything running on your network. That's why you need to test for them and eliminate them whenever possible.

Your focus for security tests on your network infrastructure should be to find weaknesses that others can see in your network so you can quantify and treat your network's level of exposure.

When you assess your company's network infrastructure security, you need to look at the following :

o Where devices, such as a firewall or an IPS, are placed on the network and how they're configured

o What external attackers see when they perform port scans and how they can exploit vulnerabilities in your network hosts

o Network design, such as Internet connections, remote access capabilities, layered defences, and placement of hosts on the network

o Interaction of installed security devices, such as firewalls, intrusion prevention systems (IPSs), antivirus, and so on

o What protocols are in use, including known vulnerable ones such as Secure Sockets Layer (SSL)

o Commonly attacked ports that are unprotected

o Network host configurations

o Network monitoring and maintenance

– If someone exploits a vulnerability in one of the items in the preceding list or anywhere in your network's security, bad things can happen :

o An attacker can launch a denial of service (DoS) attack, which can take down your Internet connection or your entire network.

o A malicious employee using a network analyzer can steal confidential information in e-mails and files sent over the network.

o A hacker can set up back-door access into your network.

o A contractor can attack specific hosts by exploiting local vulnerabilities across the network.

o Test your systems from the outside in, and the inside in (that is, on and between internal network segments and demilitarized zones [DMZs]).

o Obtain permission from partner networks to check for vulnerabilities on their systems that can affect your network's security, such as open ports, lack of a firewall, or a misconfigured router.

7.1.2 Scanning-Ports

- A port scanner shows you what's what on your network by scanning the network to see what's alive and working. Port scanners provide basic views of how the network is laid out. They can help identify unauthorized hosts or applications and network host configuration errors that can cause serious security vulnerabilities.

- The big-picture view from port scanners often uncovers security issues that might otherwise go unnoticed. Port scanners are easy to use and can test network hosts regardless of what operating systems and applications they're running. The tests are usually performed relatively quickly without having to touch individual network hosts, which would be a real pain otherwise.

- The trick to assessing your overall network security is interpreting the results you get from a port scan. You can get false positives on open ports, and you might have to dig deeper. For example, User Datagram Protocol (UDP) scans like the protocol itself are less reliable than Transmission Control Protocol (TCP) scans and often produce false positives because many applications don't know how to respond to random incoming UDP requests.

- If your results don't match after you run the tests using different tools, you might want to explore the issue further. If something doesn't look right such as a strange set of open ports it probably isn't. Test again; if you're in doubt, use another tool for a different perspective.

Port Number	Service	Protocol(s)
7	Echo	UDP
19	Chargen	TCP, UDP
20	FTP data (File Transfer Protocol)	TCP
21	FTP control	TCP
22	SSH	TCP
23	Telnet	TCP

Port Number	Service	Protocol(s)
25	SMTP (Simple Mail Transfer Protocol)	TCP
37	Time	TCP, UDP
53	DNS (Domain Name System)	UDP
69	TFTP (Trivial File Transfer Protocol)	UDP
79	Finger	TCP, UDP
80	HTTP (Hypertext Transfer Protocol)	TCP
110	POP3 (Post Office Protocol version 3)	TCP
111	SUN RPC (remote procedure calls)	TCP, UDP
135	RPC/DCE (end point mapper) for Microsoft networks	TCP, UDP
137, 138, 139, 445	NetBIOS over TCP/IP TCP, UDP	TCP, UDP
161	161 SNMP (Simple Network Management Protocol) ,	TCP, UDP
443	HTTPS (HTTP over TLS)	TCP
512, 513, 514	Berkeley r-services and r-commands (such as rsh, rexec, and rlogin)	TCP
1433	Microsoft SQL Server (ms-sql-s)	TCP, UDP
1434	Microsoft SQL Monitor (ms-sql-m)	TCP, UDP
1723	Microsoft PPTP VPN	TCP
3389	Windows Terminal Server	3389 Windows Terminal Server TCP
8080	HTTP	8080 HTTP proxy TCP

7.1.3 Ping Sweep

A ping sweep of all your network subnets and hosts is a good way to find out which hosts are alive and kicking on the network.

A ping sweep is when you ping a range of addresses using Internet Control Message Protocol (ICMP) packets.

Fig. 7.1.1 shows the command and the results of using Nmap to perform a ping sweep of a class C subnet range.
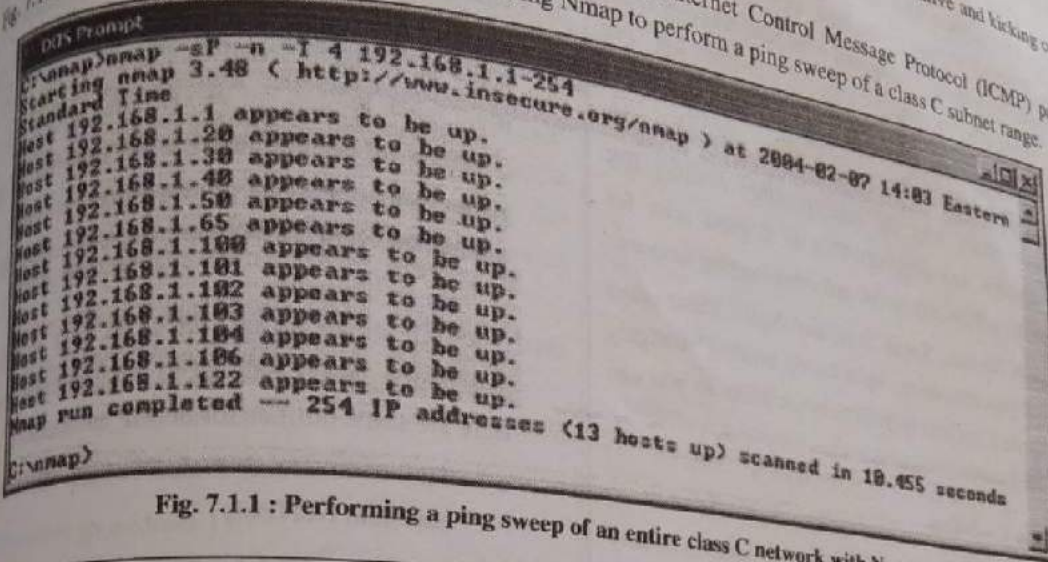
```
DOS Prompt                                                                    _|□|x|
C:\nmap>nmap -sP -n -T 4 192.168.1.1-254
Starting nmap 3.48 ( http://www.insecure.org/nmap ) at 2004-02-07 14:03 Eastern
Standard Time
Host 192.168.1.1 appears to be up.
Host 192.168.1.20 appears to be up.
Host 192.168.1.30 appears to be up.
Host 192.168.1.40 appears to be up.
Host 192.168.1.50 appears to be up.
Host 192.168.1.65 appears to be up.
Host 192.168.1.100 appears to be up.
Host 192.168.1.101 appears to be up.
Host 192.168.1.102 appears to be up.
Host 192.168.1.103 appears to be up.
Host 192.168.1.104 appears to be up.
Host 192.168.1.106 appears to be up.
Host 192.168.1.122 appears to be up.
Nmap run completed --- 254 IP addresses (13 hosts up) scanned in 10.455 seconds
C:\nmap>
```

Fig. 7.1.1 : Performing a ping sweep of an entire class C network with Nmap

Dozens of Nmap command line options exist, which can be overwhelming when you want only a basic scan. Nonetheless, you can enter Nmap on the command line to see all the options available.

The following command line options can be used for an Nmap ping sweep :

- sP tells Nmap to perform a ping scan.

- n tells Nmap not to perform name resolution.

- T4 tells Nmap to perform an aggressive (faster) scan.

- 192.168.1.1-254 tells Nmap to scan the entire 192.168.1.0

Using port scanning tools

Most port scanners operate in three steps :

The port scanner sends TCP SYN requests to the host or range of hosts you set it to scan. Some port scanners perform ping sweeps to determine which hosts are available before starting the TCP port scans.

2. The port scanner waits for replies from the available hosts.

3. The port scanner probes these available hosts for up to 65,534 possible TCP and UDP ports - based on which ports you tell it to scan to see which ones have available services on them.

- The port scans provide the following information about the live hosts on your network :

o   Hosts that are active and reachable through the network

o   Network addresses of the hosts found

o   Services or applications that the hosts may be running

(a) Nmap

After you have a general idea of what hosts are available and what ports are open, you can perform fancier scans to verify that the ports are actually open and not returning a false positive. Nmap allows you to run the following additional scans :

1.   **Connect :** This basic TCP scan looks for any open TCP ports on the host. You can use this scan to

see what's running and determine whether intrusion prevention systems (IPSs), firewalls, or other logging devices log the connections.

2. **UDP scan** : This basic UDP scan looks for any open UDP ports on the host. You can use this scan to see what's running and determine whether IPSs, firewalls, or other logging devices log the connections.

3. **SYN Stealth** : This scan creates a half-open TCP connection with the host, possibly evading IPS systems and logging. This is a good scan for testing IPSs, fire walls, and other logging devices.

4. **FIN Stealth, Xmas Tree, and Null** : These scans let you mix things up a bit by sending strangely formed packets to your network hosts so you can see how they respond.

b. **NetScan Tools Pro**

NetScan Tools Pro (www.netscantools.com) is a very nice all-in-one commercial tool for gathering general network information, such as the number of unique IP addresses, NetBIOS names, and MAC addresses. It also has a neat feature that allows you to fingerprint the operating systems of various hosts.

2. **Countermeasures against ping sweeping and port scanning**

- Enable only the traffic you need to access internal hosts preferably as far as possible from the hosts you're trying to protect and deny everything else. This goes for standard ports, such as TCP 80 for HTTP and ICMP for ping requests.

- Configure firewalls to look for potentially malicious behaviour over time (such as the number of packets received in a certain period of time) and have rules in place to cut off attacks if a certain threshold is reached, such as 10 port scans in one minute or 100consecutive ping (ICMP) requests.

🐁 7.1.4 Scanning SNMP

Simple Network Management Protocol (SNMP) is built in to virtually every network device. Network management

programs (such as HP Open View and LANDesk) use SNMP for remote network host management. Unfortunately, SNMP also presents security vulnerabilities.

1. **Vulnerabilities**

- The problem is that most network hosts run SNMP enabled with the default read/write community strings of public/private. The majority of network devices I come across have SNMP enabled and don't even need it.

- If SNMP is compromised, a hacker may be able to gather such network information as ARP tables, usernames, and TCP connections to attack your systems further.

- If SNMP shows up in port scans, you can bet that a malicious attacker will try to compromise the system. Here are some utilities for SNMP enumeration:

  o The commercial tools NetScan Tools Pro and Essential NetTools

  o Free Windows GUI-based Getif

  o Free Windows text-based SNMPUTIL

2. **Countermeasures against SNMP attacks**

- Preventing SNMP attacks can be as simple as A-B-C:

  o Always disable SNMP on hosts if you're not using it period.

  o Block the SNMP ports (UDP ports 161 and 162) at the network perimeter.

  o Change the default SNMP community read string from public and the default community write string from private to another long and complex value that's virtually impossible to guess.

- There's technically a "U" that's part of the solution: upgrade. Upgrading your systems (at least the ones you can) to SNMP version 3 can resolve many of the well-known SNMP security weaknesses.

🐁 7.1.5 Grabbing Banners

- Banners are the welcome screens that divulge software version numbers and other system information on network hosts.

This banner information might identify the operating system, the version number, and the specific service pack to give the bad guys a leg up on attacking the network.

You can grab banners by using either good old telnet or some of the tools I mention, such as Nmap and SuperScan.

Telnet

You can telnet to hosts on the default telnet port (TCP port 23) to see whether you' represented with a login prompt or any other information. Just enter the following line at the command prompt in Windows or UNIX: telnet ip_address

You can telnet to other commonly used ports with these commands :

SMTP : telnet ip_address 25

HTTP : telnet ip_address 80

POP3 : telnet ip_address 110

Countermeasures against banner-grabbing attacks

The following steps can reduce the chance of banner-grabbing attacks:

- If there isn't a business need for services that offer banner information, disable those unused services on the network host.

- If there isn't a business need for the default banners, or if you can customize the banners, configure the network host's application or operating system to either disable the banners or remove information from the banners that could give an attacker a leg up. Check with your specific vendor for information on how to do this. TCP Wrappers in Linux is another solution.

7.6 Analysing Network Data and Network Analyzer

Network analyser is a tool that allows you to look at a network and analyse data going across the wire for network optimization, security, and/or troubleshooting purposes. Like a microscope for a lab scientist, a network analyser is a must-have tool for any security professional.

- A network analyser is handy for sniffing packets on the wire. A network analyser is simply software running on a computer with a network card. It works by placing the network card in promiscuous mode, which enables the card to see all the traffic on the network, even traffic not destined for the network analyser's host. The network analyser performs the following functions :

  o Captures all network traffic

  o Interprets or decodes what is found into a human-readable format

  o Displays the content in chronological order (or however you choose to see it)

- When assessing security and responding to security incidents, a network analyser can help you :

  o View anomalous network traffic and even track down an intruder.

  o Develop a baseline of network activity and performance, such as protocols in use, usage trends, and MAC addresses, before a security incident occurs.

1. Network analyser programs

You can use one of the following programs for network analysis :

- **Savvies OmniPeek** OmniPeek is available for Windows operating systems.

- **TamoSoft's CommView** (www.tamos.com/products/commview) is a great, low cost, Windows-based alternative.

- **Cain and Abel** is a free multifunctional password recovery tool for performing ARP poisoning, capturing packets, cracking passwords, and more.

- **Wireshark** formerly known as Ethereal, is a free alternative. I download and use this tool if I need a quick fix and don't have my laptop nearby. It's not as user-friendly as most of the commercial products, but it is very powerful if you're willing to learn its ins and outs. Wireshark is available for both Windows and OS X.

- **ettercap** is another powerful (and free) utility for performing network analysis and much more on Windows, Linux, and other operating systems.

Here are a few caveats for using a network analyzer :

- To capture all traffic, you must connect the analyzer to one of the following :

  o   A hub on the network

  o   A monitor/span/mirror port on a switch

  o   A switch that you've performed an ARP poisoning attack on

- If you want to see traffic similar to what a network-based IPS sees, you should connect the network analyzer to a hub or switch monitor port or even a network tap on the outside of the firewall, as shown in Fig. 7.1.2 This way, your testing

  o   What's entering your network before the firewall filters eliminate the junk traffic.

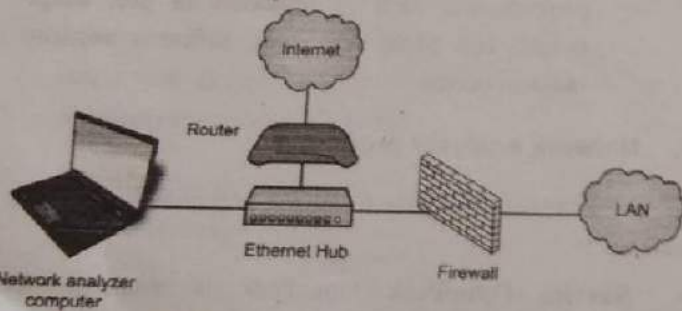 o   What's leaving your network after the traffic passes through the firewall.

Fig. 7.1.2 : Connecting a network analyzer outside the firewall.

2. Issues with Connecting a network analyzer outside the firewall

Odd traffic, such as :

- An unusual amount of ICMP packets

- Excessive amounts of multicast or broadcast traffic

- Protocols that aren't permitted by policy or shouldn't exist given your current network configuration

2. **Internet usage habits,** which can help point out malicious behaviour of a rogue insider or system that has been compromised, such as:

   - Web surfing and social media

   - E-mail

   - Instant messaging and other P2P software

3. **Questionable usage, such as:**

   - Many lost or oversized packets, indicating hacking tools or malware are

   - present

   - High bandwidth consumption that might point to a web or FTP server that doesn't belong

4. **Reconnaissance probes and system profiling from port scanners and vulnerability assessment tools,** such as a significant amount of inbound traffic from unknown hosts especially over ports that aren't used very much, such as FTP or telnet.

5. **Hacking in progress,** such as tons of inbound UDP or ICMP echo requests, SYN floods, or excessive broadcasts.

6. **Nonstandard hostnames on your network.** For example, if your systems are named Computer1, Computer2, and so on, a computer named GEEKz4evUR should raise a red flag.

7. **Hidden servers** (especially web, SMTP, FTP, DNS, and DHCP) that might be eating network bandwidth, serving illegal software, or accessing your network hosts.

8. **Attacks on specific applications** that show such commands as /bin/rm, /bin/ls, echo, and cmd.exe as well as SQL queries and JavaScript injection.

3. Countermeasures against network protocol vulnerabilities

A network analyzer can be used for good or evil. The good is to help ensure your security policies are being followed. The evil is when someone uses a network analyser against you. A few countermeasures can help prevent someone from using an unauthorized network

analyzer, although there's no way to prevent it completely

7.1.7 MAC daddy Attack

Attackers can use ARP (Address Resolution Protocol) running on your network to make their systems appear as your system or another authorized host on your network.

ARP spoofing

An excessive number of ARP requests can be a sign of an ARP spoofing attack (also called ARP poisoning) on your network.

A client running a program, such as dsniff (www.monkey.org/~dugsong/dsniff) or

Cain and Abel (www.oxid.it/cain.html), can change the ARP tables - the tables that store IP addresses to media access control (MAC) address mappings on network hosts. This causes the victim computers to think they need to send traffic to the attacker's computer rather than to the true destination computer when communicating on the network. ARP spoofing is used during man-in-the-middle (MITM) attacks.

Spoofed ARP replies can be sent to a switch, which reverts the switch to broadcast mode and essentially turns it into a hub. When this occurs, an attacker can sniff every packet going through the switch and capture anything and everything from the network.

- This security vulnerability is inherent in how TCP/IP communications are handled.

- Here's a typical ARP spoofing attack with a hacker's computer (Hacky) and two legitimate network users' computers (Joe and Bob):

1. Hacky poisons the ARP caches of victims Joe and Bob by using dsniff, ettercap, or a utility he wrote.

2. Joe associates Hacky's MAC address with Bob's IP address.

3. Bob associates Hacky's MAC address with Joe's IP address.

4. Joe's traffic and Bob's traffic are sent to Hacky's IP address first.

5. Hacky's network analyzer captures Joe's and Bob's traffic.

2. **Using Cain and Abel for ARP poisoning**

You can perform ARP poisoning on your switched Ethernet network to test your IPS or to see how easy it is to turn a switch into a hub and capture anything and everything with a network analyzer.

Perform the following steps to use Cain & Abel for ARP poisoning :

1. Load Cain and Abel and then click the Sniffer tab to enter the network analyzer mode.

   The Hosts page opens by default.

2. Click the Start/Stop APR icon (the yellow and black circle).

   The ARP poison routing (how Cain and Abel refers to ARP poisoning) process starts and enables the built-in sniffer.

3. If prompted, select the network adapter in the window that appears and then click OK.

4. Click the blue + icon to add hosts to perform ARP poisoning on.

5. In the MAC Address Scanner window that appears, ensure the All Hosts in My Subnet option is selected and then click OK.

6. Click the APR tab (the one with the yellow-and-black circle icon) to load the APR page.

7. Click the white space under the uppermost Status column heading (just under the Sniffer tab).

   This re-enables the blue + icon.

8. Click the blue + icon and the New ARP Poison Routing window shows the hosts discovered in Step 3.

9. 'Select your default route (in my case, 10.11.12.1).

   The right-hand column fills with all the remaining hosts.

10. Ctrl+click all the hosts in the right column that you want to poison.

11. **Click OK and the ARP poisoning process starts.**
This process can take anywhere from a few seconds to a few minutes depending on your network hardware and each hosts' local TCP/IP stack.

12. **You can use Cain and Abel's built-in passwords feature to capture passwords traversing the network to and from various hosts simply by clicking the Passwords tab.**

3. MAC address spoofing

- MAC address spoofing tricks the switch into thinking your computer is something else.

- You simply change your computer's MAC address and masquerade as another user.

A. UNIX-based systems : In UNIX and Linux, you can spoof MAC addresses with the ifconfig utility. Follow these steps :

1. **While logged in as root, use ifconfig to enter a command that disables the network interface.**

   Insert the network interface number that you want to disable (usually, eth0) into the command, like this :

   [root@localhost root]# ifconfig eth0 down

2. **Enter a command for the MAC address you want to use.**

   Insert the fake MAC address and the network interface number (eth0) into the command again, like this :

   [root@localhost root]# ifconfig eth0 hw ether new_mac_address

B. Windows

You can use regedit to edit the Windows Registry, but I like using a neat Windows utility called SMAC (www.klcconsulting.net/smac), which makes MAC spoofing a simple process. Follow these steps to use SMAC :

1. Load the program.

2. Select the adapter for which you want to change the MAC address.

3. Enter the new MAC address in the New Spoofed MAC Address fields and click the Update MAC button.

4. Stop and restart the network card with these steps:

   a. Right-click the network card in Network and Dialup Connections and then choose Disable.

   b. Right-click again and then choose Enable for the

5. Click the Refresh button in the SMAC interface.

- To reverse Registry changes with SMAC, follow these steps :

1. Select the adapter for which you want to change the MAC address.

2. Click the Remove MAC button.

3. Stop and restart the network card with these steps:

   a. Right-click the network card in Network and Dialup Connections and then choose Disable.

   b. Right-click again and then choose Enable for the change to take effect.

4. Testing denial of service attacks

- Denial of service (DoS) attacks are among the most common hacker attacks.

- A hacker initiates so many invalid requests to a network host that the host uses all its resources responding to the invalid requests and ignores the legitimate requests.

☞ DoS attacks

- DoS attacks against your network and hosts can cause systems to crash, data to be lost, and every user to jump on your case wondering when Internet access will be restored.

- Here are some common DoS attacks that target an individual computer or network device:

1. **SYN floods :** The attacker floods a host with TCP SYN packets.

2. **Ping of Death :** The attacker sends IP packets that exceed the maximum length of 65,535 bytes.

which can ultimately crash the TCP/IP stack on many operating systems.

3. **WinNuke :** This attack can disable networking on older Windows 95 and Windows NT computers.

Distributed DoS (DDoS) attacks have an exponentially greater impact on their victims. One of the most famous was the DDoS attack against eBay, Yahoo!, CNN, and dozens of other websites by a hacker known as MafiaBoy.

While updating this book to the third edition, there was a highly publicized DDoS attack against Twitter, Facebook, and other social media sites.

Counter measures against ARP poisoning and MAC address spoofing attacks

A few counter measures on your network can minimize the effects of an attack against ARP and MAC addresses:

Prevention : You can prevent MAC address spoofing if your switches can enable port security to prevent automatic changes to the MAC address tables.

Detection : You can detect these two types of hacks through an IPS or standalone MAC address monitoring utility.

7.1.8 Wireless LANs

Wireless local area networks or Wi-Fi specifically, the ones based on IEEE802.11 standard are increasingly being deployed into both business and home networks. Wi-Fi has been the poster child for weak security and network hack attacks since the inception of 802.11 a decade and a half ago. The stigma of unsecure Wi-Fi is starting to wane, but this isn't the time to lower your defences.

Wi-Fi offers a ton of business value, from convenience to reduced network deployment time. Whether or not your organization allow wireless network access, you probably have it, so testing for Wi-Fi security vulnerabilities is critical.

7.1.9 Implications of Wireless Network Vulnerabilities

The Wireless networks have longstanding vulnerabilities that can enable an attacker to bring your network to its knees or allow your sensitive information to be extracted right out of thin air. If your wireless network is compromised, you can experience following problems:

○ Loss of network access, including e-mail, web, and other services that can cause business downtime

○ The Loss of sensitive information, including passwords, customer data, intellectual property, and more

○ Regulatory consequences and also legal liabilities associated with the unauthorized users gaining access to your business systems

- Most of wireless vulnerabilities are in implementation of the 802.11 standard. Wireless access points (APs) and client systems have some vulnerabilities as well.

- Various fixes have come along in recent years to address these vulnerabilities, yet still many of these fixes have not been properly applied or are not enabled by default. Your employees might also install rogue wireless equipment on your network without your knowledge. Then there is "free" Wi-Fi practically everywhere your mobile workforce goes. From coffee shops to hotels to conference centres, these Internet connections are one of the most serious threats to your overall information security and a pretty difficult one to fight.

7.1.10 Wireless Network Attacks

- Various malicious hacks including DoS attacks can be carried out against your WLAN. This includes forcing APs to reveal their SSIDs during the process of being disassociated from the network and rejoining. In addition, hackers can literally jam the RF signal of an AP especially in 802.11b and 802.11g systems and force the wireless clients to re-associate to a rogue AP masquerading as the victim AP.

Network Hacking

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   7-12

- Hackers can create man-in-the-middle attacks by maliciously using a tool such as the Pineapple and can flood your network with thousands of packets per second by using the raw packet-generation tools Nping or NetScan Tools Pro enough to bring the network to its knees.

- Even more so than with wired networks, this type of DoS attack is very difficult to prevent on Wi-Fi. You can carry out several attacks against your WLAN. The associated countermeasures help protect your network from these vulnerabilities as well as from the malicious attacks previously mentioned. When testing your WLAN security, look out for the following weaknesses :

  o Unencrypted wireless traffic

  o Weak WEP and WPA pre-shared keys

  o Crackable Wi-Fi Protected Setup (WPS) PINs

  o Unauthorized APs

  o Easily circumvented MAC address controls

  o Wireless equipment that's physically accessible

  o Default configuration settings

▶▶ 7.2   Operating System Hacking

✎ 7.2.1   Introducing Windows Vulnerabilities

- Given Windows' ease of use, its enterprise-ready Active Directory service, and feature-rich .NET development platform, most organizations use the Microsoft platform for much of their networking and computing needs. Many businesses especially the small- to medium-sized ones depend solely on the Windows OS for network usage.

- Many large organizations run critical servers, such as web servers and database servers, on the Windows platform as well.

If security vulnerabilities aren't addressed and managed properly, they can bring a network or an entire organization(large or small) to its knees.

When Windows and other Microsoft software are attacked especially by a wide spread Internet-based worm or virus hundreds of thousands of organizations and millions of computers are affected. Many well-known attacks against Windows can lead to the following problems :

  o Leakage of sensitive information, including files containing healthcare information and credit card numbers

  o Passwords being cracked and used to carry out other attacks.

  o Systems taken completely offline by denial of service (DoS) attacks.

  o Full remote control being obtained

  o Entire databases being copied or deleted

1. **Choosing Tools**

Literally hundreds of Windows hacking and testing tools are available. The key is to find a set of tools that can do what you need and that you're comfortable using.

A. **Free Microsoft tools :** You can use the following free Microsoft tools to test your systems for various weaknesses:

1. **Built-in Windows programs** for NetBIOS and TCP/UDP service enumeration, such as these three :

  o nbtstat for gathering NetBIOS name table information

  o netstat for displaying open ports on the local Windows system

  o net for running various network-based commands, including viewing shares on remote Windows systems and adding user accounts after you gain are mote command prompt via Metasploit

2. **Microsoft Baseline Security Analyzer (MBSA)** to test for missing patches and basic Windows security settings

3. **Sys internals** to poke, prod, and monitor Windows services, processes, and resources both locally and over the network.

All-in-one assessment tools : All-in-one tools perform a wide variety of security tests, including the following :

- Port scanning
- OS fingerprinting
- Basic password cracking
- Detailed vulnerability mappings of the various security weaknesses that the tools find on your Windows systems

Task-specific tools : The following tools perform more specific tasks for uncovering Windows-related security flaws. These tools provide detailed insight into your Windows systems and provide information that you might not otherwise get from all-in-one assessment tools :

- Metasploit for exploiting vulnerabilities that such tools as Nexpose and Qualys discover to obtain remote command prompts, add users, setup remote backdoors, and much more
- NetScan Tools Pro for port scanning, ping sweeps, and share enumeration
- Soft Perfect Network Security Scanner for port scanning and share enumeration
- TCP View to view TCP and UDP session information
- Winfo for null session enumeration to gather such configuration information as security policies, local user accounts, and shares

Gathering Information about Your Windows Vulnerabilities

When you assess Windows vulnerabilities, start by scanning your computers to see what the bad guys can see.

System scanning : A few straightforward processes can identify weaknesses in Windows systems.

Testing : Start gathering information about your Windows systems by running an initial port scan:

- Run basic scans to find which ports are open on each Windows system: Scan for TCP ports with a port scanning tool, such as NetScan Tools Pro.

The NetScan Tools Pro results reveal several potentially vulnerable ports open on a Windows 7 system, including those for DNS (UDP port 53), the ever-popular and easily hacked NetBIOS (port 139); and SQL Server (UDP 1434).

2. Perform OS enumeration (such as scanning for shares and specific OS versions) by using an all-in-one assessment tool, such as LanGuard.

3. Determine potential security vulnerabilities. This is subjective and might vary from system to system, but what you want to look for are interesting services and applications and proceed from there.

3.   NetBIOS

You can gather Windows information by poking around with NetBIOS (Network Basic Input /Output System) functions and programs. NetBIOS allows applications to make networking calls and communicate with other hosts within a LAN.

These Windows NetBIOS ports can be compromised if they aren't properly secured :

- UDP ports for network browsing :
  - Port 137 (NetBIOS name services, also known as WINS)
  - Port 138 (NetBIOS datagram services)

- TCP ports for Server Message Block (SMB) :
  - Port 139 (NetBIOS session services, also known as CIFS)
  - Port 445 (runs SMB over TCP/IP without NetBIOS)

- Hacks

  The hacks described in the following two sections can be carried out on unprotected systems running NetBIOS.

☞ Unauthenticated enumeration

When you are performing your unauthenticated enumeration tests, you can gather configuration information about the local or remote systems two ways :

- Using all-in-one scanners, such as LanGuard or Nexpose

– Using the nbtstat program that's built in to Windows (nbtstat stands for NetBIOS over TCP/IP Statistics)

7.2.2 Understanding Linux Vulnerabilities

The Vulnerabilities and attacks against Linux are creating business risks in a growing number of organizations especially e-commerce companies, network and IT/security vendors, and cloud service providers that rely on Linux for many of their systems, including their own products. When Linux systems are hacked, the victim organizations can experience the same side effects as their Windows-using counter parts, including:

– Leakage of sensitive information

– Cracked passwords

– Corrupted or deleted databases

– Systems taken completely offline

1. Choosing Tools

You can use many Linux-based security tools to test your Linux systems. Some are much better than others. I often find that my Windows-based commercial tools do as good a job as any. My favourite are as follows :

a. **Kali Linux** toolset on a bootable DVD or .iso image file

b. **LanGuard** for port scanning, OS enumeration, and vulnerability testing

c. **NetScan Tools Pro** for port scanning, OS enumeration, and much more

d. **Nexpose** for detailed port scanning, OS enumeration, and vulnerability testing

e. **Nmap** for OS fingerprinting and detailed port scanning

f. **Nessus** for OS fingerprinting, port scanning, and vulnerability testing

2. Gathering Information about Your Linux Vulnerabilities

You can scan your Linux-based systems and gather information from both outside (if the system is a publicly-accessible host) and inside your network. That way, you can check what the bad guys see from both directions.

A. System scanning

o Linux services called daemons are the programs that run on a system and serve up various services and applications for users.

o Internet services, like as the Apache web server (httpd), telnet (telnetd), and FTP (ftpd), often give away too much information about the system, including software versions, internal IP addresses, and usernames. This information could allow hackers to exploit a known weakness in the system.

o TCP and UDP small services, such as echo, daytime, and chargen, are often enabled by default and don't need to be.

– The vulnerabilities inherent in your Linux systems depend on what services are running. You can perform basic port scans to glean information about what's running.

– The NetScan Tools Pro many potentially vulnerable services on this Linux system, including the confirmed services of SSH, HTTP, and HTTPS

7.3 Applications Hacking Messaging Systems

7.3.1 Vulnerabilities

– The proliferation and business dependence on e-mail, just about anything is fair game. Ditto with VoIP. It's downright scary what people with ill intent can do with it.

– With messaging systems, one underlying weaknesses is that many of the supporting protocols weren't designed with security in mind especially those developed several decades ago when security wasn't nearly the issue it is today.

– The funny thing is that even modern-day messaging protocols or at least the implementation of the protocols are still susceptible to serious security problems. Furthermore, convenience and usability often outweigh the need for security.

Many attacks against messaging systems are just minor nuisances; others can inflict serious harm on your information and your organization's reputation. Malicious attacks against messaging systems include the following :

o Transmitting malware

o Crashing servers

o Obtaining remote control of workstations

o Capturing information while it travels across the network

o Perusing e-mails stored on servers and workstations

o Gathering messaging-trend information via log files or a network analyzer that can tip off the attacker about conversations between people and organizations (often called traffic analysis or social network analysis)

o Capturing and replaying phone conversations

o Gathering internal network configuration information, such as hostnames and IP addresses

7.3.2 E-Mail Attacks- E-Mail Bombs

Recognizing and Countering E-Mail Attacks

The following attack exploit the most common e-mail security vulnerabilities will seen. The good point is that you can eliminate or minimize most of them to point where your information is not at risk. Some of these attacks require basic hacking methodologies :

Gathering public information, scanning and enumerating your systems, and finding and exploiting vulnerabilities. Others can be carried out by sending email or capturing network traffic.

E-mail bombs

E-mail bombs attack by creating denial of service (DoS) conditions against your e-mail software and also even your network and Internet connection by taking up a large amount of bandwidth and, sometimes, requiring large amounts of storage space.

E-mail bomb scan crash a server and provide unauthorized administrator access yes, even with the today's seemingly endless storage capacities.

i. Attachments

An attacker can create an attachment-overload attack by sending hundreds or thousands of e-mails with very large attachments to one or more recipients on your network.

Attacks using e-mail attachments

Attachment attacks have a couple of goals.

- **The whole e-mail server might be targeted for a complete interruption of service with these failures :**

  o **Storage overload:** Multiple large messages can quickly fill the total storage capacity of an e-mail server. If the messages aren't automatically deleted by server or manually deleted by individual user accounts, the server will be unable to receive new messages.

  o **Bandwidth blocking:** An attacker can crash your e-mail service or bring it to the crawl by filling the incoming Internet connection with junk. Even if your system automatically identifies and discards obvious attachment attacks, the bogus messages eat resources and delay processing of valid messages.

- **An attack on a single e-mail address** can have serious consequences if the address is for an important user or group.

ii. Connections

- A hacker can send huge number of e-mails simultaneously to addresses in your e-mail system. Malware that is present on your network can do same thing from inside your network if there is an open Simple Mail Transfer Protocol (SMTP) relay on your network.

- These connection attack scan cause the server to give up on servicing any inbound or outbound TCP requests.

- This situation can lead to the complete server lockup or crash, often resulting in condition in which the attacker is allowed administrator or a root access to system.

iii. Attacks using floods of e-mails

An attack using flood of e-mails is often carried out in spam attacks and the other denial of service attempts.

Automated e-mail security controls

You can implement the following countermeasures as an additional layer of security for your e-mail systems :

1. **Tarpitting :** Tarpitting detect inbound messages destined for the unknown users. If your e-mail server supports tarpitting, it can help prevent spam or the DoS attacks against your server. If predefined threshold is exceeded say, more than 100messages in one minute the tarpitting function effectively shuns traffic from sending IP address for a period of time.

2. **E-mail firewalls :** The E-mail firewalls and the content filtering applications from vendors like as Symantec and the Barracuda Networks can go a long way towards preventing various e-mail attacks. These tools protect practically every aspect of an e-mail system.

3. **Perimeter protection :** Although not e-mail-specific, several firewall and the IPS systems can detect various e-mail attacks and shut off the attacker in real time. This can come in handy during an attack.

4. **CAPTCHA :** Using CAPTCHA on web-based e-mail forms can help minimize the impact of automated attacks and lessen your chances of e-mail flooding and denial of service even when you're performing seemingly benign web vulnerability scans.

7.3.3 Banners

- When hacking an e-mail server, a hacker's first order of business is performing a basic banner grab to see whether he can discover what e-mail server software is running.

- This is one of the most critical tests to find out what the world knows about your SMTP, POP3, and IMAP servers.
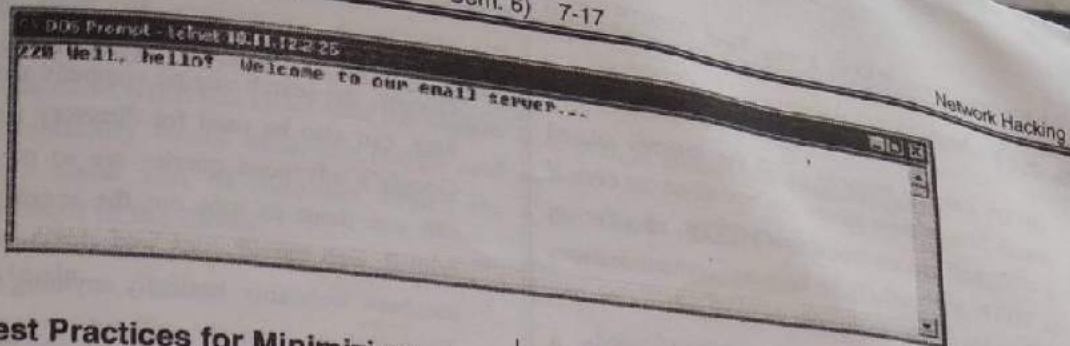
1. Gathering information

- Figure shows the banner displayed on an e-mail server when a basic telnet connection is made on port 25 (SMTP). To do this, at a command prompt, simply enter **telnet ip or_hostname_of_your_ server 25**. This opens a telnet session on TCP port 25.


```
Select DOS Prompt - telnet 10.11.12.2 25
220 Generic SMTP Server v1.0a Ready
-
```
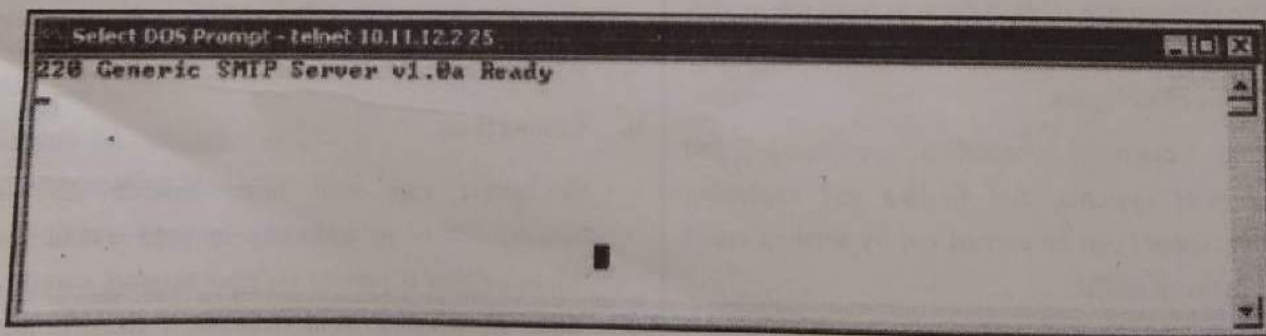
An SMTP banner showing server version information

- The e-mail software type and the server version are often very obvious and give hackers some ideas about possible attacks, especially if they search a vulnerability database for known vulnerabilities of that software version. Figure shows the same e-mail server with its SMTP banner changed from the default

Emerging Trends in Com. & Infor. Tech. (MSBTE - Sem. 6)   7-17

Network Hacking

```
DOS Prompt - telnet 10.11.12.2 25
220 Well, hello! Welcome to our email server...
```

7.3.4 Best Practices for Minimizing e-Mail Security Risks

The following countermeasures help keep messages as secure as possible :

☞ **Software solutions**

The right software can neutralize many threats:

1. **Use anti-malware software on e-mail server** better, the e-mail gateway to prevent malware from reaching e-mail clients. Cloud-based e-mail systems such as those offered by Google and Microsoft often have such protection built in. Using malware protection on your clients is a given.

2. **Apply the latest operating system and e-mail server security patches consistently and after any security alerts are released.**

3. **Encrypt (where's it reasonable).** You can use S/MIME or PGP to encrypt sensitive messages or use e-mail encryption at desktop level or server or email gateway. Better yet , you can also use TLS via thePOP3S, IMAPS, and the SMTPS protocols. The best option may be to use an e-mail security appliance or cloud service that supports sending and receiving of encrypted e-mails via a web browser over HTTPS.

4. **Make it policy for users not to open unsolicited e-mails or any attachments, especially those from unknown senders, and create ongoing awareness sessions and other reminders.**

5. **Plan for users who ignore or forget about the policy of not opening unsolicited e-mails and attachments.**

7.4 Web Applications

- The Websites and web applications are common targets for attack because they are everywhere and often open for anyone to poke and prod. Basic websites used for marketing, contact information, document downloads, and so on are especially easy forbad guy to play around with.

- Commonly-used web platforms like as WordPress and also related content management systems are especially vulnerable to attack because of their presence and also lack of testing and patching.

- For criminal hackers, websites that provide the front end to complex applications and databases that store valuable information, like as credit card and also Social Security numbers, are especially attractive.

- This is where the money is, both literally and figuratively.

Choosing Your Web Security Testing Tools

- Good web security testing tools can help ensure that you get the most from your work. As with many things in life, I find that you get what you pay for when it comes to testing for web security holes.

- These are my favourite web security testing tools:

i. **Acunetix Web Vulnerability Scanner** for all-in-one security testing, including a port scanner and an HTTP sniffer

ii. **AppSpider** for all-in-one security testing including excellent capabilities for authenticated scanning

iii. **Web Developer** for manual analysis and manipulation of web pages

7.4.1   Web Vulnerabilities

- (HTTP) make up majority of all the Internet related attacks. Most of these attacks can be carried out even if a HTTP traffic is encrypted (via HTTPS, also known as HTTP over SSL/TLS) because communications medium has nothing to do with these attacks.

- The security vulnerabilities actually lie within a websites and the applications themselves or the web server and browser software that the systems run on and communicate with.

- Many attacks against websites and the applications are just minor nuisances and also might not affect sensitive information or system availability.

- However, some attacks can be wreakhavoc on your systems, putting sensitive information at risk and even placing your organization out of the compliance with state, federal, and the international information privacy as well as security laws and regulations.

7.4.2   Directories Traversal and Countermeasures, Database System

☞ **Directory traversal**

- Directory traversal is a really basic weakness, but it can turn up interesting sometimes sensitive information about a web system. This attack involves browsing a site and looking for clues about the server's directory structure and sensitive files that might have been loaded intentionally or unintentionally.

- Perform the following tests to determine information about your website's directory structure :

i.   Crawlers

A spider program, like as the free HTTrack Website Copier ,can crawl your site to look for every publicly accessible file. To use HTTrack, simply load it, give your project a name, tell HTTrack which website(s) to mirror, and after a few minutes, possibly hours , you will have everything that's publicly accessible on the site stored on your local drive in

c:\My Web Sites.

ii.   Google

Google, the search engine company that many love to hate, can also be used for directory traversal. In fact, Google's advanced queries are so powerful that you can use them to root out the sensitive information, critical web server files and directories, credit card numbers, webcams basically anything that Google has discovered on your site without having to mirror your site and sift through everything manually. It is already sitting there in Google's cache waiting to be viewed.

- The following are a couple of advanced Google queries that you can enter directly into Google search field:

1. **site:hostname keywords :** This query searches for any keyword you list, like as SSN, confidential, credit card, and so on. An example would be:

   site:www.principlelogic.com speaker

2. **filetype:file-extension site:hostname :** This query searches for specific file types on a specific website, like as doc, pdf, db, dbf, zip, and so many These file types might contain sensitive information. An example would be:

   filetype:pdf site:www.principlelogic.com

Other advanced Google operators include the following :

1. **all in title** searches for keywords in the title of a web page.

2. **in url** searches for keywords in the URL of a web page.

3. **related** finds pages similar to this web page.

4. **link** shows other sites that link to this web page.

7.4.3   Database Vulnerabilities

- The Database systems, such as Microsoft SQL Server, MySQL, and Oracle, have lurked behind a scenes, but their value and their vulnerabilities have finally come to the fore front.

- Yes, even the mighty Oracle that was once claimed to be unhackable is susceptible to exploits similar to its competition.

With the slew of regulatory requirements governing database security, hardly any business can hide from the risks that lie within because practically every business (large and small) uses some sort of database either in-house or hosted in the cloud.

1. Choosing tools

As with wireless networks, operating systems, and so on, you need good tools if you're going to find the database security issues that count. The following are my favourite tools for testing database security:

i. **Advanced SQL Password Recovery** for cracking Microsoft SQL Server passwords

ii. **Cain and Abel** for cracking database password hashes

iii. **Nexpose** for performing in-depth vulnerability scans

iv. **SQLPing3** for locating Microsoft SQL Servers on the network, checking for blank passwords for the 'sa' account (the default SQL Server system administrator), and performing dictionary password cracking attacks

You can also use exploit tools, such as Metasploit, for your database testing.

2. Finding databases on the network

- The first step in discovering database vulnerabilities is to figure out where they're located on your network.

- It sounds funny, but many network admins I've met aren't even aware of various databases running in their environments.

- This is especially true for the free SQL Server Express database software editions that anyone can download and run on your network.

3. Scanning databases for vulnerabilities

As with operating systems and web applications, some database-specific vulnerabilities can be rooted out only by using the right tools. I use Nexpose to find such issues as :

- Buffer overflows
- Privilege escalations

- Password hashes accessible through default / unprotected accounts
- Weak authentication methods enabled

7.4.4 Best Practices for Minimizing Database Security Risk

Keeping your databases secure is actually pretty simple if you do the following :

- Run your databases on dedicated servers (or workstations, where necessary).
- Check the underlying operating systems for security vulnerabilities.
- Ensure that your databases fall within the scope of patching and system hardening.
- Require strong passwords on every database system. Most enterprise-ready databases such as Oracle and SQL Server allow you to use domain authentication(such as Active
- Directory or LDAP) so you can just tie-in your existing domain policy and user accounts and not have to worry about managing a separate set.
- Use appropriate file and share permissions to keep prying eyes away.
- De-identify any sensitive production data before it's used in non-production environments such as development or QA.
- Check your web applications for SQL injection and related input validation vulnerabilities.
- Use a network firewall, such as those available from Fortinet or Cisco and database-specific controls, such as those available from Imperva and Idera
- Perform related database hardening and management using a tool such as Microsoft Security Compliance Manager
- Run the latest version of database server software. The new security features in SQL Server 2012 and SQL Server 2016 are great advancements toward better database security.

...A SACHIN SHAH Venture

▶▶ 7.5 Multiple Choice Questions for Online Exam

Q. 1 _____ are the foundation for most technical security issues in your information systems.

(a) Network infrastructure vulnerabilities

(b) Physical infrastructure vulnerabilities

(c) Both a and b

(d) None of this

Ans. : (A)

Q. 2 An attacker can launch a _____ attack, which can take down your Internet connection or your entire network.

a. Virus   b. Denial of service (DoS)

c. worms   d. Malicous

Ans : (B)

Q. 3 A _____ can set up back-door access into your network

a. hacker   b. attacker

c. system   d. none of the above

Ans. : (A)

Q. 4 A _____ shows you what's what on your network by scanning the network to see what's alive and working.

a) port scanner   b) network

c) host   d) system

Ans. : (A)

Q. 5 _____ provide basic views of how the network is laid out.

a) Host   b) Port scanners

c) Application   d) Operating system

Ans. : (B)

Q. 6 A _____ of all your network subnets and hosts is a good way to find out which hosts are alive and kicking on the network.

a) ping sweep   b) ICMP

c) both   d) address

Ans. : (A)

Q. 7 A ping sweep is when you ping a range of addresses using _____

a) Network packet

b) Internet Control Message Protocol (ICMP) packets

c) UDP packet

d) None of the above

Ans. : (B)

Q. 8 _____ tells Nmap to perform a ping scan.

a) -sP   b) -n   c) -T   d) -T4

Ans. : (A)

Q. 9 _____ tells Nmap not to perform name resolution.

a) -sP   b) -n   c) -T   d) -T4

Ans. : (B)

Q. 10 The port scanner sends _____ requests to the host or range of hosts you set it to scan.

a) TCP SYN   b) PORT SYN

c) HOST SYN   d) none of the above

Ans. : (A)

Q. 11 The port scanner waits for from the available _____.

a) host   b) network

c) address   d) service.

Ans. : (A)

Q. 12 _____ This scan creates a half-open TCP connection with the host, possibly evading IPS systems and logging.

a) Connect   b) UDP scan

c) SYN Stealth   d) FIN Stealth

Ans. : (C)

Q. 13 _____ is a very nice all-in-one commercial tool for gathering general network information.

a) NetScanTools Pro   b) SYN stealth

c) connect   d) ping sweeping

Ans. : (A)

Q. 14 utilities for SNMP enumeration

a) NetScanTools Pro and Essential NetTools
b) Free Windows GUI-based Getif
c) Free Windows text-based SNMPUTIL
d) All of the above

Ans. : (B)

Q. 15 Telnet protocol is used to establish a connection to

a) TCP port number 21
b) TCP port number 22
c) TCP port number 23
d) TCP port number 24

Ans. : (C)

Q. 16 A _____ is a tool that allows you to look into a network and analyse datago.ing across the wire for network optimization, security, and/or troubleshooting purposes

a) network analyser
b) system analyser
c) operation analyser
d) none of the above

Ans. : (A)

Q. 17 Attackers can use _____ running on your network to make their systems appear as your system or another authorized host on your network.

a) MAC (media access control)
b) ARP (Address Resolution Protocol)
c) Both a and b
d) None of the above

Ans. : (B)

Network Hacking

Q. 18 ARP spoofing is used during _____ attacks.

a) Host
b) man-in-the-middle (MITM)
c) Cain and Abel
d) none of the above

Ans. : (B)

Q. 19 _____ attacks are among the most common hacker attacks.

a) Denial of service (DoS)
b) MAC spoofing
c) TCP spoofing
d) None of the above

Ans. : (A)

Q. 20 Wireless local area networks or Wi-Fi specifically, the ones based on IEEE _____ standard are increasingly being deployed into both business and home networks.

a) 802.11   b) 803.11
c) Both a and b   d) None of the above

Ans. : (A)

Q. 21 Wireless vulnerabilities are in implementation of the _____ standard.

a) 802.11   b) 802.1
c) 803.11   d) none of the above

Ans : (A)

Q. 22 _____ for gathering NetBIOS name table information.

a) nbtstat   b) netstat
c) net   d) none of the above

Ans. : (A)

Q. 23 _____ View to view TCP and UDP session information.

a) TCP   b) LAN
c) ARP   d) none of the above.

Ans. : (A)

Q. 24 _____ called daemons are the programs that run on a system and serve up various services and applications for users.

a) Linux services

b) IP services

c) telnet services

d) none of the above

Ans. : (A)

Q. 25 Malicious attacks against messaging systems include:

a) Transmitting malware

b) Crashing servers

c) Obtaining remote control of workstations

d) None of the above

Ans. : (A)

Q. 26 _____ attack by creating denial of service (DoS) conditions against your e-mail software

a) DoS

b) E-mail bombs

c) internet 2

d) none of the above

Ans. : (B)

Q. 27 A hacker can send huge number of e-mails simultaneously to addresses in your ___

a. e-mail system

b. Operating system

c. network system

d. none of the above

Ans. : (A)

Q. 28 _____ detect inbound messages destined for the unknown users.

a) Tarpitting

b) Email boom

c) SMTP

d) none of the above

Ans. : (A)

Q. 29 Using ___ on web-based e-mail forms can help minimize the impact of automated attacks.

a) CAPTCHA

b) SMTP

c) POP3

d) TCP

Ans. : (A)

Q. 30 The _____ are common targets for attack.

a) host and port

b) poke and prod

c) Websites and web applications

d) none of the above

Ans. : (C)

Q. 31 Which of the following tools are used for footprinting? (Choose 3 answers.)

a) Whois

b) Sam Spade

c) NMAP

d) SuperScan

e) Nslookup

Ans. : Options A, B, E.

Explanation : Whois, Sam Spade, and nslookup are all used to passively gather information about a target. NMAP and SuperScan are host and network scanning tools.

Q. 32 Banner grabbing is an example of what?

a) Passive operating system fingerprinting

b) Active operating system fingerprinting

c) Footprinting

d) Application analysis

Ans. : (A)

Explanation : Banner grabbing is not detectible; therefore it is considered passive OS fingerprinting.

Q. 33 What is the proper command to perform and NMAP SYN scan every 5 minutes?

a) nmap -ss - paranoid

b) nmap -Ss -paranoid

c) nmap -Ss -fast

d) namp -Ss -sneaky

Ans. : (B)

Explanation : The command nmap -sS - paranoid performs a SYN scan every 300 seconds or 5 minutes.

Q. 34 _____ is a weakness that can be exploited by attackers.

a) System with Virus

b) System without firewall

c) System with vulnerabilities

d) System with strong password

Ans. : (c)

Explanation : In cyber-security, a system having vulnerabilities is defined as the weakness in a system that can be exploited by cyber-criminals and attackers for their own benefit. For this, they use special tools and techniques in order to crack into the system through the vulnerabilities.

Q. 35 Risk and vulnerabilities are the same things.

a) True   b) False

Ans. : (b)

Explanation : Risk and vulnerability cannot be used interchangeably. Risk can be defined as the potential of an impact that can grow from exploiting the vulnerability. There is some vulnerability that doesn't possess risk, known as "Vulnerabilities without risk".

Q. 36 Which of them is not a wireless attack?

a) Eavesdropping   b) MAC Spoofing

c) Wireless Hijacking   d) Phishing

Ans. : (d)

Explanation : Wireless attacks are malicious attacks done in wireless systems, networks or devices. Attacks on Wi-Fi network is one common example that general people know. Other such sub-types of wireless attacks are wireless authentication attack, Encryption cracking etc.

Q. 37 What type of attack uses a fraudulent server with a relay address?

a) NTLM

b) NetBIOS

b) MITM

d) SMB

Ans. : (B)

Explanation : MITM (Man in the Middle) attacks create a server with a relay address. It is used in SMB relay attacks.

Q. 38 What is the purpose of a Denial of Service attack ?

a) Exploit a weakness in the TCP/IP stack

b) To execute a Trojan on a system

c) To overload a system so it is no longer operational

d) To shutdown services by turning them off

Ans. : (C)

Explanation : DoS attacks force systems to stop responding by overloading the processing of the 40system.

Q. 39 What are some of the most common vulnerabilities that exist in a network or system ?

a) Changing manufacturer, or recommended, settings of a newly installed application.

b) Additional unused features on commercial software packages.

c) Utilizing open source application code

d) Balancing security concerns with functionality and ease of use of a system

Ans. : (B)

Explanation : Linux is an open source code and considered to have greater security than the commercial Windows environment. Balancing security. Ease of use and functionality can open vulnerabilities that already exist.

Manufacturer settings, or default settings, may provide basic protection against hacking threats, but need to change to provide advance support. The unused features of application code provide an excellent opportunity to attack and cover the attack. commercial Windows environment. Balancing security. Ease of use and functionality can open vulnerabilities that already exist. Manufacturer settings, or default settings, may provide basic protection against hacking threats, but need to change to provide

advance support. The unused features of application code provide an excellent opportunity to attack and cover the attack.

Q. 40 What is the sequence of a TCP connection?

a) syn-ack-fin   b) syn-syn ack-ack

c) syn-ack   d) syn-syn-ack

Ans. : (B)

Explanation : A three-handed connection of TCP will start with a SYN packet followed by a SYN-ACK packet. A final ACK packet will complete the connection.

Chapter Ends...

□□□