ISM (UNIT-3)

Q.1 what are the various components of PKI?

Ans: public key infrastructure (PKI) include certification authorities, registration authorities, repositories, and archives.

1. Certification Authority (CA)

- The CA confirms the identities of parties sending and receiving electronic payments or other communications.
- Authentication is a necessary element of many formal communications between parties, including payment transactions.
- In most check-cashing transactions, a driver’s license with a picture is sufficient authentication.
- A personal identification number (PIN) provides electronic authentication for transactions at a bank automated teller machine (ATM).

2. Registration Authority (RA)

- A registration authority (RA) is an entity that is trusted by the CA to register for the identity of users to a CA.

3. Repository

- A repository is a database of active digital certificates for a CA system.
- The main business of the repository is to provide data that allows users to confirm the status of digital certificates for individuals and businesses that receive digitally signed messages.
- These message recipients are called relying parties. CAs post certificates and CRLs to repositories.

4. Archive

- An archive is a database of information to be used in settling future disputes.
- The business of the archive is to store and protect sufficient information to determine if a digital signature on an “old” document should be trusted.

Q.2 Explain mesh and hierarchical PKI structure

Ans: Most enterprises that deploy a PKI will choose either a “mesh” or a “hierarchical” architecture:

1. Mesh Architecture

- In mesh architecture independent CA issue certificate for each other.
- A relying party knows the public key of a CA one that issued his certificate.
- The relying party verifies certificate by verifying a certification path of certificates that leads from that trusted CA.
- CAs cross certify with each other, that is they issue certificates to each other, and combine the two in a crossCertificatePair**.**
- For example, Alice knows the public key of CA 3, while Bob knows the public key of CA 4. There are several certification paths that lead from Bob to Alice. The shortest requires Alice to verify Bob's certificate, issued by CA 4, then CA 4's certificate issued by CA 5 and finally CA 5's certificate, issued by CA 3. CA 3 is Alice's CA and she trusts CA 3 and knows its public key.

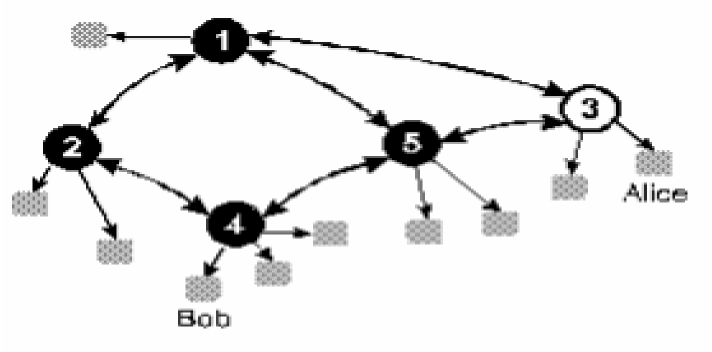


Figure: Mesh Infrastructure

2. Hierarchical Architecture

- In hierarchical architecture a "root" CA that issues certificates to subordinate CAs. These CAs may issue certificates to CAs below them in the hierarchy, or to users.
- In a hierarchical PKI, every relying party knows the public key of the root CA.
- Any certificate may be verified by verifying the certification path of certificates from the root CA.
- Alice verifies Bob's certificate, issued by CA 4, then CA 4's certificate, issued by CA 2, and then CA 2's certificate issued by CA 1, the root, whose public key she knows.

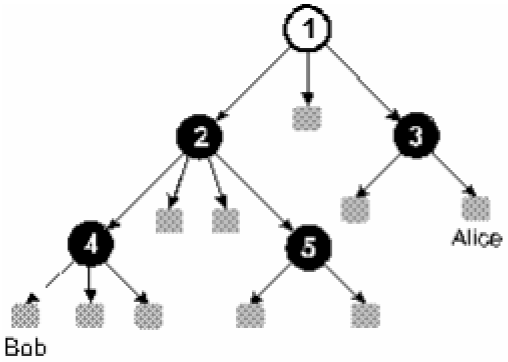
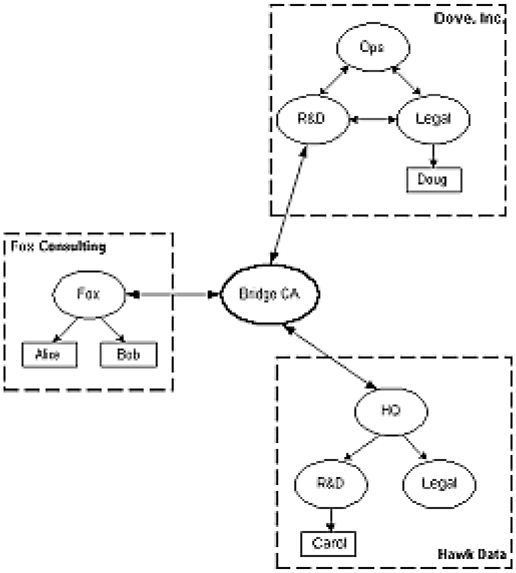


Figure: Hierarchical Infrastructure

Q.3 Explain bridge PKI architecture.

Ans:

- In bridge PKI architecture we introduce a new CA called **a Bridge CA**, whose establish relationships with enterprise PKIs.
- Unlike a mesh CA, the Bridge CA does not issue certificates directly to users. Unlike a root CA in a hierarchy, the Bridge CA is not intended for use as a trust point.
- All PKI users consider the Bridge CA an intermediary.
- The Bridge CA establishes peer-to-peer relationships with different enterprise PKIs. These relationships can be combined to form a bridge of trust connecting the users from the different PKIs.
- If the trust domain is implemented as a hierarchical PKI, the Bridge CA will establish a relationship with the root CA.
- If the domain is implemented as a mesh PKI, the bridge will establish a relationship with only one of its CAs that CAs called as principal CA.
- In Figure, the Bridge CA has established relationships with three enterprise PKIs.
- The first is Bob's and Alice's CA, the second is Carol's hierarchical PKI, and the third is Doug's mesh PKI.
- None of the users trusts the Bridge CA directly.
- Alice and Bob trust the CA that issued their certificates; they trust the Bridge CA because the Fox CA issued a certificate to it.
- Carol's trust point is the root CA of her hierarchy; she trusts the Bridge CA because the root CA issued a certificate to it.
- Doug trusts the CA in the mesh that issued his certificate; he trusts the Bridge CA because there is a valid certification path from the CA that issued him a certificate to the Bridge CA.



Q.4 Explain the two basic data structures used in PKIs

Ans: Two basic data structures are used in PKIs are the public key certificate and the certificate revocation lists.

1. X.509 Public Key Certificates

- The X.509 public key certificate format [IETF 01] has evolved into a flexible and powerful mechanism.
- It may be used to convey a wide variety of information. Much of that information is optional, and the contents of mandatory fields may vary as well.
- There are ten common fields: six mandatory and four optional.
- The mandatory fields are: the serial number, the certificate signature algorithm identifier, the certificate issuer name, the certificate validity period, the public key, and the subject name.
- There are four optional fields: the version number, two unique identifiers, and the extensions.
    - **Version:** The version field describes the syntax of the certificate.
    - **Serial number:** The serial number is an integer assigned by the certificate issuer to each certificate and it must be unique.
    - **Signature**: The signature field indicates which digital signature algorithm was used to protect the certificate.
    - **Issuer:** The issuer field contains the X.500 distinguished name of the TTP that generated the certificate.
    - **Validity:** The validity field indicates the dates on which the certificate becomes valid and the date on which the certificate expires.
    - **Subject**: The subject field contains the distinguished name of the holder of the private key corresponding to the public key in this certificate. The subject may be a CA, a RA.

- **Subject public key information:** The subject public key information field contains the subject's public key, optional parameters, and algorithm identifier.
- **Issuer unique ID and subject unique ID:** These fields contain identifiers, and only appear in version 2 or version 3 certificates.
- **Extensions:** This optional field only appears in version 3 certificates. If present, this field contains one or more certificate extensions.
- **Subject type**: This field indicates whether a subject is a CA or an end entity.

2. Certificate Revocation Lists (CRLs)

- CRLs is a mechanism that provide a status update for the certificates they have issued.
- The CRL is protected by a digital signature of the CRL issuer.
- If the signature can be verified, CRL users know the contents have not been tampered with since the signature was generated.
- The CRL contains the following fields:
    - **Version:** The optional version field describes the syntax of the CRL.
    - **Signature:** The signature field contains the algorithm identifier for the digital signature algorithm used by the CRL issuer to sign the CRL.
    - **Issuer:** The issuer field contains the X.500 distinguished name of the CRL issuer.
    - **This update:** The this-update field indicates the issue date of this CRL.
    - **Next update:** The next-update field indicates the date by which the next CRL will be issued.
    - **Revoked certificates:** The revoked certificates structure lists the revoked certificates. The entry for each revoked certificate contains the certificate serial number, time of revocation, and optional CRL entry extensions.
    - **CRL Extensions**: The CRL extensions field is used to provide additional information about the whole CRL. Again, this field may only appear if the version is v2.

Q.5 Write a note on physical architecture of PKI.

Ans:

- In physical architecture PKI components be implemented on separate systems, that is, the CA on one system, the RA on a different system, and directory servers on other systems.
- CA system contain sensitive data so that should be place behind an additional organizational firewall is recommended so that it is protected both from the Internet and from systems in the organization itself.

- If distinct organizations wish to access certificates from each other, their directories will need to be made available to each other and possibly to other organizations on the Internet.
- However, some organizations will use the directory server for much more than simply a repository for certificates.
- The directory server may contain sensitive data to the organization and thus the directory may be too sensitive to be made publicly available.
- A typical solution would be to create a directory that contains only the public keys or certificates, and to locate this directory at the border of the organization - this directory is referred to as a **border directory**. A likely location for the directory would be outside the organization's firewall.
- The main directory server located within the organization's protected network.
- Users within the organization would use the main directory server, whereas other systems and organizations would access only the border directory.
- When a user in organization A wishes to send encrypted e-mail to a user in organization B, user A would then retrieve user B's certificate from organization B's border directory, and then use the public key in that certificate to encrypt the e-mail.

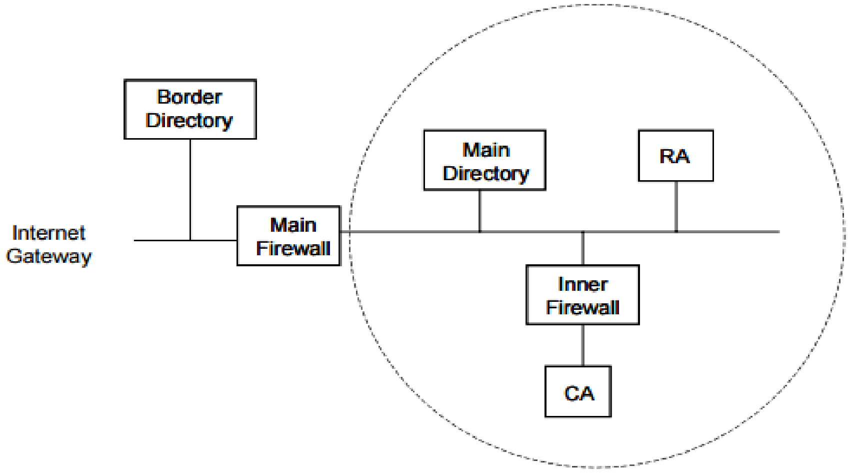


Figure: PKI Physical Topology

Q.6 List the most commonly logged types of information and their potential benefits.

Ans: There are four types of logged types of information are as follows:

1. Client requests and server responses

- It’s helpful in reconstructing sequences of events and determining their apparent outcome.
- If the application logs successful user authentications, it is usually possible to determine which user made each request.
- Some applications can perform highly detailed logging, such as e-mail servers recording the sender, recipients, subject name, and attachment names for each e-mail; Web servers recording each URL requested and the type of response provided by the server; and business applications recording which financial records were accessed by each user.

2. Account information

- Account information such as successful and failed authentication attempts, account changes and use of privileges.
- It can be used to identify who has used the application and when each person has used it.

3. Usage information

- It includes number of transactions occurring in a certain period and the size of transactions.
- This can be useful for certain types of security monitoring.

4. Significant operational actions

- Significant operational actions such as application startup and shutdown, application failures, and major application configuration changes.
- This can be used to identify security compromises and operational failures.

Q.7 State & explain the common log management infrastructure functions

Ans: The following items describe common log management infrastructure functions:

1. General

- **Log parsing** is extracting data from a log so that the parsed values can be used as input for another logging process.
- **Event filtering** is the suppression of log entries from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.
- In **event aggregation**, similar entries are consolidated into a single entry containing a count of the number of occurrences of the event.

2. Storage

- **Log rotation** is closing a log file and opening a new log file when the first file is considered to be complete. The primary benefits of log rotation are preserving log entries and keeping the size of log files manageable.
- **Log archival** is retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server.
- **Log compression** is storing a log file in a way that reduces the amount of storage space needed for the file without altering the meaning of its contents.
- In **log normalization**, each log data field is converted to a particular data representation and categorized consistently.
- **Log file integrity** checking involves calculating a message digest for each file and storing the message digest securely to ensure that changes to archived logs are detected.

3. Analysis

- **Event correlation** is finding relationships between two or more log entries.
- **Log viewing** is displaying log entries in a human-readable format.
- **Log reporting** is displaying the results of log analysis.

4. Disposal

- **Log clearing** is removing all entries from a log that precede a certain date and time. Log clearing is often performed to remove old log data that is no longer needed on a system because it is not of importance or it has been archived.

Q.8 what are the various types of network & host based security software.

Ans: Common types of network-based and host based security software include the following:

1. Antimalware Software

- The most common form of antimalware software is antivirus software, which typically records all instances of detected malware, file and system disinfection attempts.
- Antispyware software and other types of antimalware software (e.g., rootkit detectors) are also common sources of security information.

2. Intrusion Detection and Intrusion Prevention Systems

- Intrusion detection and intrusion prevention systems record detailed information on suspicious behavior and detected attacks, as well as any actions intrusion prevention systems performed to stop malicious activity in progress.

3. Remote Access Software

- Remote access is often granted and secured through virtual private networking (VPN).
- VPN systems typically log successful and failed login attempts, as well as the dates and times each user connected and disconnected, and the amount of data sent and received in each user session.

4. Web Proxies

- Web proxies are intermediate hosts through which Web sites are accessed.
- Web proxies make Web page requests on behalf of users, and they cache copies of retrieved Web pages to make additional accesses to those pages more efficient.

5. Vulnerability Management Software

- Vulnerability management software, which includes patch management software and vulnerability assessment software, typically logs the patch installation history and vulnerability status of each host, which includes known vulnerabilities and missing software updates.

6. Authentication Servers

- Authentication servers, including directory servers and single sign-on servers, typically log each authentication attempt, including its origin, username, success or failure, and date and time.

7. Routers

- Routers may be configured to permit or block certain types of network traffic based on a policy.

8. Firewalls

- Like routers, firewalls permit or block activity based on a policy; however, firewalls use much more sophisticated methods to examine network traffic.
- Firewalls can also track the state of network traffic and perform content inspection. Firewalls tend to have more complex policies and generate more detailed logs of activity than routers.

9. Network Quarantine Servers

- Network Quarantine Servers check each remote host’s security posture before allowing it to join the network.

- Network quarantine servers log information about the status of checks, including which hosts were quarantined and for what reasons.

Q.9 what are the challenges in log management?

Ans: There are three categories of log challenges are as follows:

1. Log Generation and Storage

- In a typical organization, many hosts' OSs, security software, and other applications generate and store logs. This complicates log management in the following ways:

  i. Many Log Sources

  - Logs are located on many hosts throughout the organization, necessitating log management to be performed throughout the organization.
  - Also, a single log source can generate multiple logs—for example, an application storing authentication attempts in one log and network activity in another log.

  Ii. Inconsistent Log Content

  - Each log source records certain pieces of information in its log entries, such as host IP addresses and usernames.
  - For efficiency, log sources often record only the pieces of information that they consider most important.
  - This can make it difficult to link events recorded by different log sources because they may not have any common values recorded.

  iii. Inconsistent Timestamps

  - Each host that generates logs typically references its internal clock when setting a timestamp for each log entry.
  - If a host's clock is inaccurate, the timestamps in its logs will also be inaccurate. This can make analysis of logs more difficult.
  - For example, timestamps might indicate that event a happened 45 seconds before event B, when event A actually happened two minutes after event B.

  Iv. Inconsistent Log Formats

  - Many of the log source types use different formats for their logs, such as comma-separated or tab-separated text files, databases, syslog.

  - Some logs are designed for humans to read, while others are not; some logs use standard formats, while others use proprietary formats.

2. Log Protection

- Logs contain records of system and network security, they need to be protected from breaches of their confidentiality and integrity.
- For example, logs capture sensitive information such as users’ passwords and the content of e-mails.
- Logs that are secured improperly in storage or in transit might also be susceptible to intentional and unintentional alteration and destruction.
- Organizations also need to protect the availability of their logs.
- Many logs have a maximum size, such as storing the 10,000 most recent events, or keeping 100 megabytes of log data.
- When the size limit is reached, the log might overwrite old data with new data or stop logging altogether, both of which would cause a loss of log data availability.

3. Log Analysis

- Within most organizations, network and system administrators have been responsible for performing log analysis.
- Administrators who are responsible for performing log analysis often receive no training on doing it also, administrators often do not receive tools that are effective at automating much of the analysis process.
- Many of these tools are particularly helpful in finding patterns that humans cannot easily see, such as correlating entries from multiple logs that relate to the same event.
- Log analysis is often treated as reactive—something to be done after a problem has been identified through other means—rather than proactive.

Q.10 Explain log management infrastructure.

Ans:

- A log management infrastructure consists of the hardware, software, networks, and media used to generate, transmit, store, analyze, and dispose of log data.
- Most organizations have one or more log management infrastructures.
- A log management infrastructure typically comprises the following three tie**rs:**

  1. Log Generation

  - The first tier contains the hosts that generate the log data.
  - Some hosts run logging client applications or services that make their log data available through networks to log servers in the second tier.

2. Log Analysis and Storage

- The second tier is composed of one or more log servers that receive log data or copies of log data from the hosts in the first tier
- Servers that receive log data from multiple log generators are sometimes called collectors or aggregators.
- Log data may be stored on the log servers themselves or on separate database servers.

3. Log Monitoring

- The third tier contains consoles that may be used to monitor and review log data and the results of automated analysis.
- Log monitoring consoles can also be used to generate reports.
- In some log management infrastructures, consoles can also be used to provide management for the log servers and clients.

Q.11 what are the various functions of log management infrastructure?

Ans:

- Log management infrastructures typically perform several functions that assist in the storage, analysis, and disposal of log data.
- The following items describe common log management infrastructure functions:

1. General

- **Log parsing** is extracting data from a log so that the parsed values can be used as input for another logging process.
- **Event filtering** is the suppression of log entries from analysis, reporting, or long-term storage because their characteristics indicate that they are unlikely to contain information of interest.
- In **event aggregation**, similar entries are consolidated into a single entry containing a count of the number of occurrences of the event.

2. Storage

- **Log rotation** is closing a log file and opening a new log file when the first file is considered to be complete. The primary benefits of log rotation are preserving log entries and keeping the size of log files manageable.
- **Log archival** is retaining logs for an extended period of time, typically on removable media, a storage area network (SAN), or a specialized log archival appliance or server.

- **Log compression** is storing a log file in a way that reduces the amount of storage space needed for the file without altering the meaning of its contents.
- In **log normalization**, each log data field is converted to a particular data representation and categorized consistently.
- **Log file integrity** checking involves calculating a message digest for each file and storing the message digest securely to ensure that changes to archived logs are detected.

3. Analysis

- **Event correlation** is finding relationships between two or more log entries.
- **Log viewing** is displaying log entries in a human-readable format.
- **Log reporting** is displaying the results of log analysis.

4. Disposal

- **Log clearing** is removing all entries from a log that precede a certain date and time. Log clearing is often performed to remove old log data that is no longer needed on a system because it is not of importance or it has been archived.

Q.12 Write short note on Syslog Security.

Ans:

- Syslog was developed at a time when the security of logs was not a major consideration.
- Shortcoming of most syslog implementations is that they cannot use encryption to protect the integrity or confidentiality of logs in transit.
- As the security of logs has become a greater concern, several implementations of syslog have been created that place a greater emphasis on security.
- Most have been based on a proposed standard, RFC 3195, which was designed specifically to improve the security of syslog.
- RFC 3195 can support log confidentiality, integrity, and availability through several features, including the following:

  1. Reliable Log Delivery
  - Several syslog implementations support the use of Transmission Control Protocol (TCP) in addition to UDP.
  - TCP is a connection-oriented protocol that attempts to ensure the reliable delivery of information across networks.
  - Using TCP helps to ensure that log entries reach their destination.

  2. Transmission Confidentiality Protection

- RFC 3195 recommends the use of the Transport Layer Security (TLS) protocol to protect the confidentiality of transmitted syslog messages.
- TLS can protect the messages during their entire transit between hosts.

3. Transmission Integrity Protection and Authentication

- RFC 3195 used message digest algorithm to integrity protection and authentication if they are desired.
- RFC 3195 recommends the use of MD5.
- Federal agencies should use SHA instead of MD5 for message digests whenever feasible.

Q.13 Explain the Need for Log Management

Ans:

- Log management can benefit an organization in many ways. It helps to ensure that computer security records are stored in sufficient detail for an appropriate period of time.
- Routine log reviews and analysis are beneficial for identifying security incidents, policy violations and operational problems shortly after they have occurred, and for providing information useful for resolving such problems.
- The following is a listing of key regulations, standards, and guidelines that help define organizations’ needs for log management:

The following is a listing of key regulations, standards, and guidelines that help define organizations’ needs for log management:

1. Federal Information Security Management Act of 2002 (FISMA)

- FISMA emphasizes the need for each Federal agency to develop, document, and implement an organization-wide program to provide information security for the information systems that support its operations and assets.

2. Gramm-Leach-Bliley Act (GLBA)

- GLBA requires financial institutions to protect their customers’ information against security threats.
- Log management can be helpful in identifying possible security violations and resolving them effectively.

3. Health Insurance Portability and Accountability Act of 1996 (HIPAA)

- HIPAA includes security standards for certain health information.
- NIST SP 800-66, An Introductory Resource Guide for Implementing the HIPAA Security Rule, lists HIPAA-related log management needs.

4. Sarbanes-Oxley Act (SOX) of 2002

- Although SOX applies primarily to financial and accounting practices.
- SOX can be supported by reviewing logs regularly to look for signs of security violations, including exploitation.

Q.14 List & Explain the classic categories of malware.

Ans: Malware has become the greatest external threat to most hosts, causing damage and requiring extensive recovery within most organizations.
The following are the classic categories of malware:

1. Viruses

- A virus self-replicates by inserting copies of itself into host programs or data files.
- Viruses are often triggered through user interaction, such as opening a file or running a program.
- Viruses can be divided into the following two subcategories:

  i. Compiled Viruses
  - A compiled virus is executed by an operating system.
  - Types of compiled viruses include file infector viruses, which attach themselves to executable programs.
  - Boot sector viruses, which infect the master boot records of hard drives.
  - Multipartite viruses, which combine the characteristics of file infector and boot sector viruses.

  ii. Interpreted Viruses
  - Interpreted viruses are executed by an application.
  - Within this subcategory, macro viruses take advantage of the capabilities of applications' macro programming language to infect application documents and document templates.
  - Scripting viruses infect scripts that are understood by scripting languages processed by services on the OS.

2. Worms

- A worm is a self-replicating, self-contained program that usually executes itself without user intervention.
- Worms are divided into two categories:

  i. Network Service Worms
  - A network service worm takes advantage of a vulnerability in a network service to propagate itself and infect other hosts.

  ii. Mass Mailing Worms
  - A mass mailing worm is similar to an email-borne virus but is self-contained, rather than infecting an existing file.

3. Trojan Horses

- A Trojan horse is a self-contained, non-replicating program that, while appearing to be benign, actually has a hidden malicious purpose.

- Trojan horses either replace existing files with malicious versions or add new malicious files to hosts.

4. Malicious Mobile Code

- Malicious mobile code is software with malicious intent that is transmitted from a remote host to a local host and then executed on the local host, typically without the user's explicit instruction.
- Popular languages for malicious mobile code include Java, ActiveX, JavaScript, and VBScript.

5. Blended Attacks

- A blended attack uses multiple infection or transmission methods.
- For example, a blended attack could combine the propagation methods of viruses and worms.

Q.15 List& Explain the popular attacker tools.

Ans:

- Attacker tools allow attackers to have unauthorized access to or use of infected hosts and their data, or to launch additional attacks.
- Popular types of attacker tools are as follows:

  1. Backdoors
  - A backdoor is a malicious program that listens for commands on a certain TCP or UDP port.
  - Most backdoors allow an attacker to perform a certain set of actions on a host, such as acquiring passwords or executing arbitrary commands.

  2. Keystroke Loggers
  - A keystroke logger monitors and records keyboard use.
  - Some require the attacker to retrieve the data from the host, whereas other loggers actively transfer the data to another host through email, file transfer, or other means.

  3. Rootkits
  - A rootkit is a collection of files that is installed on a host to alter its standard functionality in a malicious and stealthy way.

  4. Web Browser Plug-Ins
  - A web browser plug-in provides a way for certain types of content to be displayed or executed through a web browser.
  - Malicious web browser plug-ins can monitor all use of a browser.

  5. E-Mail Generators
  - An email generating program can be used to create and send large quantities of email, such as malware and spam, to other hosts without the user's permission or knowledge.

  6. Attacker Toolkits
  - Many attackers use toolkits containing several different types of utilities and scripts that can be used to probe and attack hosts, such as packet sniffers, port scanners, vulnerability scanners, password crackers, and attack programs and scripts.

Q.16 what are the recommended capabilities of an antivirus software?

Ans: Antivirus software providing protection through the following recommended capabilities:

- Scanning critical host components such as startup files and boot records.
- Watching real-time activities on hosts to check for suspicious activity, Antivirus software should be configured to perform real-time scans of each file as it is downloaded, opened, or executed, which is known as on-access scanning.
- Monitoring the behavior of common applications, such as email clients, web browsers, and instant messaging software.
- Scanning files for known malware. Antivirus software on hosts should be configured to scan all hard drives regularly to identify any file system infections.
- Identifying common types of malware as well as attacker tools.
- **Disinfecting files**, which refers to removing malware from within a file, and quarantining **files**, which means that files containing malware are stored in isolation for future disinfection or examination. Disinfecting a file is generally preferable to quarantining it because the malware is removed and the original file restored.

Q.17 Write a note on sandboxing.

- Sandboxing refers to a security model where applications are run within a sandbox.
- A controlled environment that restricts what operations the applications can perform and that isolates them from other applications running on the same host.
- In a sandbox security model, typically only authorized “safe” operations may be performed within the sandbox.
- The sandbox prohibits applications within the sandbox from performing any other operations.
- Sandboxing provides several benefits in terms of malware incident prevention and handling.
- The sandbox also restricts access to system resources, such as memory and the file system, to keep the sandbox’s applications isolated from the host’s other applications.
- The sandboxing environment—the isolation—can further reduce the impact of the malware by restricting what information and functions the malware can access.
- Another benefit of sandboxing is that the sandbox itself can be reset to a known good state every time it is initialized.

Q.18 Explain malware incident response life cycle in detail.

Ans:

- The incident response life cycle has four major phases: preparation, detection and analysis, containment/eradication/recovery and post-incident activity.
- The initial phase of malware incident response involves policy, awareness activities, vulnerability mitigation, and security tools to reduce the number of malware incidents.

- Detection phase is necessary to alert the organization whenever incidents occur.
- Faster detection and handling can help reduce the number of infected hosts and the damage done.
- For each incident, the organization should act appropriately, based on the severity of the incident, to mitigate its impact by containing it, eradicating infections, and ultimately recovering from the incident.
- The organization may need to jump back to the detection and analysis phase during containment, eradication, and recovery—for example, to check for additional infections that have occurred since the original detection was done.
- After an incident has been handled, the organization should issue a report that details the cause and cost of the incident and the steps the organization should take to prevent future incidents and to prepare more effectively to handle incidents that do occur.

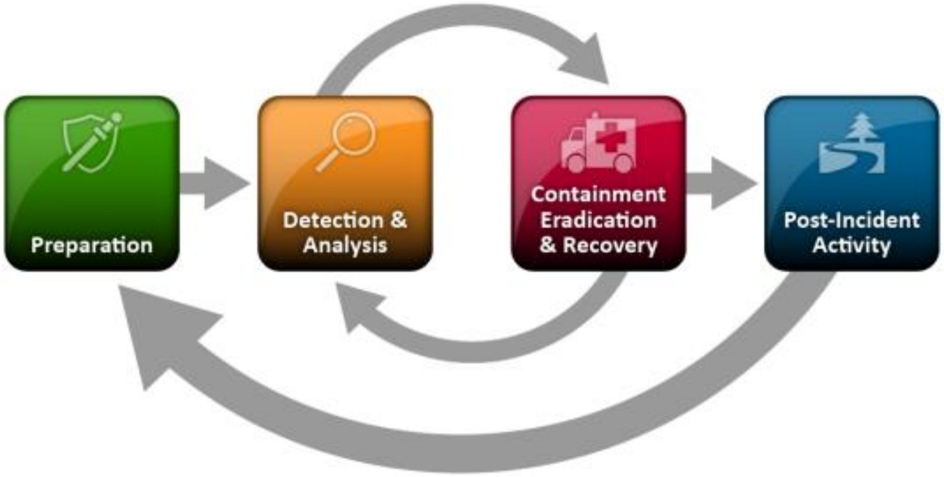


Figure: incident response lifecycle

Q.19 List and explain the major component of containment of malware.
Ans:

- Malware incident containment has two major components:
- **Stopping the spread of malware** and **preventing further damage to hosts**.
- In addressing an incident, it is important for an organization to decide which methods of containment to employ initially, early in the response.
- Organizations should have strategies and procedures in place for making containment-related decisions.
- Containment strategies should support incident handlers in selecting the appropriate combination of containment methods based on the characteristics of a particular situation.
- Specific containment-related recommendations include the following:
  - It can be helpful to provide users with instructions on how to identify infections and what measures to take if a host is infected.

  - If malware cannot be identified and contained by updated antivirus software, organizations should be prepared to use other security tools to contain it.
  - Organizations should be prepared to shut down or block services used by malware to contain an incident and should understand the consequences of doing so.
  - Organizations should be prepared to place additional temporary restrictions on network connectivity to contain a malware incident, such as suspending Internet access or physically disconnecting hosts from networks.

Q.20 Explain the three main categories of patch and vulnerability metrics.

Ans: There are three main categories of patch and vulnerability metrics: susceptibility to attack, mitigation response time, and cost.

1. Measuring a System's Susceptibility to Attack

- An organization's susceptibility to attack can be approximated by several measurements.
- An organization can measure the number of patches needed, the number of vulnerabilities, and the number of network services running on a per system basis.
- These measurements should be taken individually for each computer within the system, and the results then aggregated to determine the system-wide result.
- Both raw results and ratios (e.g., number of vulnerabilities per computer) are important.
- The raw results help reveal the overall risk a system faces because the more vulnerabilities, unapplied patches, and exposed network services that exist, the greater the chance that the system will be penetrated.

2. Mitigation Response Time

- It is also important to measure how quickly an organization can identify, classify, and respond to a new vulnerability and mitigate the potential impact within the organization.
- Response time has become increasingly important, because the average time between a vulnerability announcement and an exploit being released has decreased.
- There are three primary response time measurements that can be taken:

  i. Response Time for Vulnerability and Patch Identification
  - This metric measures how long it takes the PVG to learn about a new vulnerability or patch.
  - This measurement should be taken on a sampling of different patches and vulnerabilities and should include all of the different resources the PVG uses to gather information.

  Ii. Response Time for Patch Application
  - This metric measures how long it takes to apply a patch to all relevant IT devices within the system.
  - This measurement should be taken on patches where it is relatively easy for the PVG to verify patch installation.

Iii. Response Time for Emergency Configuration Changes

- This metric applies in situations where a vulnerability exists that must be mitigated but where there is no patch.
- In such cases the organization is forced to make emergency configuration changes that may reduce functionality to protect the organization from exploitation of the vulnerability.

3. Cost

- There are four main cost measurements that should be taken:

  i. Cost of the Patch and Vulnerability Group
  - When justifying the cost of the PVG to management, it will be useful to estimate the amount of system administrator labor that has been saved by centralizing certain functions within the PVG.

  ii. Cost of System Administrator Support
  - As organizations improve in their overall efforts to measure the real cost of IT security, measuring the cost of patch and vulnerability measurement with respect to system administrator time will become easier.

  iii. Cost of Enterprise Patch and Vulnerability Management Tools
  - This measurement includes patching tools, vulnerability scanning tools, vulnerability Web portals, vulnerability databases, and log analysis tools.
  - Organizations should first calculate the purchase price and annual maintenance cost for each software package. Organizations should then calculate an estimated annual cost that includes software purchases and annual maintenance.
  - If the software will be regularly upgraded, the upgrade price should be used instead of the purchase price.

    Estimated annual cost = Sum of annual maintenance for each product + Sum of (purchase price or upgrade price / life expectancy in years) for each product

Q.21 what is The Patch and Vulnerability Group & what are their duties?
Ans:

- The PVG should be a formal group that incorporates representatives from information security and operations.
- These representatives should include individuals with knowledge of vulnerability and patch management, as well as system administration, intrusion detection, and firewall management.
- Personnel who already provide system or network administration functions, perform vulnerability scanning, or operate intrusion detection systems are also likely candidates for the PVG.
- The size of the group and the amount of time devoted to PVG duties will vary broadly across various organizations.
- Much depends on the size and complexity of the organization, the size and complexity of its network, and its budget.
- The duties of the PVG are as follows:

  1. Create a System Inventory

- The PVG should use existing inventories of the organization’s IT resources to determine which hardware equipment, operating systems, and software applications are used within the organization.

2. Monitor for Vulnerabilities, Remediation, and Threats

- The PVG is responsible for monitoring security sources for vulnerability announcements, patch and non-patch remediation, and emerging threats that correspond to the software within the PVG’s system inventory.

3. Prioritize Vulnerability Remediation.

- The PVG should prioritize the order in which the organization addresses vulnerability remediation.

4. Create an Organization-Specific Remediation Database

- The PVG should create a database of remediation that need to be applied to the organization.

5. Distribute Vulnerability and Remediation Information to Local Administrators

- The PVG is responsible for informing local administrators about vulnerabilities and remediation that correspond to software packages included within the PVG scope and that are in the organizational software inventory.

6. Perform Automated Deployment of Patches

- The PVG should deploy patches automatically to IT devices using enterprise patch management tools.

7. Configure Automatic Update of Applications Whenever Possible and Appropriate

- Many newer applications provide a feature that checks the vendor’s Web site for updates. This feature can be very useful in minimizing the level of effort required to identify, distribute, and install patches.

8. Vulnerability Remediation Training

- The PVG should train administrators on how to apply vulnerability remediation. In organizations that rely on end users to patch computers, the PVG must also train users on this function.

Q.22 what are the primary methods of remediation that can be applied to an affected system?

Ans: There are three primary methods of remediation that can be applied to an affected system:

1. Security Patch Installation

- Applying a security patch repairs the vulnerability, since patches contain code that modifies the software application to address and eliminate the problem.
- Patches downloaded from vendor Web sites are typically the most up-to date and are likely free of malicious code.

2. Configuration Adjustment

- Adjusting how an application or security control is configured can effectively block attack vectors and reduce the threat of exploitation.

- Common configuration adjustments include disabling services and modifying privileges, as well as changing firewall rules and modifying router access controls.

3. Software Removal

- Removing or uninstalling the affected software or vulnerable service eliminates the vulnerability and any associated threat.
- Determining how the system is used, removing unnecessary software and services.

Q.23 who are involved in log management planning? Explain their responsibilities.

Ans: Teams and individual roles often involved in log management include the following:

1. System and network administrators

- System and network administrators are usually responsible for configuring logging on individual systems and network devices, analyzing those logs periodically, reporting on the results of log management activities, and performing regular maintenance of the logs and logging software.

2. Security administrators

- Security administrators are usually responsible for managing and monitoring the log management infrastructures, configuring logging on security devices (e.g., firewalls, network based intrusion detection systems, antivirus servers), reporting on the results of log management activities.

3. Computer security incident response teams

- Computer security incident response teams use log data when handling some incident.

4. Application developers

- Application developers Application developers may need to design or customize applications so that they perform logging in accordance with the logging requirements and recommendations.

5. Information security officer

- Information security officer may oversee the log management infrastructures.

6. Chief information officers (CIO)

- Chief information officers (CIO) oversee the IT resources that generate, transmit, and store the logs.

7. Auditors

- Auditors may use log data when performing audits.

Q.24 what are the steps included in developing logging policies?

Ans:

1. Log generation

- Which types of hosts must or should perform logging.
- Which host components must or should perform logging.
- Which types of events each component must or should log.
- How frequently each type of event must or should be logged.

2. Log transmission

- Which types of hosts must or should transfer logs to a log management infrastructure.
- Which types of entries and data characteristics must or should be transferred from individual hosts to a log management infrastructure.
- How log data must or should be transferred.
- How frequently log data should be transferred from individual hosts to a log management infrastructure.

3. Log storage and disposal

- How often logs should be rotated.
- How the confidentiality, integrity, and availability of each type of log data must or should be protected while in storage.
- How long each type of log data must or should be preserved.
- How unneeded log data must or should be disposed of at both the system level and the infrastructure level.
- How much log storage space must or should be available at both the system level and the infrastructure level.

4. Log analysis

- How often each type of log data must or should be analyzed at both the system level and the infrastructure level.
- Who must or should be able to access the log data at both the system level and the infrastructure level and how such accesses should be logged.
- What must or should be done when suspicious activity or an anomaly is identified.
- How the confidentiality, integrity, and availability of the results of log analysis must or should be protected while in storage at both the system level and the infrastructure level and in transit.

Q.25 List and explain the components of key management infrastructure.

Ans: There are four components of key management infrastructure are as follows:

1. Central Oversight Authority

- The KMI's central oversight authority is the entity that provides overall KMI data synchronization and system security oversight for an organization or set of organizations.
- The central oversight authority coordinates protection policy and practices documentation.
- It serves as the source for common and system level information required by service agents.

2. Key Processing Facility

- Key processing services typically include one or more of the following:
  - Acquisition or generation of public key certificates
  - Initial generation and distribution of keying material
  - Maintenance of a database that maps user entities to an organization's certificate/key structure
  - Maintenance and distribution of compromise key lists (CKLs) and/or certificate revocation lists (CRLs)

3. Service Agents

- Service agents support organizations' KMIs as single points of access for other KMI nodes.
- All transactions initiated by client nodes are either processed by a service agent or forwarded to other nodes for processing.
- Service agents may provide registration, directory, and support for data recovery services as well as provide access to relevant documentation, such as policy statements and infrastructure devices.
- Service agents may also process requests for keying material (e.g., user identification credentials), and assign and manage KMI user roles and privileges.

4. Client Nodes

- Client nodes are interfaces for managers, devices, and applications to access KMI functions, including the requesting of certificates and other keying material.
- Client nodes provide interfaces to end user entities (e.g., encryption devices) for the distribution of keying material and for the generation of requests for keying material.

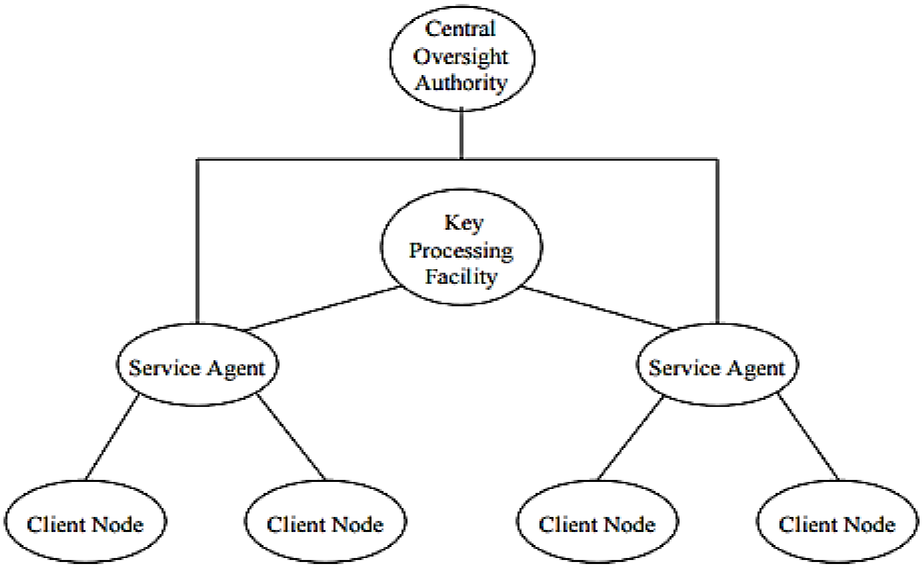


Figure: KMI Components

Q.26 Write a short note on key management policy.

Ans:

- A key management policy is a set of rules that are established to describe the goals, responsibilities, and overall requirements for the management of cryptographic keying material used to protect private or critical facilities, processes, or information.
- Key Management Policies (KMP) are implemented through a combination of security mechanisms and procedures.

- An organization uses security mechanisms (e.g. alarms, random number generators, encryption algorithms, and signature and authentication algorithms) as tools to implement a policy.
- The policy document or documents that comprise the KMP will include high-level key management structure and responsibilities, governing standards and guidelines, organizational dependencies and other relationships, and security objectives.
- The KMP is used to guide the development of KMPSs for each PKI CA or symmetric key management group that operates under its provisions.
- Auditors and accreditors will use the KMP as the basis for their reviews of PKI CA and/or symmetric key KMI operations.

Q.27 what are the security objectives of key management policy?
Ans: The security objectives should include the identification of:

- The nature of the information to be protected (e.g., financial transactions, confidential information, critical process data).
- The classes of threats against which protection is required (e.g., the unauthorized modification of data, replay of communications).
- The cryptographic protection mechanisms to be employed (e.g., message authentication, digital signature, and encryption).
- Protection requirements for cryptographic processes and keying material (e.g. confidentiality of keying material).
- Applicable statutes, and executive directives and guidance to which the KMI and its supporting documentation shall conform.

Q.30 List & explain the KMI components in detail.
Ans: Refer Question No: 25

Q.31 Write a short note on Key Management Policy.
Ans: Refer Question No: 26

Q.35 List various PKI data structures. Explain in short.
Ans: Refer Question no: 4

Q.36 what is the need for log management?
Ans: Refer Question no: 13

Q.37 what are the challenges in log management?
Ans: Refer Question no: 9

Q.38 Explain the tiers used in a log management infrastructure
Ans: Refer Question no: 10

Q.39 Define roles and responsibilities of the persons involved in log management.
Ans: Refer Question no: 23

Q.40 List and explain various forms of malware.
Ans: Refer Question no: 14

Q.41 List and explain the popular types of attacker tools.
Ans: Refer Question no: 15