SMVS
Page No.
Date : / /

Information Security Concept

* E-Commerce Security :

=> E-Commerce refers to a all the transaction that can be do over the internet.

Security is a important part of perform any types of transaction using the computer network.

=> E-Commerce Security Requirement :

1 Confidentiality : All the information should not be accessible to an unauthorized system or user.

2 Integrity : Information should not be altered during its transmission over the network.

3 Availability : Information should available whenever ~~un~~authorized user want to access.

SMVS
Page No.
Date : / /

4 Authenticity: There should be system that can authenticate the user to access the authorized system.

5 Non-Repudiability: Once authorized user can perform any action that can not be change by user.

6 Encryption: Information should be encrypted and decrypted only by the authorized user.

7 Auditability: All the Data should be recorded or formated such a way that can audited for integrity requirement.

=> E-Commerce Security Measures:

1 Encryption: In E-Commerces system sender data can be encrypted using the key and that will be only decrypt using this key or different key.

2 Digital Signature: A Digital Signature ensure the authenticity of the E-commerce system data.

3 Security Certificate: Security Certificate is unique digital id used to verify the identity of website or E-commerce system.

* Computer Forensics:

=) Computer Forensics is the scientific discipline focused on investigating and analyzing digital devices.

This Process involves structured investigation methods.

=) Types:

1 Disk Forensics: Disk Forensics extract and analyze data from primary and secondary storage of computer.

2 Network Forensics: This Forensics Monitor and analyz the network

traffic to understand network-related problem.

3 Database Forensic: Focuses on examine and analyize the database with its metadata.

4 Malware Forensic: This Forensic Focuses on identify and analyzing malicious software.

5 Email Forensic: This Forensic recovere and analyze email communication.

6 Memory Forensic: This Forensic deals with system memory such as registers, cache and RAM.

7 Mobile Phone Forensic: This Forensic Focuses on examing and analyze the mobile phone data such as contacts, call logs, SMS etc.

SMVS
Page No.
Date : / /

=> Characteristics :

1 Identification : The First step is Computer Forensics involves identify the evidence present on digital device including personal computer, mobile device.

2 Preservation : Data must be isolated, secured and prevent from the unauthorized user to avoid tampering and create different copies of data.

3 Analysis : Forensics experts analyze and examine the data to uncover detail about what happed and How it happend.

4 Documentation : Forensics experts have to create proper document to trak the investigation process and required for further analysis.

5 Presentation : Forensics experts have to summerizing the evidence, explaning the method used and provide clear amount of investiga-tion's result.

SMVS
Page No.
Date : / /

* Digital Forensics Science with its Life cycle.

=> Digital Forensics Science is mainly focused on identification, analysis the digital information.

Digital Forensics is investigating the Digital devices or devices information.

The Forensics experts identification, collection, analysis and reporting the valuable digital information on digital devices.

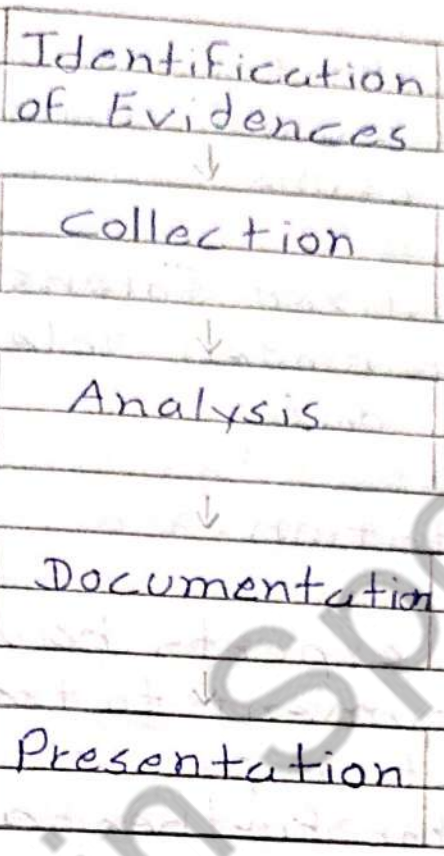
It consist 5 step to Investigation Digital Devices.

1 Identification of Evidences:

The Forensics experts identify storage media, hardware, operating system releted to the ~~gr~~ digital crime.

Experts collect all the devices evidence by conducting the

survey of environment



2 Collection:

Expert ensure that all identified digital evidence is preserved without alteration.

Create exact copies of digital evidence to analyz, keeping the Original data intact.

SMVS
Page No.
Date : / /

3 Analysis :

Analyze collected evidence to extract relevant information related to crime.

Use specialized forensic tools to uncover hidden, deleted or encrypted data.

4 Documentation :

Forensics experts have to create proper document to track the investigation process and required for further analysis.

Create detailed reports that explain the finding in a clear and structure manner.

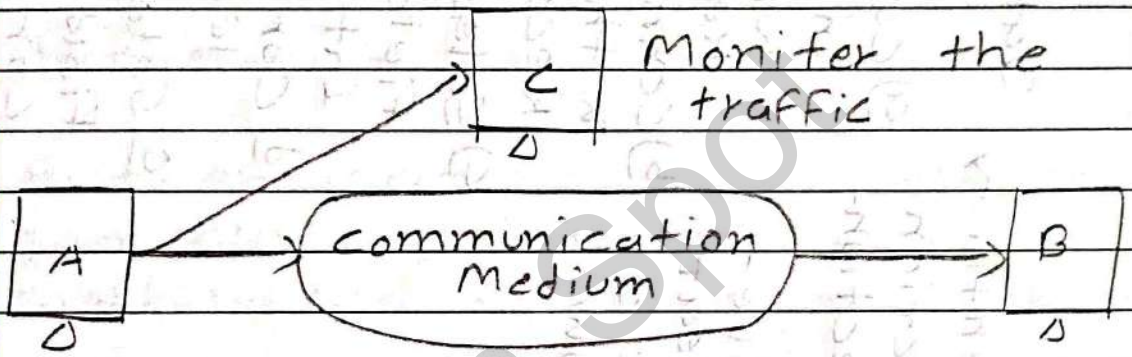
5 Presentation :

Forensics experts have to summerizing the evidence, explanation the method used and provide clear amount of investigation's result.

(ii) Traffic Analysis:

In this attack, attacker is moniter the Traffic of the two system.

In this attack, attacker is moniter the length of data, Frquency of data and also identify the two hosts.



* Explain Security Services in OSI Architecture.

=> Security Services is one of the most important part in Open System Interconnection Architecture.

Security Services is provides different types of services that can be work as a Protocol Layer in OSI Architecture.

Security Services is provided by

a system to given a specific kind of protection to system resources.

There are mainly Five Categories of Security Services.

- Security Services
  - Access Control
  - Authentication
    - a) Peer Entity
    - b) Data Origin
  - Data Confidentiality
    - a) Connection
    - b) Connection-less
    - c) Selective-Repeat
    - d) Traffic Flow
  - Non-Repudation
    - a) Non-Repudation Origin
    - b) Non-Repudation Destination
  - Data Integrity
    - a) Connection Integrity with Recovery
    - b) Conn. Int. without Recovery
    - c) Selective Field Conn.
    - d) Connection-less Int.
    - e) Selective Field Connection-less Int.

1 Access Control:

This services is use to protect the system resource from the unauthorized system.

Access Control only allow the authorized system to access the system resource.

2 Authentication:

Authentication is assures that communicating entity is authorized system or user.

(a) Peer Entity Authentication:

This Security Service that Verifies the identity of two system which both system do communication with each other.

(b) Data Origin:

This Security Services supports for the validation of the source of message that can send by Sender to the Receiver.

3 Non-Repudation:

This Service provides protection against the denial of any System for communication.

(a) Non-Repudation Origin:

This Service Assures that the message is send by the authorized system.

(b) Non-Repudation Destination:

This Service Assures that the message is receive by the authorized system.

4 Data Confidentiality:

Data Confidentiality is used to protect the sensitive information from the unauthorized system.

(a) Connection Confidentiality:

This Service Provides Protection of all the system User data on a connection.

(b) Connection-less Confidentiality:

This Service Provides Protection

of the system user data in a single data block.

(c) Selective-Field:

The Data Confidentiality of selective field is provide within the user data on a connection or in single data block.

(d) Traffic-Flow:

This services is provides protection in the information which is observation by traffic Flow.

5 Data Integrity:

This Security Service Assures that which data is ~~receied~~ received by a system that data is send by authorized system.

(a) Connection Integrity with Recovery:

This Security Service detects the any modification of any data within a entire data sequence with its recovery.

(b) Connection Integrity Without Recovery:

This Security Services detects the any modification of data within a entire data sequence, but it is not provides its data recovery.

(c) ~~Selective Field Communication~~

(c) Selective Field Connection Integrity:

This Security Services detects the any modification of data only within a selected user data Fields.

(d) Connection-Less:

This Security Services Provides the integrity of a single connection less data block and may detect the data modification.

(e) Selective Field Connection-less Integrity.

This Security Services detects the any modification of data within a selected user data Fields in Single connection less data block.

Page No.
Date :

* Explain Security Goals in Information Security.

=> This are the main Security Goals.

1 Information is always protect from being sttolen, attacked or altered.

2 Information can be follow this three goals.

- Protect the Confidentiality of the Information.
- Preserve the Integrity of the Information.
- Information must be available to authorized users.

3 For Protect the information we have to use CIA Tried.

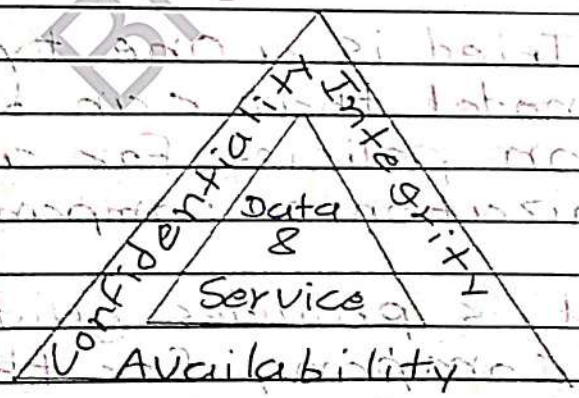
(ii) Confidentiality :

Confidentiality is used to protect the sensitive information from the unauthorized system.

Information must be provided only to the authorized users or system.

In Confidentiality, we have to use Data Confidentiality and Privacy for the protect the information.

Data Confidentiality assures that only authorized system can access the information and information is disclosed for every unauthorized system.



(iii) Integrity :

Integrity is used to ensures that every information is accurate, consistent and trust worthy.

Authorized user is always get unaltered and reliable information.

Integrity can be use Data Integrity and System Integrity.

Data Integrity assures that every information can be changed or altered by only authorized user.

System Integrity assures that every function in system is performs in an unimparied way.

(iii) Availability:

Availability assures that a system must be provide information when it is needed.

Information is always accesible to every authorized system even system facing failures.

Information or service is always work with the authorized users or system.

4 Authenticity : For access the information we have to verify the identity of users, systems and Prevent unauthorized access.

5 Accountability : In Information Security, we have to trace the actions of individuals or systems to be access specific entity.