Unit-3

Need for Physical Security :-

→ Physical security has emerged as important aspect of security.

→ Physical threat to a computer system could be result of loss of whole computer system, damage of hardware, damage to software, theft of computer system, Natural disaster like fire, flood, earthquake.

⊛ Acts of terrorism is also a threat to computer.

→ physical security of information security means its physical protection. This can be done by security workstation where monitoring can be done.

Physical security is a measure to protect computer system or the place where information system resources are placed.

Physical security covers :-

1. Access controls
2. Damage of Hardware
3. failure of supporting utilities.
4. Natural Disaster including fire, floods, earthquake etc
5. Vandalism.

Scanned by CamScanner

In other words, Physical security means protection of site, control centres, theft, vandalism, accidental damage, natural disaster.

→ It requires solid building, control centres, proper security, reliable power supplies, protection from intruder & preparedness in case of emergency.

Access controls includes

→ Role management (refers to user sides)

→ Rule management - (refers to Resource side that which resource is accessible to whom).

Disaster And control :- The equipment used in information system are sensitive to many factors such as power supply, cleaniness & environment.

factors :-

① Electrical Interruptions :- In many rural areas, power cut is a serious problem. Frequent power cut can have serious business impact Data may not be available at required time due to power cut.

Scanned by CamScanner

Measures:- (1) Use stabilizers to control voltage fluctuations.

(2) Use UPS with sufficient amount of batteries to have atleast 30 minute power backup.

(3) Install line filters to control voltage spikes.

(2) Earthquake:- An earthquake is shaking caused by sudden movements of rocks in earth's crust. Sometimes this can be extremely violent.

Measures:- (1) Keep computer system in safe buildings

(2) Do not keep devices near glass.

(3) Use antivibration devices to secure computer systems.

(3) Fire:- Electronic items were not manufactured made to be in High humidity & heat. The heat of fire can effect & melt any substrate if it gets not enough.

Measures:- (1) Keep fire extinguishers near computer systems.

(2) Proper training to staff

(3) Do not allow smoking near equipment.

Scanned by CamScanner

(4) Lightening :- It is a sudden electrostatic discharge during an electrical storm between ~~clouds~~ clouds or cloud & ground

measures :- 1. Install surge suppressors.
2. Use UPS for power supply without interruption

3.

(5) flood :- In case of flood, computer system may be destroyed.

measures :-
1. Use computer systems on some table or rack, means on same height from ground.
2. Preparedness in case of emergency.

(6) Liquid Leakage :- Leaking pipes may destroy computer system or data by destroying its chip or hardware

measures :- (1) Keep liquid proof covers
(2) Install water detector on structural floors.

(7) Environmental failures :- It may include air conditioning, humidity or water controls.

measures :- (1) Keep temperature at 10-25°C
(2) humidity levels should be 20-70%

Scanned by CamScanner

Basic Tenets of Physical Security :-

Basic tenets of Physical Security includes:-

1. Deterrence Methods
2. Intrusion detection & Electronic surveillance
3. Access control
4. Security personnel

(1) Deterrence Method :-

The aim of deterrence Method is to convince attacker that strong defense has been applied so it is hard to make successful attacks. This can be done by:-

→ Physical barrier (includes wall, fence or any vehicle barrier which if not prevent but can delay attacks. Access points should has physical security controls such as Security doors, shutters, grills etc.)

→ Natural surveillance (Space for information system should be in a manner that is visible to security personnel & authorized users so that intruder are unable to perform unauthorized activity without being seen).

→ Security lighting :- (It means close observation of people entering & exiting. It may include CCTVs (closed circuit television systems) or guard services.

Scanned by CamScanner

② Intrusion detection & Electronic surveillance

IDS are designed to detect unauthorized entry, identify its location & signals a req with an alarm.

→ It can be done by alarm systems / sensors / ~~vids~~ video surveillance.

→ Alarm system alerts security personnel in case of unauthorized access.

→ Motion sensors can detect unauthorised person.

→ Video surveillance can be done with CCTVs But it requires real time ~~usant~~ monitoring in order to caught intruders.

③ Access Controls :- Access to information system resources must always be provided only on "Need to know basis". It can be done by :-

- Mechanical access controls :- includes gates, doors, shutters, grills, locks.
- Electronic access control :- Controls user life cycle times, dates & individual access points.
- Policies :- made such as who is allowed to enter which area.

④ Security personnel :- Human Resources can be deployed at check points to make a security check so that only ~~out~~ authorised person can access. Security staffs can do patrolling, respond to alarms & monitor video

Scanned by CamScanner

Physical Entry Controls :- Physical entry (4)
control can be made by :-

1. Protection of secure areas.
2. Controlling visitors & outsiders.
3. care for journalist entry.
4. physical security of building & office premises
5. Locks.
6. safety from fire hazards.

⇒(1) Protection of secure Areas :- One has to make protection of secure areas in order to have safety & security.
measures :- (1) wearing of ID cards.
(2) Regular review of Policies of access rights.
(3) Regular audit of system.
(4) preparedness in case of emergency.
(5) maintanence of entry & exit detail of each visitor.
(6) The guard should be have emergency contact numbers in case of serious problem.

(2) Controlling Visitors & outsiders :-
outsiders should not be allowed to enter in rooms where confidential information is kept. Proper notice (mentioning which are areas where visitors are not allowed) should be pasted.. Visitors should be issued temporary passes after having

Scanned copy of their identity cards.
→ Policies should be clear whether visitors may use their cameras or not.
→ Visitor records should be maintained.

③ Care for Journalist or Media People Entry :- As people from media are always important, but without prior approval they may not be allowed to take photographs or video of any thing during their visit.
→ People from organisation should assist Journalist during their visit.

④ Physical Security of Building & office :-
IDS (intrusion detection system) should be installed as per policies of organisation
→ IDS should be maintained by inhouse team rather than outsourcing.
→ Important information systems or confidential information should be kept away from public access.
→ Entire premises or office building should be divided into different groups & they should be monitored through their respective incharges.

Scanned by CamScanner

(5) locks :- physical security is necessary to secure computer, networks, disk drives and electronic media.

→ work stations can be secured by an anchor pad which is a metal pad with locking rods.

(6) Safety from fire hazards :- All devices that use electricity have a potential to become dangerous, coupled with rapid strides in technology that has made computers system that can get very hot.

→ In most instances, safety devices built within computer system should provide adequate safety but there may be cases when due to unforeseen circumstances, a fire happen.

measures :- (1) Regular cleaning & maintenance of equipment.

(2) Do not expose computer equipment to water

(3) Cables used should not be damaged.

(4) fire proof products should be taken.

(5) fire security personnels / professionals should be engaged in physical securities of data centres & computer control centre

Scanned by CamScanner

Access Control

→ Access control provides protection against unauthorized access. This can be done through user identification & user authentication.

User Identification :- It is a logical entity used to identify a user on a system, software or within any IT environment.

User Authentication :- It is the process of proving that claimed identification is genuine. Proof of identification can be :-

1. PIN 2. Password 3. ID card
4. User's Biological characteristics verification.

Biometrics :- Biometric industry Guru Ben Miller has given following definition in 1987.

" Biometric technologies are automated methods of verifying or recognizing the identity of living person based on physical or behavioral characteristics ".

Biometrics (Greek word) → Bios, Metrikos → means life measurement.

Scanned by CamScanner

Biometric system is a reliable measure of security. (6)

Popular Biometric authentication systems are:-

1. finger Print
2. Iris
3. Retina
4. Voice Pattern
5. face Recognition
6. DNA (Processing time is long)
7. Palm
8. Hand Print
9. Gait Recognition (every person has a peculiar way of walking).

Why we use Biometric?

→ Convenient authentication
→ Increased need for strong authentication
→ Decreased cost
→ Increased government & industry adaptation
→ Increased accountability
→ Fraud detection.

How Biometric System works?

Biometric system works in 3 steps:-

1. Enrollment:- Before a user can begin using biometric system., he/she must complete an enrollment process. The user must provide his details depending upon Biometric technology used..

Scanned by CamScanner

(2) Usage:- When user wishes to access System, or building guarded with biom... the user authenticates according to procedure which could mean swiping a finger etc

(3) Update:- For type of biometrics that changes slowly over time eg facial Recognition system the biometric system may need to update

Characteristics of Biometric System:-

(1) Universality:- It means every person should have the particular (biometric used) characteristics eg:- finger print

(2) Uniqueness:- Which indicates that no two person should be same in terms of characteristics.

(3) Permanence:- It means characteristics should be invariant over time.

(4) Collectability:- The characteristic can be measured quantitavely.

(5) Performance:- It refers to achievable identification accuracy.

(6) Acceptability:- It is Acceptance Ratio, It indicates to what extent people are willing to accept Biometric System.

Scanned by CamScanner

(7) Circumvention:- Refers to how easily is to fool the system by fraud.

Storage Requirement:- Amount of information each party need to store

(9) Communication Requirement:- for authentication system, number & context size of messages that need to exchange.

(b) Computational Requirement:- Degree of Computation needs to be performed.

(11) Implementation Cost:- Associated implementation Cost eg:- special Hardware for biometric

(12) Cryptographic Primitives:- whether specialised cryptographic primitives need to be employed or standardised established primitives can be used.

Key Success factors for Biometric System

(1) Accuracy:- Accuracy is most critical characteristics of a biometrics identification verification system. If system can not accurately separate an authentic person from an imposer, it is of no use.

Scanned by CamScanner

There are 2 main issues :-
→ FRR (false Rejection Rate) Specificity
→ FAR (false acceptance Rate) Sensitivity

(1) FRR :- This Rate is generally expressed as percentage. It is Rate at which authentic persons are rejected as unidentified or unverified persons. It also known as Type 1 error.

⇒ Reverse situation is FAR (false acceptance Rate). FAR is Rate at which unenrolled or imposer person are accepted as authentic, enrolled person. by Biometric system. It is Type II error.

(2) Crossover Error Rate (CER) :- It is Rate at which FAR & FRR matches. It is also known as ERR (Equal Error rate). It is most important measure of Biometric accuracy.

(*) FNMR (false Non match Rate) is the probability that a user's template will be incorrectly judged to Not match his/her enrollment template.

(*) ERR is Rate at which FNMR is equal to FMR.

Scanned by CamScanner

(8) Speed & Throughput Rate :- Data processing capability of biometric system decides the speed (It is stated as how fast the accept or reject decision is taken).

(3) Acceptability by users :- This is related to social stigma attached to biometric system. given their nature & lack of awareness. social stigma like Eye rethna scanning requires users to trust that system will not damage their eyes.

(4) Uncooperative users may damage the biometric scanning equipment.

(*) All the persons in an organisation must be agreed upon the installation of biometric system.

(9) Reliability of Biometric System :- Biometric system should work in an accurate manner. Reliability is probability that a matcher system will correctly identified the mate.. Only authorized persons must be allowed to access & must reject others without breakdown its performance accuracy or speed.

Scanned by CamScanner

(5) Data storage Requirements :- Large size of biometric match templates, even with current ultra high speed processors, large data files take longer than small files to process.

* This is specially for biometric system that do full identification.

(6) Enrollment time in Biometric - In earlier time, biometric system had enrollment procedures requiring many steps taking minutes to complete.

* Accepted standard for enrollment time is 2 minute per person.

* Most of system available in market today meet this standard

(7) Uniqueness :- Biometric system must be based upon unique characteristics of the employees. Out of many physical characteristics 3 can be considered unique.

- fingerprint
- Retina of eye.
- Iris of eye.

Scanned by CamScanner

Benefits of Biometric System

Benefits of Biometric over traditional Authentication Methods :-

① Increased security :- Resources are accessible only to authorised users & are kept protected from unauthorised users.

* Passwords & PINs are easily guessed.
* Tokens can be stolen.
* Password & Pins can be shared.

But Biometric information can not be stolen or shared.

② Increased Convenience :- Password can be forgotten. No risk of remembering in Biometric. Biometric can offer greater convenience than system based on remembering multiple password.

③ Increased Accountability :- Given increased awareness of security issues in enterprise & in customer facing applications the need for strong auditing & reporting has grown more pronounced.

* Benefits of accountability apply primarily to enterprise, corporation & home user.

Scanned by CamScanner

(2) Benefits of Biometric in Identification :-
In identification system, biometric can still be used for security, convenience & accountability especially when they are deployed to a modest Number of users. However, identification systems are more often deployed in large scale environment.

(i) Fraud Detection :- Identification Systems are deployed to determine whether a person's biometric information exists more than once in a database.

⇒ By locating & identifying individuals who have already registered for a program or service, biometrics can reduce fraud eg:- Driving license.

(ii) Fraud Deterrence :- It is primary benefit of Biometric system in large scale identification system. It can be difficult to return a highly certain match against millions of existing biometric records.

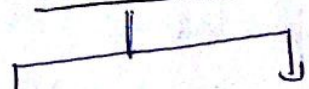
(*) If presence of biometric, can deter individual from attempting to enroll multiple times in public benefit or driver's license system then public agency has saved money & ensured integrity of its records.

Scanned by CamScanner

Criteria for Selection of Biometrics

The steps for selecting a biometric solution are :-

(1) Identify the selection Criteria :-



The process includes understanding the physical & logical environments, establishing physical environments such as size, weight. Then determine acceptable accuracy & rates of failure

(2) Identify the field of Possible Solution :- Closure analysis of requirements, features & bug budget should help you to get one or two type of biometric approaches that may work for you.

(3) Test Potential solution :- Get some user involved in the testing their observations & feedback may be more valuable than you may realize.

(4) Choose the Solution :- After you have tested some solution, you should be able to make a selection.

Scanned by CamScanner

Design issues in Biometric System

Steps of a Biometric System :-

① Sample Acquistion :- Biometric data is collected in this step using sensors.

② Feature Extraction :- The collected sample is transformed into the template

③ Quality Verification :- This step establishes a reference image or template by repeating the sample acquistion & feature extraction.

④ Template Storage :- Reference template are registered in data base.

⑤ Template Matching :- Compalison of real time input data is done with stored reference templates.

⑥ Decision :- Result of acceptance or rejection is declared.

⇒ Design Issues :-

① Storage & Protection of the Template :- Firstly it scans the images then store, & afterward it matches. depending on the design of biometric system, the matching process can be performed at different

Scanned by CamScanner

locations such as processor, local PC, remote (11)
server or on any portable medium. There are many different mode of protection & different combination to store reference template. The choice of optice the right configuration is clearly application dependent.

② Ensuring Accuracy of Biometric System

Steps :- (1) System Performance
(2) Communication Interface
(3) Decision step
(4) Template matching
(5) Case of Use
(6) Acquistion speed
(7) Processing speed.

③ Mode of operation of Biometric System :-

Design issues are not only to understand. but for which we need to define a clear policy.

Interoperability issues in Biometrics :-

The major concerned related to biometric are interoperability in cross application of biometrics. The ISO/IEC JTCI SC37 Committee has addressed the inter operability issues in various biometric systems.

Scanned by CamScanner

One important thing is standardization in order to enable the interoperability of Signature Systems, is the interchange format for storage & transfer of signature data. The whole feature set must allow interoperability at a feature level samples collected on different types of devices.

Why Standards?

The main motivation of biometric standard is to define requirements, formats & software specification enabling inter-operability between biometric systems, especially authentication system.

Standard organizations :-

1) **ISO/ANSI/X9 Committee, ISO (International Standard Organization)** :- is the most important international organization. The Biometric ISO standard have been defined in conjunction with IEC (International Electrochemical Commission)

→ ANSI (American National Standards Institute).

Scanned by CamScanner

is United States Technical Advisory Group focussed on information & data security.

(2) CBEFF :- Common biometric exchange file format was created by NIST & biometric Consortium. It defines a generic common set of data needed to support different biometric systems.

(3) ICAO :- The international Civil Aviation organization defines standards for Photographic scene & digital Requirement for facial & fingerprint images.

(4) ANSI/NIST/FBI :- have developed the standard ANSI/NIST - JTL for exchange & interopelability among different components or databases.

Cost of Biometrics :- Cost may vary between different technology. It may depend on :-

(1) System Architecture
(2) Type of Application
(3) Storage Requirement
(4) Means & technologies used for data Protection
(5) Databases used
(6) Security of system.

Scanned by CamScanner

Economic & Social Aspects of Bio

Economic Aspects :- Economic transactions are frequently taking place Now a days biometric technologies are storing Identific technology.. it helps in reducing fraud cases & helps consumes to make more efficient transactions

Economic Aspects are :-

① Concept of optimal Identity :- In this digital society, economic importance of identity is growing, but strongest ID protection is not necessarily the optimal one

② Negative implications of stronger Identifications There is no doubt that stronger identification help in reducing cases of errors & abuse but if found, they will be potentially more dangerous.

③ Interoperability is vital for market operation :- Some key players of biometric business may form a cluster that will not interopelate & leads to monopolization or dominance by them

Biometric-related IPRs threaten open competition :- The unregulated exploitation of IPR to aspects of biometrics can significantly reduce competition in Biometrics.

(5) Public Sector uptake will Shape the market :- The increased use of biometric of e-Governance or government projects may increase the trust in people's eye. It could be a key levels to ensure open & competitive markets, & rapid & socially productive's innovations.

Social Aspects :- The main social issues are :-

(1) Clarity of Purpose :- "function creep" is an important concern i.e technology & processes used for one purpose will be extended to other purposes (but not discussed / agreed upon at time of their implementation). It is important to be clear about what needs of application are & how biometrics will be able to achieve them.

Scanned by CamScanner

(2) Interoperability & equivalence of Pe... & process :- Process equivalence (i.e. Bi... procedures that are same everywhere) is extremely important as it impacts system performance.

(3) Human factors engineering, usability & social exclusion :- Human factors such as age, ethnicity, gender, diseases or disabilities ~~at~~ ought to be studied on a case-by-case basis. Research on usability & user friendliness of biometrics is still in progress.

(4) Element of trust :- Trust should be maintained between governments & citizens. But when government control is perceived as excessive, disproportionate & too efficient, an erosion of trust can appear.

Scanned by CamScanner

Legal challenges of Biometrics :-

Biometric technologies are set to play a big role in commercial security but firms must ensure that they do not fall foul of data protection or human rights law.

⇒ Legal challenges remain to use of biometric technologies by both public institutions & business.

⇒ Legal issues may include purpose to which information about individuals is collected & now it can then be used.

⇒ It also looks the ability to access information & redress inaccuracies & providing robust enough security.

Use of biometric brings with it important legal issues such as :-

① Remediation :- Refers to legal steps take to deal with fraudlent use of biometric such as identity fraud by altering biometr traits. Thus it will be important for policy & law to both address the prepetrator to identify fraud & induce system owners to create an environment that minimizes opportunity for misuse of biometric sampl

④ Reliability :- As Biometrics are deployed more broadly & in more contexts; a proper understanding of extent to which they gather & results they produce can be relied upon will be critical.

⑤ Privacy :- The human right act states that we are all entitled to respect for our private life. The use of biometric data must be fair & limited to specific purposes. It should be transparent that how & why information will be used & not going beyond this without prior agreement.

legal aspects can be summarized as :-

① Enabling legal Environment.
② Opacity / Transparency Rules implementation
③ Use of biometrics in law enforcement.

Scanned by CamScanner

Framework of Information Security :- (15)

An information security framework is a series of documented processes that are used to define policies & procedures around the implementation & management of information security controls in an enterprise environment.

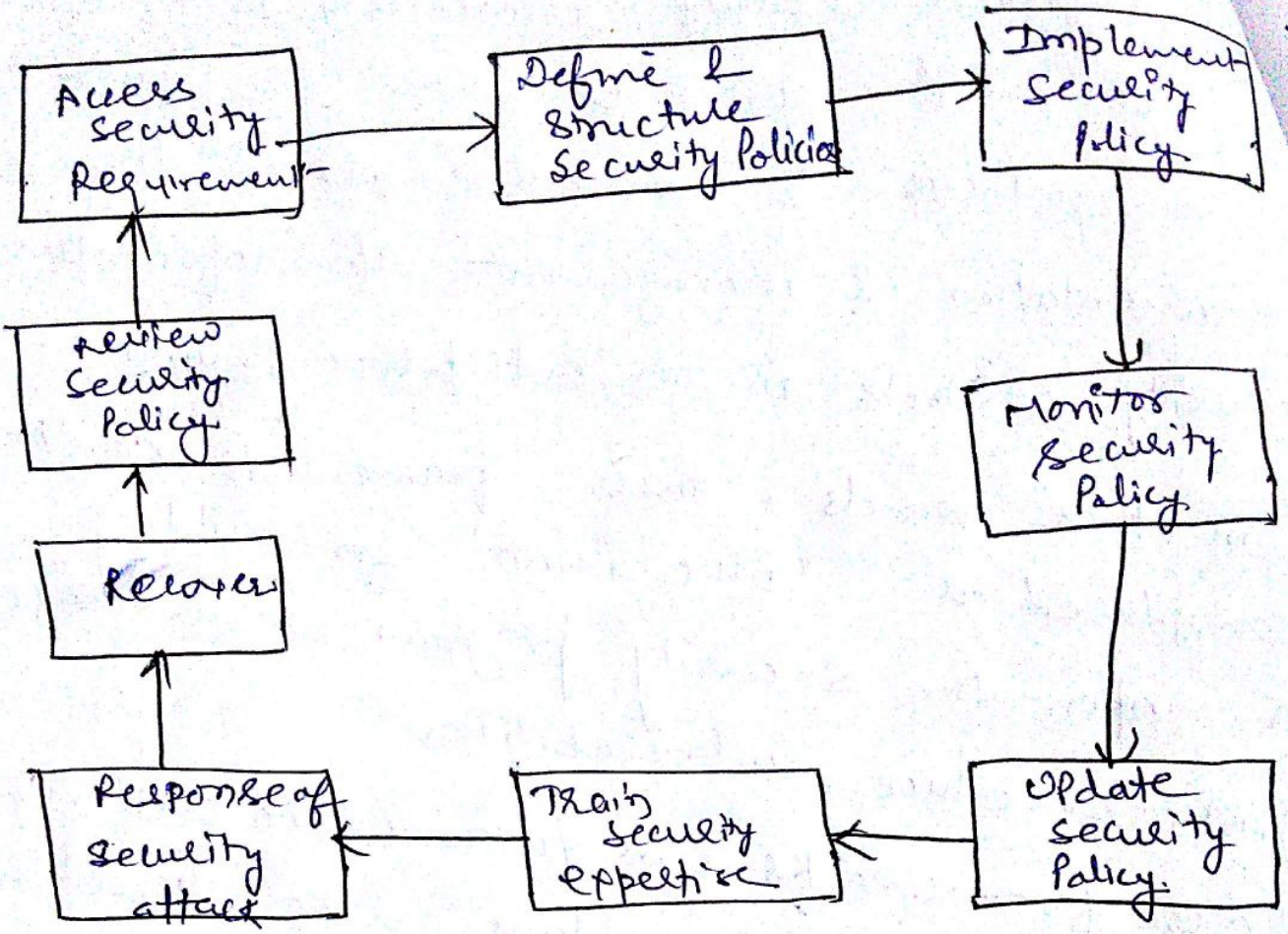
⇒ In other words, these framework can be considered as "Blue Print" for building an information security program to manage risk & reduce vulnerabilities.

⇒ These frameworks can further be customized to solve specific problems. like "blue print" are customized to meet their specification & use. They come in various degrees of complexity & scale.

(*) for an IT security system to work, a well defined framework needs to be developed. involving all stakeholders & it needs to be self-tuning over time to be useful.

Scanned by CamScanner

Security framework :-



Some of Security framework are :-

1. Iso 27000 - series
2. NIST 800-30 : Risk Management
3. Payment Card Industry Data Security Standard (PCI DSS)
4. COBIT 5 : Control objectives for information Related Technology.
5. COPPA : (Children's Online Privacy Protection Act).

Scanned by CamScanner

Security Metrics

metrics is used to measure the implementation of security Policy, the result of security Services & impact of security events of an organisation.

Measurement is the process of assigning symbols, usually numbers to represent an attribute of an entity.

metrics is standard of measurement using quantitative statistical & mathematical Analysis.

measurement is a one time view while metrics are produced by taking measurements over time & comparing them

⇒ Developing Security metrics & implementing them through systematic process involves a good understanding for :-

1. Vulnerabilities
2. Quality Attributes
3. Security Analysis of Threats
4. security Impacts.

Scanned by CamScanner

Basics :- NIST (National Institute of Standard & Technology) define metrics as tools designed to facilitate decision making & improve performance & accountability through collection, analysis & reporting of relevant performance-related data.

(*) metrics are simply a standard of measurement. It is standard of measuring security, specially specifically measuring an organization's security Posture.

Classifications :-

(1) Security Metric Categories :-

① Platform
② Network
③ Incident
④ Vendor
⑤ People
⑥ Industry.

Scanned by CamScanner

Security Metrics Model :- Security Metrics (17)
model is of 2 types :-

(1) Compliance metrics :- It measures how effective central security efforts are in driving down risk.

(2) Adequacy metrics :- It measures the risk involved between user's behaviour & organisational Policy.

(3) Components of security Metrics Model :-
① object
② security objective
③ Method of measurement

(4) In organizational Context :-
① Business impact
② Program results
③ Process implementation

(5) Security Metric Type :-
① Real Time :- ① Number of concurrent connections to VPN.
② It is usually from incident response System.

Scanned by CamScanner

(2) Polled :- The number of password reset requests.

(3) Incident Based :-

(1) Number of machine infected.

(2) Number of Vendors Suffering from infecting of ~~worm~~ worm.

Why Security Metrics are Important ?

The implementation of security metric is one of way of measuring the effectiveness of a company's security Program. The development & delivery of Programs & services with Results can be measured. The core of every business is having good performance metrics & carefully planned Program.

In creating useful metrics, data can be gathered from everywhere.

Metrics for security is valuable & meaningful if they produce proven or quantifiable data like result in percentages or averages.

Scanned by CamScanner

Metrics for Business unit Score cards Should have following Criteria :-

1. They measure behaviour of business unit is accountable for.
2. All business units contribute data to them.
3. They contain necessary information to support business unit correlation.

Benefits of Security Metrics :-

1. organization can improve security & accountability by deploying security metrics.
2. Security metrics can be created to measure each aspect of organization's security. eg:- Results of Risk assessment, security Testing & evaluation can be quantified & used as a source for security metrics.
3. Security ~~Measure~~ metrics help to determine effectiveness of implemented processes, Procedures & Controls.

Scanned by CamScanner

Information security Vs Privacy :-

① Privacy is concerned with collection & use of personal data.	① Security is concerned with protection of that personal data.
② Privacy is individual's right to keep this data to himself.	② Security is impersonal.
③ It is concerned with what is collected or how it is used.	③ It is concerned with protection of information by means of encryption, authentication etc.

④ If a company has sold, disclosed or rented consumer information that was entrusted to them without getting prior approval is clearly the breach of Privacy.

⑤ It is all practices & processes that are in place to ensure data is not being used or accessed by unauthorized individuals or parties. It also ensures accuracy & reliability.

Scanned by CamScanner

UNIT-IV

What is Cryptography?

Cryptography ,which comes from the Greek work kryptos,meaning ―hidden‖,and graphein, meaning ―to write‖,is aprocess of making and using codes to secure the transmission of information.

Cryptoanalysis is the process of obtaining the original message (called plaintext) from an encrypted message (called the cipher ext) without knowing the algorithms and keys used to perform the encryption.

Encryption is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is; to anyone without the tools to convert the encrypted message back to its original format.

Decryption is the process of converting the cipher text into a message that conveys readily understood meaning.

Basic Encryption Definitions.

Encryption Definitions

Algorithm: the mathematical formula used to convert an unencrypted message into an encrypted message.

Cipher: the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components

Packet Sniffers

 A network tool that collects copies of packets from the network and analyzes them

 Can be used to eavesdrop on the network traffic

 To use a packet sniffer legally, you must be:

 on a network that the organization owns

 under direct authorization of the owners of the network

 have knowledge and consent of the content creators (users)

Content Filters

 Although technically not a firewall, a content filter is a software filter that allows administrators to restrict accessible content from within a network

 The content filtering restricts Web sites with inappropriate content

Trap and Trace

 Trace: determine the identity of someone using unauthorized access

 Better known as honey pots, they distract the attacker while notifying the Administrator

What is Cryptography?

Cryptography ,which comes from the Greek work kryptos,meaning ―hidden‖,and graphein, meaning ―to write‖,is aprocess of making and using codes to secure the transmission of information.

Cryptoanalysis is the process of obtaining the original message (called plaintext) from an encrypted message (called the cipher ext) without knowing the algorithms and keys used to perform the encryption.

Encryption is the process of converting an original message into a form that is unreadable to unauthorized individuals-that is; to anyone without the tools to convert the encrypted message back to its original format.

Decryption is the process of converting the cipher text into a message that conveys readily understood meaning.

Basic Encryption Definitions.

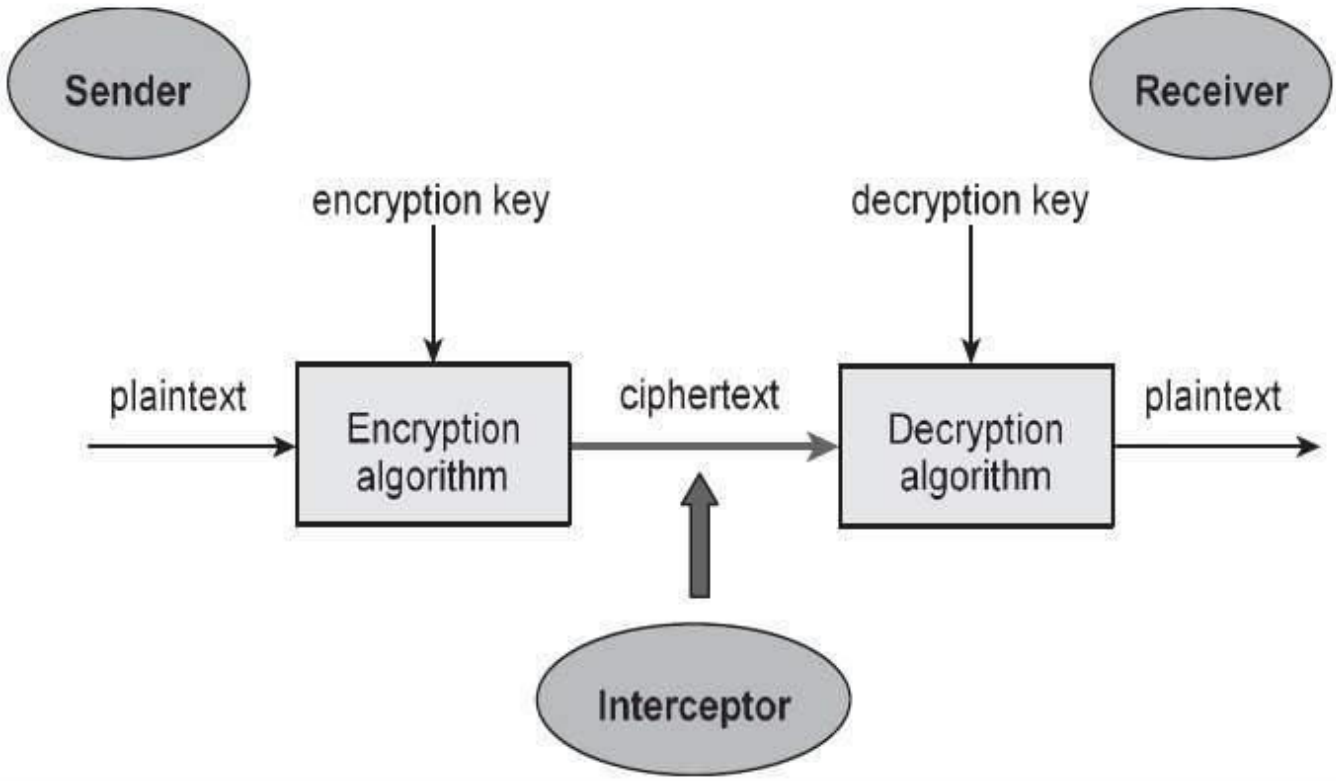
Encryption Definitions

Algorithm: the mathematical formula used to convert an unencrypted message into an encrypted message.

Cipher: the transformation of the individual components (characters, bytes, or bits) of an unencrypted message into encrypted components

Ciphertext or cryptogram: the unintelligible encrypted or encoded message resulting from an encryption.
Code: the transformation of the larger components (words or phrases) of an unencrypted message into encrypted components.
Cryptosystem: the set of transformations necessary to convert an unencrypted message into an encrypted message.
Decipher: to decrypt or convert ciphertext to plaintext.
Encipher: to encrypt or convert plaintext to ciphertext.
Key or cryptovariable: the information used in conjunction with the algorithm to create ciphertext from plaintext.
Keyspace: the entire range of values that can possibly be used to construct an individual key.
Link encryption: a series of encryptions and decryptions between a number of systems, whereby each node decrypts the message sent to it and then re-encrypts it using different keys and sends it to the next neighbor, until it reaches the final destination.
Plaintext: the original unencrypted message that is encrypted and results from successful decryption.
Steganography: the process of hiding messages in a picture or graphic. **Work factor**: the amount of effort (usually in hours) required to perform cryptanalysis on an encoded message.
A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services. A cryptosystem is also referred to as a **cipher system**.

Let us discuss a simple model of a cryptosystem that provides confidentiality to the information being transmitted. This basic model is depicted in the illustration below −



The illustration shows a sender who wants to transfer some sensitive data to a receiver in such a way that any party intercepting or eavesdropping on the communication channel cannot extract the data.

The objective of this simple cryptosystem is that at the end of the process, only the sender and the receiver will know the plaintext.

Components of a Cryptosystem

The various components of a basic cryptosystem are as follows −

- **Plaintext.** It is the data to be protected during transmission.
- **Encryption Algorithm.** It is a mathematical process that produces a ciphertext for any given plaintext and encryption key. It is a cryptographic algorithm that takes plaintext and an encryption key as input and produces a ciphertext.
- **Ciphertext.** It is the scrambled version of the plaintext produced by the encryption algorithm using a specific the encryption key. The ciphertext is not guarded. It flows on public channel. It can be intercepted or compromised by anyone who has access to the communication channel.
- **Decryption Algorithm,** It is a mathematical process, that produces a unique plaintext for any given ciphertext and decryption key. It is a cryptographic algorithm that takes a ciphertext and a decryption key as input, and outputs a plaintext. The decryption algorithm essentially reverses the encryption algorithm and is thus closely related to it.
- **Encryption Key.** It is a value that is known to the sender. The sender inputs the encryption key into the encryption algorithm along with the plaintext in order to compute the ciphertext.
- **Decryption Key.** It is a value that is known to the receiver. The decryption key is related to the encryption key, but is not always identical to it. The receiver inputs the decryption key into the decryption algorithm along with the ciphertext in order to compute the plaintext.

For a given cryptosystem, a collection of all possible decryption keys is called a**key space**.

An **interceptor** (an attacker) is an unauthorized entity who attempts to determine the plaintext. He can see the ciphertext and may know the decryption algorithm. He, however, must never know the decryption key.

Types of Cryptosystems

Fundamentally, there are two types of cryptosystems based on the manner in which encryption-decryption is carried out in the system −

- Symmetric Key Encryption
- Asymmetric Key Encryption

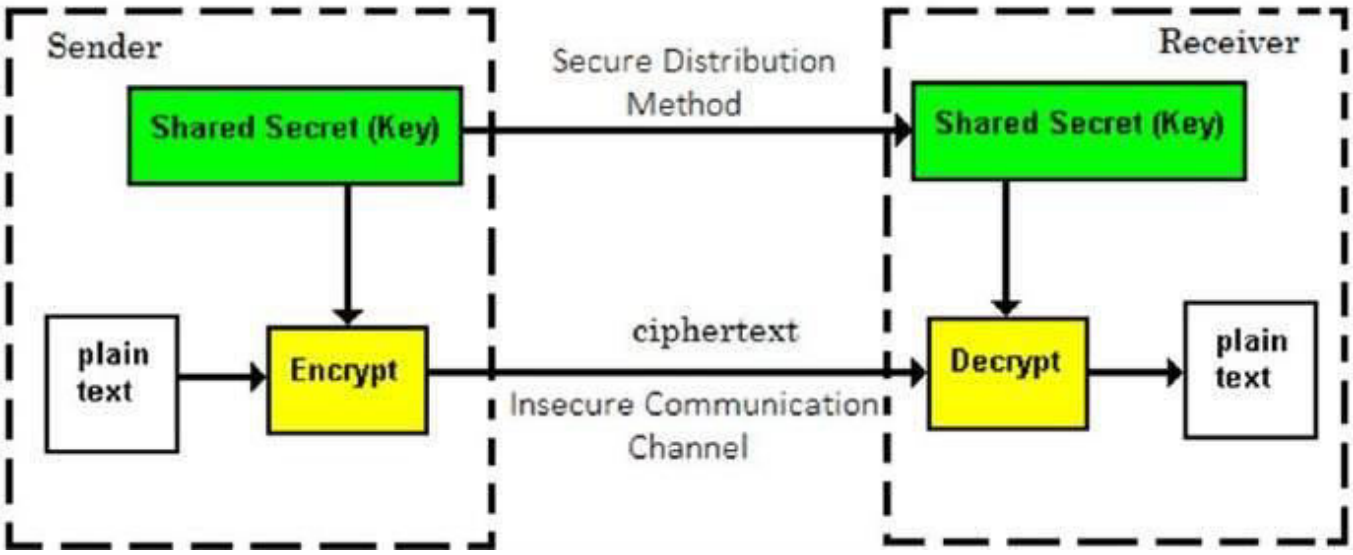
The main difference between these cryptosystems is the relationship between the encryption and the decryption key. Logically, in any cryptosystem, both the keys are closely associated. It is practically impossible to decrypt the ciphertext with the key that is unrelated to the encryption key.

Symmetric Key Encryption

The encryption process where **same keys are used for encrypting and decrypting** the information is known as Symmetric Key Encryption.

The study of symmetric cryptosystems is referred to as **symmetric cryptography**. Symmetric cryptosystems are also sometimes referred to as**secret key cryptosystems**.

A few well-known examples of symmetric key encryption methods are − Digital Encryption Standard (DES), Triple-DES (3DES), IDEA, and BLOWFISH.



Prior to 1970, all cryptosystems employed symmetric key encryption. Even today, its relevance is very high and it is being used extensively in many cryptosystems. It is very unlikely that this encryption will fade away, as it has certain advantages over asymmetric key encryption.

The salient features of cryptosystem based on symmetric key encryption are −

- Persons using symmetric key encryption must share a common key prior to exchange of information.
- Keys are recommended to be changed regularly to prevent any attack on the system.
- A robust mechanism needs to exist to exchange the key between the communicating parties. As keys are required to be changed regularly, this mechanism becomes expensive and cumbersome.
- In a group of **n** people, to enable two-party communication between any two persons, the number of keys required for group is **n × (n – 1)/2**.
- Length of Key (number of bits) in this encryption is smaller and hence, process of encryption-decryption is faster than asymmetric key encryption.
- Processing power of computer system required to run symmetric algorithm is less.

Challenge of Symmetric Key Cryptosystem

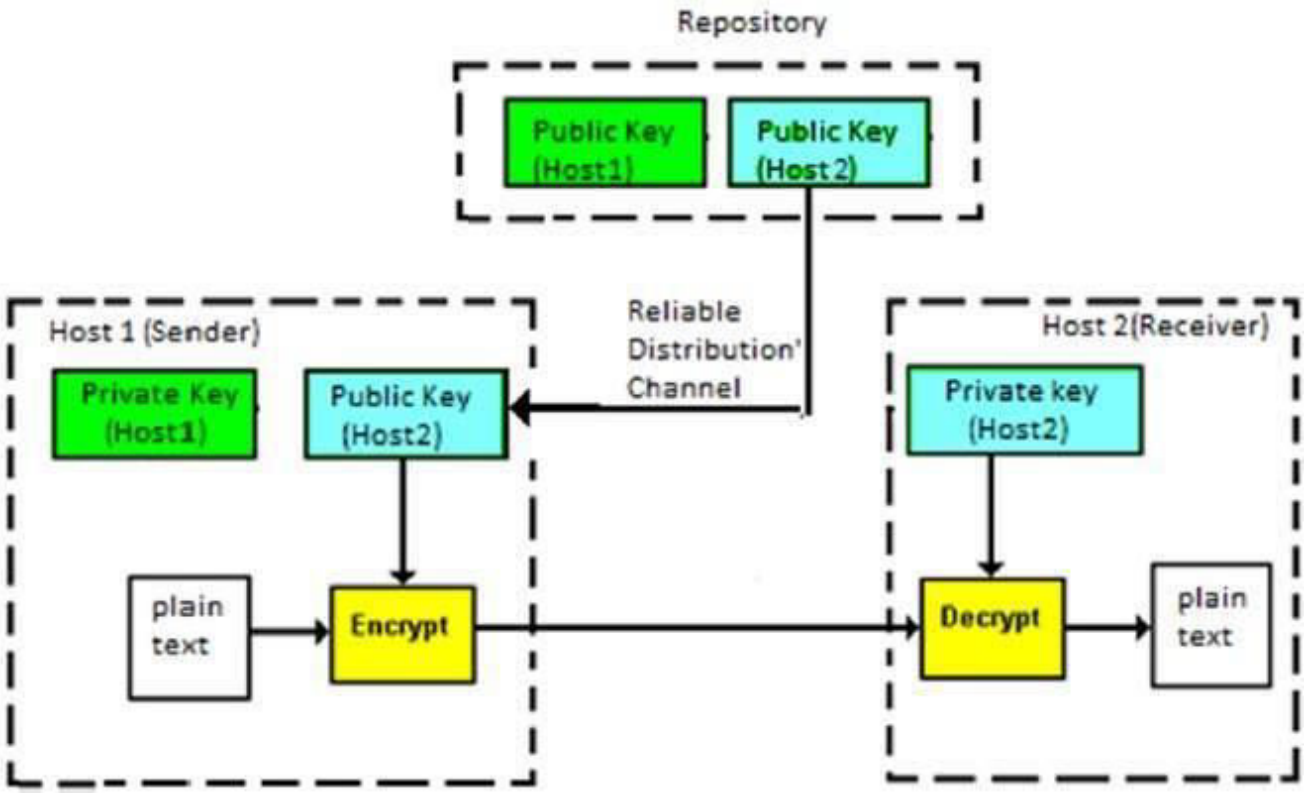
There are two restrictive challenges of employing symmetric key cryptography.

- **Key establishment** − Before any communication, both the sender and the receiver need to agree on a secret symmetric key. It requires a secure key establishment mechanism in place.
- **Trust Issue** − Since the sender and the receiver use the same symmetric key, there is an implicit requirement that the sender and the receiver ‘trust’ each other. For example, it may happen that the receiver has lost the key to an attacker and the sender is not informed.

These two challenges are highly restraining for modern day communication. Today, people need to exchange information with non-familiar and non-trusted parties. For example, a communication between online seller and customer. These limitations of symmetric key encryption gave rise to asymmetric key encryption schemes.

Asymmetric Key Encryption

The encryption process where **different keys are used for encrypting and decrypting the information** is known as Asymmetric Key Encryption. Though the keys are different, they are mathematically related and hence, retrieving the plaintext by decrypting ciphertext is feasible. The process is depicted in the following illustration −



Asymmetric Key Encryption was invented in the 20th century to come over the necessity of pre-shared secret key between communicating persons. The salient features of this encryption scheme are as follows −

- Every user in this system needs to have a pair of dissimilar keys,**private key** and **public key**. These keys are mathematically related − when one key is used for encryption, the other can decrypt the ciphertext back to the original plaintext.
- It requires to put the public key in public repository and the private key as a well-guarded secret. Hence, this scheme of encryption is also called **Public Key Encryption**.
- Though public and private keys of the user are related, it is computationally not feasible to find one from another. This is a strength of this scheme.
- When *Host1* needs to send data to *Host2,* he obtains the public key of*Host2* from repository, encrypts the data, and transmits.
- *Host2* uses his private key to extract the plaintext.
- Length of Keys (number of bits) in this encryption is large and hence, the process of encryption-decryption is slower than symmetric key encryption.
- Processing power of computer system required to run asymmetric algorithm is higher.

Symmetric cryptosystems are a natural concept. In contrast, public-key cryptosystems are quite difficult to comprehend.

You may think, *how can the encryption key and the decryption key are 'related', and yet it is impossible to determine the decryption key from the encryption key?* The answer lies in the mathematical concepts. It is possible to design a cryptosystem whose keys have this property. The concept of public-key cryptography is relatively new. There are fewer public-key algorithms known than symmetric algorithms.

Challenge of Public Key Cryptosystem

Public-key cryptosystems have one significant challenge − the user needs to trust that the public key that he is using in communications with a person really is the public key of that person and has not been spoofed by a malicious third party.

This is usually accomplished through a Public Key Infrastructure (PKI) consisting a trusted third party. The third party securely manages and attests to the authenticity of public keys. When the third party is requested to provide the public key for any communicating person X, they are trusted to provide the correct public key.

The third party satisfies itself about user identity by the process of attestation, notarization, or some other process − that X is the one and only, or globally unique, X. The most common method of making the verified public keys available is to embed them in a certificate which is digitally signed by the trusted third party.

Relation between Encryption Schemes

A summary of basic key properties of two types of cryptosystems is given below −

	Symmetric Cryptosystems	**Public Key Cryptosystems**
Relation between Keys	Same	Different, but mathematically related
Encryption Key	Symmetric	Public
Decryption Key	Symmetric	Private

Due to the advantages and disadvantage of both the systems, symmetric key and public-key cryptosystems are often used together in the practical information security systems.

Issues in Document Security

Documents face threats of many kinds. Customer lists, sales-strategy reports, and detailed revenue statistics might fall into the hands of competitors. Confidential personal data given by customers and employees could be compromised leading to lawsuits. Identification details like bank-account login information or credit-card details might be stolen by thieves. Because of these possibilities in today's world, the issue of document security should be a top concern.

1. Security measures under a document management system seek to protect business data and business interests, comply with legal requirements, such as protection of privacy, and prevent financial losses through ID theft and fraud.
2. Document security is generally ensured by restricting access to the documents. In a paper-based system, highly sensitive documents can be kept under lock and key for viewing by only top managers, for example.
3. It's practically impossible to ensure adequate security for documents under a paper-based system because keeping all documents under lock and key can affect business results. For example, decision makers might find that documents that provide decision-support information cannot be assembled quickly enough.
4. Electronic document management systems can improve things in a major way because access to particular folders and documents can be selectively restricted using electronic means. For example, employees can be categorized into different levels, and each level can have different access rights and permissions.
5. Access rights typically include viewing and editing privileges, i.e. some might be allowed to view a particular document but not modify it. Others might have full rights, including editing privileges. Users might also have to provide passwords to access the documents. This can theoretically prevent unauthorized persons from accessing documents at an employee's workstation.
6. As will be evident, permissions alone cannot provide full safeguards. An employee might not log out after accessing a document, and if that person leaves the workstation, someone else might then be able to view it. Training employees to follow best practices for security is a key element of overall document security.
7. It has been reported that most security lapses are due to employees, either through carelessness or dishonesty. It's very important to provide access rights strictly on a need-to-have basis, with each employee (including senior employees) being able to access only those documents that they require to complete their specific tasks.
8. Any document management system must maintain audit trails that keep track of who accessed which document and when, and what changes were made during each access. The trail must then be monitored by a responsible person for any unusual activities.
9. The existence of the Internet allows threats to come from external sources. Specific dangers from viruses and other malicious software, from hackers who can wipe out valuable business data, and from identity thieves have become far more serious today.
10. These external threats are guarded against through the installation of security software such as anti-virus and anti-spyware programs, implementation of firewalls and secure-access mechanisms, such as SSL, and regular updates to operating systems and applications. Software developers typically issue patches to plug any possible security loopholes.
11. Authentication of documents is another key security precaution. Developments like electronic signatures can not only help senders sign outgoing documents, but also enable recipients to ensure that the documents they receive are indeed from who they claim to be, and that no alterations have occurred since it was authenticated.
12. Above all, regular reviews must be carried out to identify any security vulnerabilities, including practices like creating backups and implementing document retention and destruction policies. Documents that have exceeded their lifetimes must be shredded rather than left around.

As document security has become a vital concern, several helpful organizations have issued guidelines to help companies deal with these security issues. One such example is ISO 27002, a standard implemented by the International Standards Organization dealing specifically with information security. Implementing these policies and practices can help your organization improve the security of your documents and information.

System Of Keys

One of the most important aspects of any **cryptographic system is key management**; which is very difficult and, therefore, sometimes neglected.[1] A very common mistake is mixing different key types and reusing the same key for different purposes. An example with devastating consequences is the reuse of the same symmetric key for both*symmetric authentication* in CBC-MAC and *symmetric data encryption* in CBC encryption.

This page shows the classification of key types from the point of view of key management. In a key management system each key should be labeled with one such type and that key should never be used for a different purpose. According to NIST SP 800-57 the following types of keys exist:

Private signature key

Private signature keys are the private keys of asymmetric (public) key pairs that are used by public key algorithms to generate digital signatures with possible long-term implications. When properly handled, private signature keys can be used to provide authentication, integrity and non-repudiation.

Public signature verification key

A public signature verification key is the public key of an asymmetric key pair that is used by a public key algorithm to verify digital signatures, either to authenticate a user's identity, to determine the integrity of the data, for non-repudiation, or a combination thereof.

Symmetric authentication key

Symmetric authentication keys are used with symmetric key algorithms to provide assurance of the integrity and source of messages, communication sessions, or stored data.

Private authentication key

A private authentication key is the private key of an asymmetric key pair that is used with a public key algorithm to provide assurance as to the integrity of information, and the identity of the originating entity or the source of messages, communication sessions, or stored data.

Public authentication key

A public authentication key is the public key of an asymmetric key pair that is used with a public key algorithm to determine the integrity of information and to authenticate the identity of entities, or the source of messages, communication sessions, or stored data.

Symmetric data encryption key

These keys are used with symmetric key algorithms to apply confidentiality protection to information.

Symmetric key wrapping key

Symmetric key wrapping keys are used to encrypt other keys using symmetric key algorithms. Key wrapping keys are also known as key encrypting keys.

Symmetric and asymmetric random number generation keys

These are keys used to generate random numbers.

Symmetric master key

A symmetric master key is used to derive other symmetric keys (e.g., data encryption keys, key wrapping keys, or authentication keys) using symmetric cryptographic methods.

Private key transport key

Private key transport keys are the private keys of asymmetric key pairs that are used to decrypt keys that have been encrypted with the associated public key using a public key algorithm. Key transport keys are usually used to establish keys (e.g., key wrapping keys, data encryption keys or MAC keys) and, optionally, other keying material (e.g.,initialization vectors).

Public key transport key

Public key transport keys are the public keys of asymmetric key pairs that are used to encrypt keys using a public key algorithm. These keys are used to establish keys (e.g., key wrapping keys, data encryption keys or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).

Symmetric key agreement key

These symmetric keys are used to establish keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors) using a symmetric key agreement algorithm.

Private static key agreement key

Private static key agreement keys are the private keys of asymmetric key pairs that are used to establish keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).

Public static key agreement key

Public static key agreement keys are the public keys of asymmetric key pairs that are used to establish keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).

Private ephemeral key agreement key

Private ephemeral key agreement keys are the private keys of asymmetric key pairs that are used only once to establish one or more keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).

Public ephemeral key agreement key

Public ephemeral key agreement keys are the public keys of asymmetric key pairs that are used in a single key establishment transaction to establish one or more keys (e.g., key wrapping keys, data encryption keys, or MAC keys) and, optionally, other keying material (e.g., Initialization Vectors).

Symmetric authorization key

Symmetric authorization keys are used to provide privileges to an entity using a symmetric cryptographic method. The authorization key is known by the entity responsible for monitoring and granting access privileges for authorized entities and by the entity seeking access to resources.

Private authorization key

A private authorization key is the private key of an asymmetric key pair that is used to provide privileges to an entity.

Public authorization key

A public authorization key is the public key of an asymmetric key pair that is used to verify privileges for an entity that knows the associated private authorization key.

Public Key Cryptography

Public-key cryptography and related standards underlie the security features of many products such as signed and encrypted email, single sign-on, and Secure Sockets Layer (SSL) communications. This chapter covers the basic concepts of public-key cryptography.

Internet traffic, which passes information through intermediate computers, can be intercepted by a third party:

- *Eavesdropping*. Information remains intact, but its privacy is compromised. For example, someone could gather credit card numbers, record a sensitive conversation, or intercept classified information.

- *Tampering*. Information in transit is changed or replaced and then sent to the recipient. For example, someone could alter an order for goods or change a person's resume.

- *Impersonation.* Information passes to a person who poses as the intended recipient. Impersonation can take two forms:
    - *Spoofing*. A person can pretend to be someone else. For example, a person can pretend to have the email address **jdoe@example.net** or a computer can falsely identify itself as a site called **www.example.net**.
    - *Misrepresentation.* A person or organization can misrepresent itself. For example, a site called **www.example.net** can purport to be an on-line furniture store when it really receives credit-card payments but never sends any goods.

Public-key cryptography provides protection against Internet-based attacks through:

- *Encryption and decryption* allow two communicating parties to disguise information they send to each other. The sender encrypts, or scrambles, information before sending it. The receiver decrypts, or unscrambles, the information after receiving it. While in transit, the encrypted information is unintelligible to an intruder.
- *Tamper detection* allows the recipient of information to verify that it has not been modified in transit. Any attempts to modify or substitute data are detected.
- *Authentication* allows the recipient of information to determine its origin by confirming the sender's identity.
- *Nonrepudiation* prevents the sender of information from claiming at a later date that the information was never sent.

1.1. Encryption and Decryption

Encryption is the process of transforming information so it is unintelligible to anyone but the intended recipient.*Decryption* is the process of decoding encrypted information. A cryptographic algorithm, also called a *cipher*, is a mathematical function used for encryption or decryption. Usually, two related functions are used, one for encryption and the other for decryption.
With most modern cryptography, the ability to keep encrypted information secret is based not on the cryptographic algorithm, which is widely known, but on a number called a *key* that must be used with the algorithm to produce an encrypted result or to decrypt previously encrypted information. Decryption with the correct key is simple. Decryption without the correct key is very difficult, if not impossible.

1.1.1. Symmetric-Key Encryption

With symmetric-key encryption, the encryption key can be calculated from the decryption key and vice versa. With most symmetric algorithms, the same key is used for both encryption and decryption, as shown inFigure 1.1, “Symmetric-Key Encryption”.

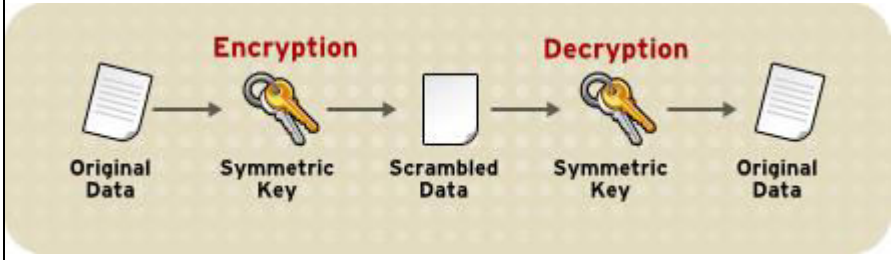


Figure 1.1. Symmetric-Key Encryption

Implementations of symmetric-key encryption can be highly efficient, so that users do not experience any significant time delay as a result of the encryption and decryption. Symmetric-key encryption also provides a degree of authentication, since information encrypted with one symmetric key cannot be decrypted with any other symmetric key. Thus, as long as the symmetric key is kept secret by the two parties using it to encrypt communications, each party can be sure that it is communicating with the other as long as the decrypted messages continue to make sense.

Symmetric-key encryption is effective only if the symmetric key is kept secret by the two parties involved. If anyone else discovers the key, it affects both confidentiality and authentication. A person with an unauthorized symmetric key not only can decrypt messages sent with that key, but can encrypt new messages and send them as if they came from one of the legitimate parties using the key.

Symmetric-key encryption plays an important role in SSL communication, which is widely used for authentication, tamper detection, and encryption over TCP/IP networks. SSL also uses techniques of public-key encryption, which is described in the next section.

1.1.2. Public-Key Encryption

Public-key encryption (also called asymmetric encryption) involves a pair of keys, a public key and a private key, associated with an entity. Each public key is published, and the corresponding private key is kept secret. (For more information about the way public keys are published, see Section 1.3, "Certificates and Authentication".) Data encrypted with a public key can be decrypted only with the corresponding private key.Figure 1.2, "Public-Key Encryption" shows a simplified view of the way public-key encryption works.

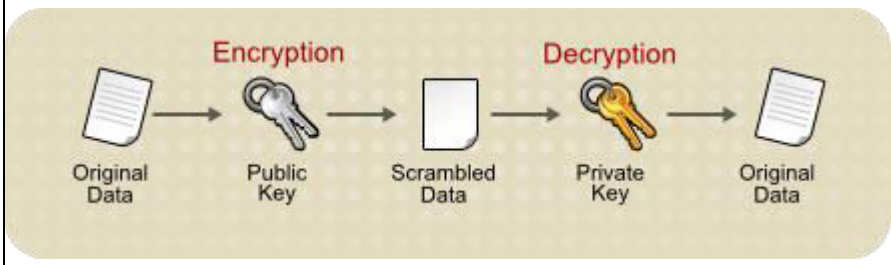


Figure 1.2. Public-Key Encryption

The scheme shown in Figure 1.2, "Public-Key Encryption" allows public keys to be freely distributed, while only authorized people are able to read data encrypted using this key. In general, to send encrypted data, the data is encrypted with that person's public key, and the person receiving the encrypted data decrypts it with the corresponding private key.

Compared with symmetric-key encryption, public-key encryption requires more processing and may not be feasible for encrypting and decrypting large amounts of data. However, it is possible to use public-key encryption to send a symmetric key, which can then be used to encrypt additional data. This is the approach used by the SSL/TLS protocols.

The reverse of the scheme shown in Figure 1.2, "Public-Key Encryption" also works: data encrypted with a private key can be decrypted only with the corresponding public key. This is not a recommended practice to encrypt sensitive data, however, because it means that anyone with the public key, which is by definition published, could decrypt the data. Nevertheless, private-key encryption is useful because it means the private key can be used to sign data with a digital signature, an important requirement for electronic commerce and other commercial applications of cryptography. Client software such as Mozilla Firefox can then use the public key to confirm that the message was signed with the appropriate private key and that it has not been tampered with since being signed. Section 1.2, "Digital Signatures" illustrates how this confirmation process works.

1.1.3. Key Length and Encryption Strength

Breaking an encryption algorithm is basically finding the key to the access the encrypted data in plain text. For symmetric algorithms, breaking the algorithm usually means trying to determine the key used to encrypt the text. For a public key algorithm, breaking the algorithm usually means acquiring the shared secret information between two recipients.

One method of breaking a symmetric algorithm is to simply try every key within the full algorithm until the right key is found. For public key algorithms, since half of the key pair is publicly known, the other half (private key) can be derived using published, though complex, mathematical calculations. Manually finding the key to break an algorithm is called a brute force attack.

Breaking an algorithm introduces the risk of intercepting, or even impersonating and fraudulently verifying, private information.

The *key strength* of an algorithm is determined by finding the fastest method to break the algorithm and comparing it to a brute force attack.

For symmetric keys, encryption strength is often described in terms of the size or *length* of the keys used to perform the encryption: longer keys generally provide stronger encryption. Key length is measured in bits. For example, 128-bit keys with the RC4 symmetric-key cipher supported by SSL provide significantly better cryptographic protection than 40-bit keys used with the same cipher. The 128-bit RC4 encryption is 3×10^{26} times stronger than 40-bit RC4 encryption.

An encryption key is considered full strength if the best known attack to break the key is no faster than a brute force attempt to test every key possibility.

Different types of algorithms — particularly public key algorithms — may require different key lengths to achieve the same level of encryption strength as a symmetric-key cipher. The RSA cipher can use only a subset of all possible values for a key of a given length, due to the nature of the mathematical problem on which it is based. Other ciphers, such as those used for symmetric-key encryption, can use all possible values for a key of a given length. More possible matching options means more security.

Because it is relatively trivial to break an RSA key, an RSA public-key encryption cipher must have a very long key — at least 1024 bits — to be considered cryptographically strong. On the other hand, symmetric-key ciphers are reckoned to be equivalently strong using a much shorter key length, as little as 80 bits for most algorithms.

Digital Signature

Digital signatures are the public-key primitives of message authentication. In the physical world, it is common to use handwritten signatures on handwritten or typed messages. They are used to bind signatory to the message.

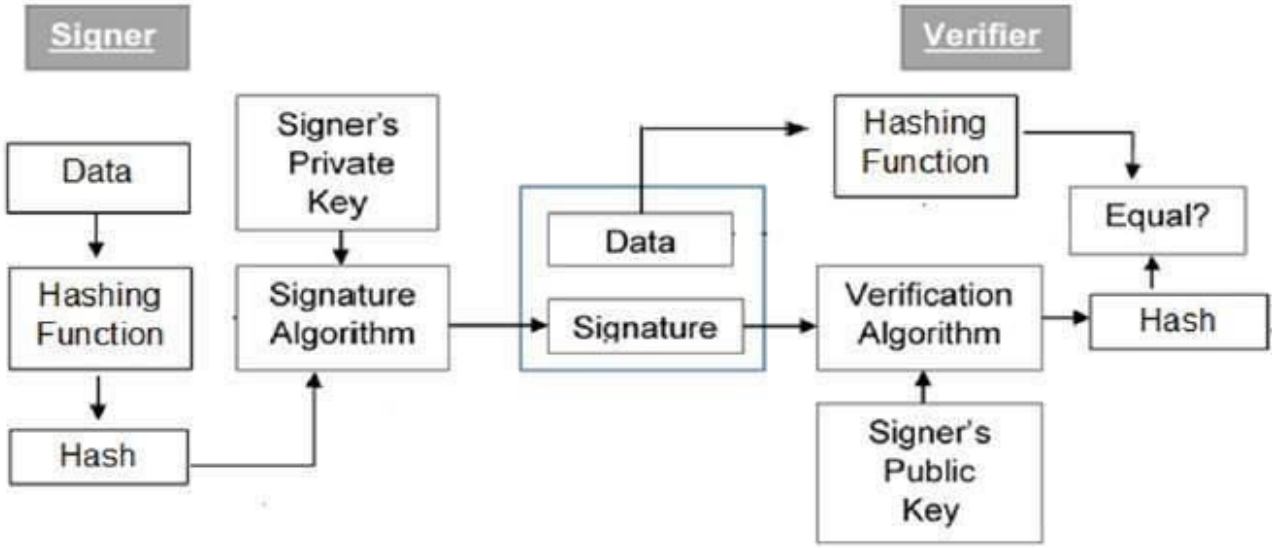
Similarly, a digital signature is a technique that binds a person/entity to the digital data. This binding can be independently verified by receiver as well as any third party.

Digital signature is a cryptographic value that is calculated from the data and a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender and he should not be able to repudiate the origination of that message. This requirement is very crucial in business applications, since likelihood of a dispute over exchanged data is very high.

Model of Digital Signature

As mentioned earlier, the digital signature scheme is based on public key cryptography. The model of digital signature scheme is depicted in the following illustration −



The following points explain the entire process in detail −

- Each person adopting this scheme has a public-private key pair.
- Generally, the key pairs used for encryption/decryption and signing/verifying are different. The private key used for signing is referred to as the signature key and the public key as the verification key.
- Signer feeds data to the hash function and generates hash of data.
- Hash value and signature key are then fed to the signature algorithm which produces the digital signature on given hash. Signature is appended to the data and then both are sent to the verifier.
- Verifier feeds the digital signature and the verification key into the verification algorithm. The verification algorithm gives some value as output.
- Verifier also runs same hash function on received data to generate hash value.
- For verification, this hash value and output of verification algorithm are compared. Based on the comparison result, verifier decides whether the digital signature is valid.
- Since digital signature is created by 'private' key of signer and no one else can have this key; the signer cannot repudiate signing the data in future.

It should be noticed that instead of signing data directly by signing algorithm, usually a hash of data is created. Since the hash of data is a unique representation of data, it is sufficient to sign the hash in place of data. The most important reason of using hash instead of data directly for signing is efficiency of the scheme.

Let us assume RSA is used as the signing algorithm. As discussed in public key encryption chapter, the encryption/signing process using RSA involves modular exponentiation.

Signing large data through modular exponentiation is computationally expensive and time consuming. The hash of the data is a relatively small digest of the data, hence **signing a hash is more efficient than signing the entire data**.

Importance of Digital Signature

Out of all cryptographic primitives, the digital signature using public key cryptography is considered as very important and useful tool to achieve information security.

Apart from ability to provide non-repudiation of message, the digital signature also provides message authentication and data integrity. Let us briefly see how this is achieved by the digital signature −

- **Message authentication** − When the verifier validates the digital signature using public key of a sender, he is assured that signature has been created only by sender who possess the corresponding secret private key and no one else.

- **Data Integrity** − In case an attacker has access to the data and modifies it, the digital signature verification at receiver end fails. The hash of modified data and the output provided by the verification algorithm will not match. Hence, receiver can safely deny the message assuming that data integrity has been breached.

- **Non-repudiation** − Since it is assumed that only the signer has the knowledge of the signature key, he can only create unique signature on a given data. Thus the receiver can present data and the digital signature to a third party as evidence if any dispute arises in the future.

By adding public-key encryption to digital signature scheme, we can create a cryptosystem that can provide the four essential elements of security namely − Privacy, Authentication, Integrity, and Non-repudiation.

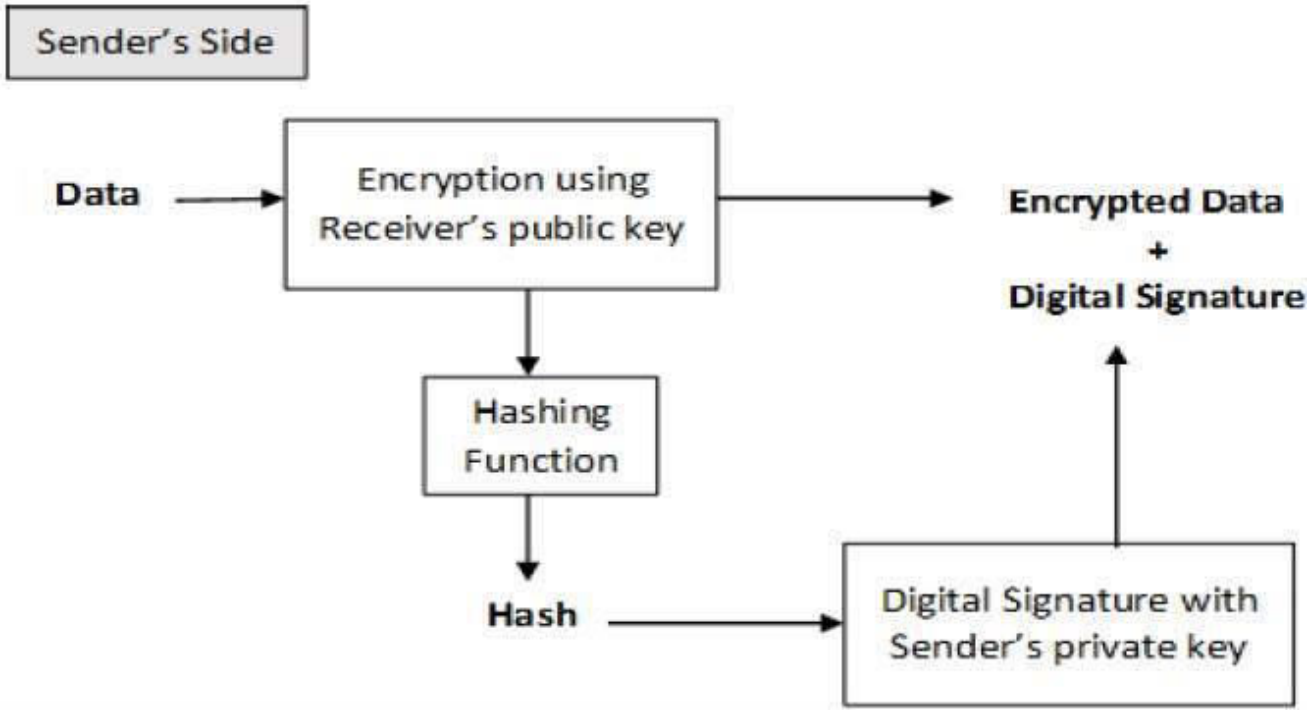
Encryption with Digital Signature

In many digital communications, it is desirable to exchange an encrypted messages than plaintext to achieve confidentiality. In public key encryption scheme, a public (encryption) key of sender is available in open domain, and hence anyone can spoof his identity and send any encrypted message to the receiver.

This makes it essential for users employing PKC for encryption to seek digital signatures along with encrypted data to be assured of message authentication and non-repudiation.

This can archived by combining digital signatures with encryption scheme. Let us briefly discuss how to achieve this requirement. There are **two possibilities, sign-then-encrypt** and **encrypt-then-sign**.

However, the crypto system based on sign-then-encrypt can be exploited by receiver to spoof identity of sender and sent that data to third party. Hence, this method is not preferred. The process of encrypt-then-sign is more reliable and widely adopted. This is depicted in the following illustration −



The receiver after receiving the encrypted data and signature on it, first verifies the signature using sender's public key. After ensuring the validity of the signature, he then retrieves the data through decryption using his private key.

Finger Prints

The History of Fingerprinting

· Francis Galton published his book "Finger Prints" (1892) which stated:
· there are three types of fingerprint patterns
· prints are unique to each individual
· prints do not change over time
· A classification system that allowed the filing of many thousands of fingerprints was developed in 1891
· The first systematic and official use of fingerprints in the United States was in New York City for the Civil Service Commission in 1891.
· In 1924, the fingerprint records of the Bureau of Investigation and Leavenworth Prison merged to form identification records at the FBI. This is the largest collection of fingerprints in the world.

Fingerprints are made when oil from the body is mixed with other body sweat and dirt. When you then touch something, these adhere or stick to the surface of the object.

Fingerprint Patterns

· arch patterns have lines that start at one side of the print and then move toward the center of the print and leave on the other side of the print

· whorl patterns have a lot of circles that do not exit on either side of the print

· loop patterns have lines that start at one side of the print and then move toward the center of the print and leave on the same side of the print they started on

Types of fingerprints left at crime scenes

· visible prints are fingerprints that one can see with the naked eye

· latent prints are fingerprints that are invisible

· plastic prints are fingerprints that leave an impression on objects such as soap or wax

Methods used to obtain fingerprints

· Ink pad or pencil smudge
· dusting
· impression
· fuming with super glue

Fingerprint Principles

According to criminal investigators, fingerprints follow 3 fundamental principles:

1. A fingerprint is an **individual** characteristic; no two people have been found with the **exact** same fingerprint pattern.
2. A fingerprint **pattern** will remain **unchanged** for the **life** of an individual; however, the print itself may change due to permanent scars and skin diseases.
3. Fingerprints have general characteristic **ridge** patterns that allow them to be systematically identified.

Fingerprint Classes

There are 3 specific classes for all fingerprints based upon their visual pattern: arches, loops, and whorls. Each group is divided into smaller groups as seen in the lists below.

1. **Arch:-** Plain arch and Tented arch
2. **Loop**:- Radial Loop and Ulnar loop
3. **Whorl:-** Plain whorl, Central pocket whorl, Double loop whorl and Accidentical

#Firewalls #

A firewall is any device that prevents a specific type of information from moving between the untrusted network outside and the trusted network inside There are five recognized generations of firewalls
The firewall may be:
1.a separate computer system
2.a service running on an existing router or server
3. a separate network containing a number of supporting devices

Different generations of firewalls:.

First Generation

Called packet filtering firewalls Examines every incoming packet header and selectively filters packets based on address, packet type, port request, and others factors The restrictions most commonly implemented are based on: IP source and destination address Direction (inbound or outbound)

Second Generation

TCP or UDP source and destination port-requests **Second Generation** Called application-level firewall or proxy server

 Often a dedicated computer separate from the filtering router

 With this configuration the proxy server, rather than the Web server, is exposed to the outside world in the DMZ

 Additional filtering routers can be implemented behind the proxy server

 The primary disadvantage of application-level firewalls is that they are designed for a specific protocol and cannot easily be reconfigured to protect against attacks on protocols for which they are not designed

Third Generation

 Called stateful inspection firewalls

 Keeps track of each network connection established between internal and external systems using a state table which tracks the state and context of each packet in the conversation by recording which station sent what packet.

 These firewalls can track connectionless packet traffic such as UDP and remote procedure calls (RPC) traffic

Fourth Generation

While static filtering firewalls, such as first and third generation, allow entire sets of one type of packet to enter in response to authorized requests, a dynamic packet filtering firewall allows only a particular packet with a particular source, destination,and port address to enter through the firewall

 It does this by understanding how the protocol functions, and opening and closing ―doors‖ in the firewall, based on the information contained in the packet header. In this manner, dynamic packet filters are an intermediate form, between traditional static packet filters and application proxies

Fifth Generation

 The final form of firewall is the kernel proxy, a specialized form that works under the Windows NT Executive, which is the kernel ofWindows NT

 It evaluates packets at multiple layers of the protocol stack, by checking security in the kernel as data is passed up and down the stack

Firewalls are categorized by processing modes :-

The five processing modes are

1) Packet filtering
2) Application gateways
3) Circuit gateways
4) MAC layer firewalls
5) Hybrids

Packet-filtering Routers

 Most organizations with an Internet connection have some form of a router as the interface at the perimeter between the organization‘s internal networks and the external service provider

 Many of these routers can be configured to filter packets that the organization does not allow into the network

 This is a simple but effective means to lower the organization‘s risk to external attack

 The drawback to this type of system includes a lack of auditing and strong authentication

 The complexity of the access control lists used to filter the packets can grow and degrade network performance

Screened-Host Firewall Systems

• Combine the packet-filtering router with a separate, dedicated firewall such as an application proxy server

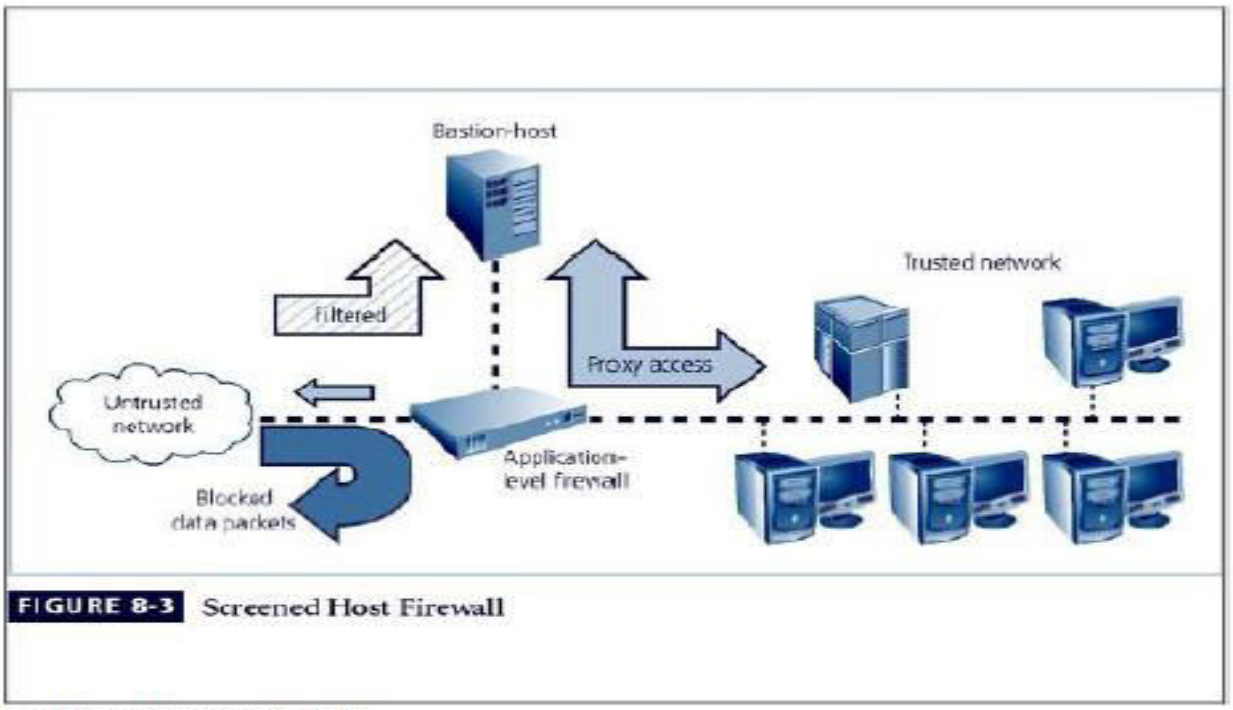


FIGURE 8-3 Screened Host Firewall

Dual homed host firewalls

- Dual-homed Host Firewalls
- The bastion-host contains two NICs (network interface cards) One NIC is connected to the external network, and one is connected to the internal network. With two NICs all traffic must physically go through the firewall to move between the internal and external networks
- A technology known as network-address translation (NAT) is commonly implemented with this architecture to map from real, valid, external IP addresses to ranges of internal IP addresses that are non-routable

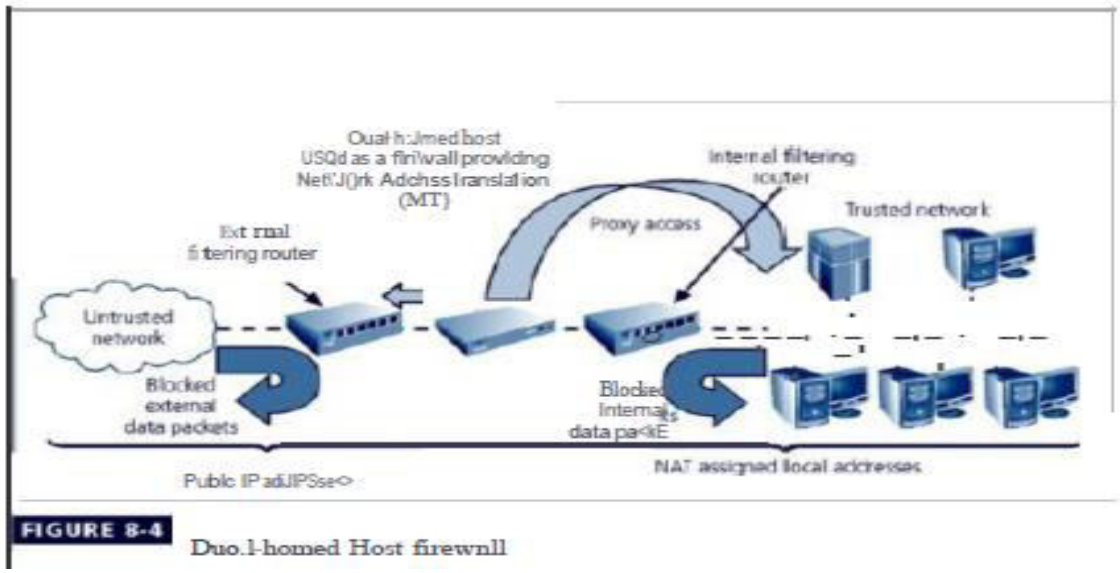


FIGURE 8-4 Duo.l-homed Host firewnll

Screened-Subnet Firewalls? Screened-Subnet Firewalls (with DMZ)

 Consists of two or more internal bastion-hosts, behind a packet-filtering router, with each host protecting the trusted network

 The first general model consists of two filtering routers, with one or more dual- homed bastion-host between them

 The second general model involves the connection from the outside or untrusted network going through this path:

o Through an external filtering router

o Into and then out of a routing firewall to the separate network segment known as the DMZ.

The factors to be considered while selecting a right firewall

Selecting the Right Firewall

 What type of firewall technology offers the right balance of protection features and cost for the needs of the organization?

 What features are included in the base price? What features are available at extra cost? Are all cost factors known?

 How easy is it to set up and configure the firewall? How accessible are staff technicians with the mastery to do it well?

 Can the candidate firewall adapt to the growing network in the target organization?

What are Sock Servers?

 The SOCKS system is a proprietary circuit-level proxy server that places special .SOCKS client-side agents on each workstation

 Places the filtering requirements on the individual workstation, rather than on a single point of defense (and thus point of failure)

 This frees the entry router of filtering responsibilities, but then requires each

A SOCKS system can require additional support and management resources to configure and manage possibly hundreds of individual clients, versus a single device or set of devices

Design and Implementation Issues of Firewall

Firewall Recommended Practices :-

 All traffic from the trusted network is allowed out .The firewall device is always inaccessible directly from the public network. Allow Simple Mail Transport Protocol (SMTP) data to pass through your firewall, but insure it is all routed to a well-configured SMTP gateway to filter and route messaging traffic securely

 All Internet ControlMessage Protocol (ICMP) data should be denied

 Block telnet (terminal emulation) access to all internal servers from the public networks

 When Web services are offered outside the firewall, deny HTTP traffic from reaching your internal networks by using some form of proxy access or DMZ architecture

Network Protection

Network security is the security provided to a network from unauthorized access and risks. It is the duty of network administrators to adopt preventive measures to protect their networks from potential security threats.

Computer networks that are involved in regular transactions and communication within the government, individuals, or business require security. The most common and simple way of protecting a network resource is by assigning it a unique name and a corresponding password.

Types of Network Security Devices

Active Devices

These security devices block the surplus traffic. Firewalls, antivirus scanning devices, and content filtering devices are the examples of such devices.

Passive Devices

These devices identify and report on unwanted traffic, for example, intrusion detection appliances.

Preventative Devices

These devices scan the networks and identify potential security problems. For example, penetration testing devices and vulnerability assessment appliances.

Unified Threat Management (UTM)

These devices serve as all-in-one security devices. Examples include firewalls, content filtering, web caching, etc.

Firewalls

A firewall is a network security system that manages and regulates the network traffic based on some protocols. A firewall establishes a barrier between a trusted internal network and the internet.

Firewalls exist both as software that run on a hardware and as hardware appliances. Firewalls that are hardware-based also provide other functions like acting as a DHCP server for that network.

Most personal computers use software-based firewalls to secure data from threats from the internet. Many routers that pass data between networks contain firewall components and conversely, many firewalls can perform basic routing functions.

Firewalls are commonly used in private networks or *intranets* to prevent unauthorized access from the internet. Every message entering or leaving the intranet goes through the firewall to be examined for security measures.

An ideal firewall configuration consists of both hardware and software based devices. A firewall also helps in providing remote access to a private network through secure authentication certificates and logins.

Hardware and Software Firewalls

Hardware firewalls are standalone products. These are also found in broadband routers. Most hardware firewalls provide a minimum of four network ports to connect other computers. For larger networks − e.g., for business purpose − business networking firewall solutions are available.

Software firewalls are installed on your computers. A software firewall protects your computer from internet threats.

Antivirus

An antivirus is a tool that is used to detect and remove malicious software. It was originally designed to detect and remove viruses from computers.

Modern antivirus software provide protection not only from virus, but also from worms, Trojan-horses, adwares, spywares, keyloggers, etc. Some products also provide protection from malicious URLs, spam, phishing attacks, botnets, DDoS attacks, etc.

Content Filtering

Content filtering devices screen unpleasant and offensive emails or webpages. These are used as a part of firewalls in corporations as well as in personal computers. These devices generate the message "Access Denied" when someone tries to access any unauthorized web page or email.

Content is usually screened for pornographic content and also for violence- or hate-oriented content. Organizations also exclude shopping and job related contents.

Content filtering can be divided into the following categories −

- Web filtering
- Screening of Web sites or pages
- E-mail filtering
- Screening of e-mail for spam
- Other objectionable content

Intrusion Detection Systems

Intrusion Detection Systems, also known as Intrusion Detection and Prevention Systems, are the appliances that monitor malicious activities in a network, log information about such activities, take steps to stop them, and finally report them.

Intrusion detection systems help in sending an alarm against any malicious activity in the network, drop the packets, and reset the connection to save the IP address from any blockage. Intrusion detection systems can also perform the following actions −

- Correct Cyclic Redundancy Check (CRC) errors
- Prevent TCP sequencing issues
- Clean up unwanted transport and network layer options

Perimeter for Network Protection

A network perimeter is the boundary between the private and locally managed-and-owned side of a network and the public and usually provider-managed side of a network. A perimeter is the fortified boundary of the network that might include the following aspects:

- Border routers
- Firewalls
- IDSs
- IPSs
- VPN devices
- Software architecture
- DMZs and screened subnets

Let's take a look at these perimeter components in closer detail.

Border Routers

Routers are the traffic cops of networks. They direct traffic into, out of, and within our networks. The*border router* is the last router you control before an untrusted network such as the Internet. Because all of an organization's Internet traffic goes through this router, it often functions as a network's first and last line of defense through initial and final filtering.

Firewalls

A *firewall* is a chokepoint device that has a set of rules specifying what traffic it will allow or deny to pass through it. A firewall typically picks up where the border router leaves off and makes a much more thorough pass at filtering traffic. Firewalls come in several different types, including static packet filters, stateful firewalls, and proxies. You might use a static packet filter such as a Cisco router to block easily identifiable "noise" on the Internet, a stateful firewall such as a Check Point FireWall-1 to control allowed services, or a proxy firewall such as Secure Computing's Sidewinder to control content. Although firewalls aren't perfect, they do block what we tell them to block and allow what we tell them to allow.

Intrusion Detection Systems

An *IDS* is like a burglar alarm system for your network that is used to detect and alert on malicious events. The system might comprise many different IDS sensors placed at strategic points in your network. Two basic types of IDS exist: network-based (NIDS), such as Snort or Cisco Secure IDS, and host-based (HIDS), such as Tripwire or ISS BlackICE. NIDS sensors monitor network traffic for suspicious activity. NIDS sensors often reside on subnets that are directly connected to the firewall, as well as at critical points on the internal network. HIDS sensors reside on and monitor individual hosts.

In general, IDS sensors watch for predefined signatures of malicious events, and they might perform statistical and anomaly analysis. When IDS sensors detect suspicious events, they can alert in several different ways, including email, paging, or simply logging the occurrence. IDS sensors can usually report to a central database that correlates their information to view the network from multiple points.

Intrusion Prevention Systems

An *IPS* is a system that automatically detects and thwarts computer attacks against protected resources. In contrast to a traditional IDS, which focuses on notifying the administrator of anomalies, an IPS strives to automatically defend the target without the administrator's direct involvement. Such protection may involve using signature-based or behavioral techniques to identify an attack and then blocking the malicious traffic or system call before it causes harm. In this respect, an IPS combines the functionality of a firewall and IDS to offer a solution that automatically blocks offending actions as soon as it detects an attack.

As you will learn in Chapter 11, "Intrusion Prevention Systems," some IPS products exist as standalone systems, such as TippingPoint's UnityOne device. Additionally, leading firewall and IDS vendors are incorporating IPS functionality into their existing products.

Virtual Private Networks

A *VPN* is a protected network session formed across an unprotected channel such as the Internet. Frequently, we reference a VPN in terms of the device on the perimeter that enables the encrypted session, such as Cisco VPN Concentrator. The intended use might be for business partners, road warriors, or telecommuters. A VPN allows an outside user to participate on the internal network as if connected directly to it. Many organizations have a false sense of security regarding their remote access just because they have a VPN. However, if an attacker compromises the machine of a legitimate user, a VPN can give that attacker an encrypted channel into your network. You might trust the security of your perimeter, but you have little control over your telecommuters' systems connecting from home, a hotel room, or an Internet café. Similar issues of trust and control arise with the security of nodes connected over a VPN from your business partner's network.

Software Architecture

Software architecture refers to applications that are hosted on the organization's network, and it defines how they are structured. For example, we might structure an e-commerce application by splitting it into three distinct tiers:

- The web front end that is responsible for how the application is presented to the user
- The application code that implements the business logic of the application
- The back-end databases that store underlying data for the application

Software architecture plays a significant role in the discussion of a security infrastructure because the primary purpose of the network's perimeter is to protect the application's data and services. When securing the application, you should ensure that the architecture of the software and the network is harmonious.

De-Militarized Zones and Screened Subnets

We typically use the terms *DMZ* and *screened subnet* in reference to a small network containing public services connected directly to and offered protection by the firewall or other filtering device. A DMZ and a screened subnet are slightly different, even though many people use the terms interchangeably. The term DMZ originated during the Korean War when a strip of land at the 38th parallel was off-limits militarily. A DMZ is an insecure area between secure areas. Just as the DMZ in Korea was in front of any defenses, the DMZ, when applied to networks, is located outside the firewall. A firewall or a comparable traffic-screening device protects a screened subnet that is directly connected to it. Remember this: A DMZ is in front of a firewall, whereas a screened subnet is behind a firewall.

A screened subnet is an isolated network that is connected to a dedicated interface of a firewall or another filtering device. The screened subnet is frequently used to segregate servers that need to be accessible from the Internet from systems that are used solely by the organization's internal users. The screened subnet typically hosts "public" services, including DNS, mail, and web. We would like to think these servers are *bastion hosts*. A bastion is a well-fortified position. When applied to hosts on a network, fortifying involves hardening the operating system and applications according to best practices. As attacks over time have shown, these servers are not always well fortified; in fact, they are sometimes vulnerable despite being protected by a firewall. We must take extra care fortifying these hosts because they are the target of the majority of attacks and can bring the attacker closer to accessing even more critical internal resources.

Network Attacks #

Without security measures and controls in place, your data might be subjected to an attack. Some attacks are passive, meaning information is monitored; others are active, meaning the information is altered with intent to corrupt or destroy the data or the network itself.

Your networks and data are vulnerable to any of the following types of attacks if you do not have a security plan in place.

Eavesdropping

In general, the majority of network communications occur in an unsecured or "cleartext" format, which allows an attacker who has gained access to data paths in your network to "listen in" or interpret (read) the traffic. When an attacker is eavesdropping on your communications, it is referred to as sniffing or snooping. The ability of an eavesdropper to monitor the network is generally the biggest security problem that administrators face in an enterprise. Without strong encryption services that are based on cryptography, your data can be read by others as it traverses the network.

Data Modification

After an attacker has read your data, the next logical step is to alter it. An attacker can modify the data in the packet without the knowledge of the sender or receiver. Even if you do not require confidentiality for all communications, you do not want any of your messages to be modified in transit. For example, if you are exchanging purchase requisitions, you do not want the items, amounts, or billing information to be modified.

Identity Spoofing (IP Address Spoofing)

Most networks and operating systems use the IP address of a computer to identify a valid entity. In certain cases, it is possible for an IP address to be falsely assumed— identity spoofing. An attacker might also use special programs to construct IP packets that appear to originate from valid addresses inside the corporate intranet.

After gaining access to the network with a valid IP address, the attacker can modify, reroute, or delete your data. The attacker can also conduct other types of attacks, as described in the following sections.

Password-Based Attacks

A common denominator of most operating system and network security plans is password-based access control. This means your access rights to a computer and network resources are determined by who you are, that is, your user name and your password.

Older applications do not always protect identity information as it is passed through the network for validation. This might allow an eavesdropper to gain access to the network by posing as a valid user.

When an attacker finds a valid user account, the attacker has the same rights as the real user. Therefore, if the user has administrator-level rights, the attacker also can create accounts for subsequent access at a later time.

After gaining access to your network with a valid account, an attacker can do any of the following:

- Obtain lists of valid user and computer names and network information.
- Modify server and network configurations, including access controls and routing tables.
- Modify, reroute, or delete your data.

Denial-of-Service Attack

Unlike a password-based attack, the denial-of-service attack prevents normal use of your computer or network by valid users.

After gaining access to your network, the attacker can do any of the following:

- Randomize the attention of your internal Information Systems staff so that they do not see the intrusion immediately, which allows the attacker to make more attacks during the diversion.
- Send invalid data to applications or network services, which causes abnormal termination or behavior of the applications or services.
- Flood a computer or the entire network with traffic until a shutdown occurs because of the overload.
- Block traffic, which results in a loss of access to network resources by authorized users.

Man-in-the-Middle Attack

As the name indicates, a man-in-the-middle attack occurs when someone between you and the person with whom you are communicating is actively monitoring, capturing, and controlling your communication transparently. For example, the attacker can re-route a data exchange. When computers are communicating at low levels of the network layer, the computers might not be able to determine with whom they are exchanging data.

Man-in-the-middle attacks are like someone assuming your identity in order to read your message. The person on the other end might believe it is you because the attacker might be actively replying *as you* to keep the exchange going and gain more information. This attack is capable of the same damage as an application-layer attack, described later in this section.

Compromised-Key Attack

A key is a secret code or number necessary to interpret secured information. Although obtaining a key is a difficult and resource-intensive process for an attacker, it is possible. After an attacker obtains a key, that key is referred to as a compromised key.

An attacker uses the compromised key to gain access to a secured communication without the sender or receiver being aware of the attack.With the compromised key, the attacker can decrypt or modify data, and try to use the compromised key to compute additional keys, which might allow the attacker access to other secured communications.

Sniffer Attack

A *sniffer* is an application or device that can read, monitor, and capture network data exchanges and read network packets. If the packets are not encrypted, a sniffer provides a full view of the data inside the packet. Even encapsulated (tunneled) packets can be broken open and read unless they are encrypted *and* the attacker does not have access to the key.

Using a sniffer, an attacker can do any of the following:

- Analyze your network and gain information to eventually cause your network to crash or to become corrupted.
- Read your communications.

Application-Layer Attack

An application-layer attack targets application servers by deliberately causing a fault in a server's operating system or applications. This results in the attacker gaining the ability to bypass normal access controls. The attacker takes advantage of this situation, gaining control of your application, system, or network, and can do any of the following:

- Read, add, delete, or modify your data or operating system.
- Introduce a virus program that uses your computers and software applications to copy viruses throughout your network.
- Introduce a sniffer program to analyze your network and gain information that can eventually be used to crash or to corrupt your systems and network.
- Abnormally terminate your data applications or operating systems.
- Disable other security controls to enable future attacks.

Intrusion Detection Systems (IDSs)

An IDS operates as either network-based, when the technology is focused on protecting network information assets, or host-based, when the technology is focused on protecting server or host information assets

IDSs use one of two detection methods, signature-based or statistical anomaly-based

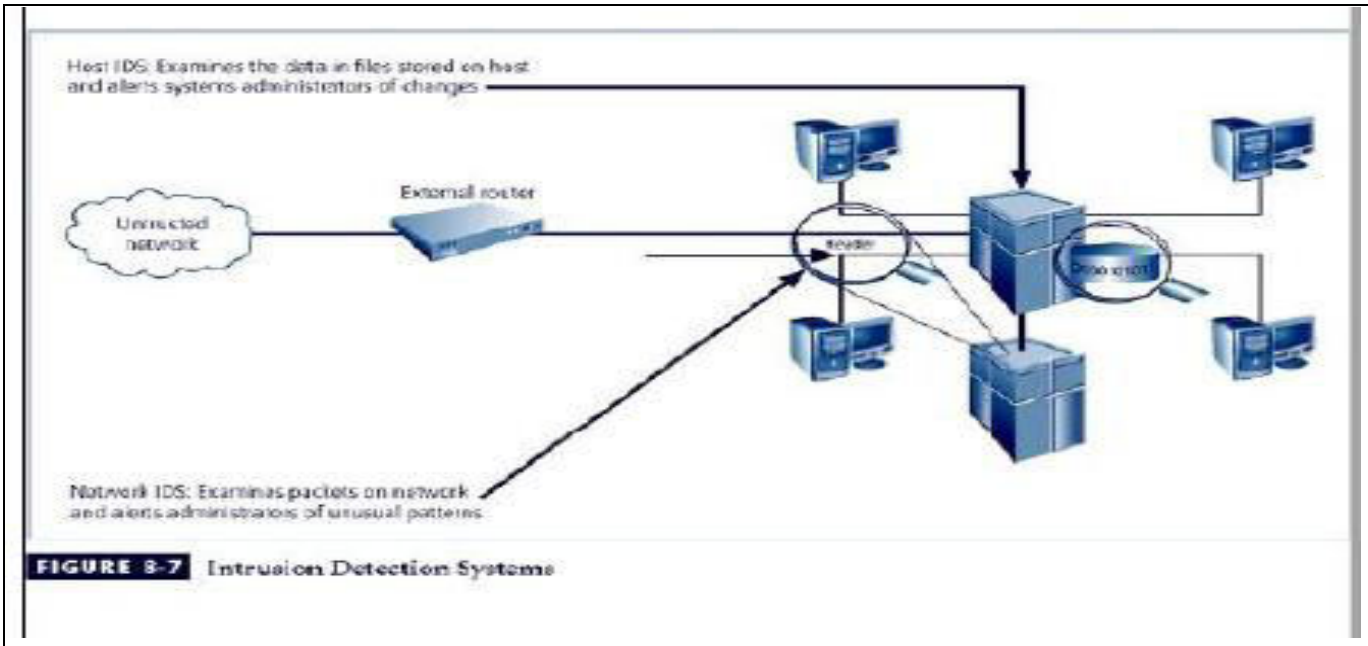


FIGURE 8-7 Intrusion Detection Systems

Different types of IDSs

a) **Network-based IDS**

A network-based IDS(NIDS) resides on a computer or an appliance connected to a segment of an organization's network and monitors traffic on that network segment,looking for indications of ongoing or successful attacks.

b) **Host-based IDS**

A Host-based IDS(HIDS) works differently from a network-based version of IDS.

While a netwerok-based-IDS resides on a network segment and monitors activities across that segment,a host-based IDS resides on a particular computer or server,known as the host and monitors activity only on that system. HIDs are also known as System Integrity Verifiers as they benchmark and monitor the status of key system files and detect when an intruder creates, modifies or deletes monitored files. A HIDs is also capable of monitoring system configuration databases, such as windows registries, in addition to stored configuration files like .ini, .cfg, and .dat files.

c) **Application-based IDS**

A refinement of Host-based IDs is the application-based IDS(AppIDS). Whereas the HIDs examines a single system for file modification, the application based IDs examines an application for abnormal incidents. It looks for anomalous occurrences such as users exceeding their authorization, invalid file executions etc.

d) **Signature-based IDS**

It is based on detection methods. A signature-based IDS (also called Knowledge- based IDs) examines data traffic in search of patterns that match known signatures – that is, preconfigured, predetermined attack patterns.

Many attacks have clear and distinct signatures such as

(i) footprinting and fingerprinting activities, have an attack pattern that includes the use of ICMP,DNS querying,and e-mail routing analysis

(ii) Exploits involve a specific attack sequence designed to take advantage of a vulnerability to gain access to a system

(iii) Denial of Service(DoS) and Distributed Denial of Service(DDoS) attacks.

e)**Statistical Anomaly-Based IDS**(Also called Behaviour-based IDS)

This approach is used for detecting intrusions based on the frequency with which certain network activities takes place. Statistical Anomaly-Based IDS collects statistical summaries by observing traffic that is known to be normal. A baseline is established based on normal period. The Stats IDs periodically sample network activity, and using statistical methods ,compares the sampled network activity to the baseline. When the measured activities are outside the baseline parameters,it is said to be exceeding the clipping level; at this point, the IDS will trigger an alert to notify the administrator.

f) **Log File Monitors(LFM)**

Log File Monitor(LFM) is an approach to IDS that is similar to NIDS. Using L Fm the system reviews the log files generated by servers, network devices, and when other IDSs. These systems look for patterns and signatures in the log files that may indicate an attack or intrusion is in process or has already succeeded.

What are Honey Pots, Honey Nets,and Padded Cell Systems?

A class of powerful security tools that go beyond routine intrusion detection is known variously as honey pots, honey nets,and padded cell systems. Oney pots are decoy systems designed to lure potential attackers away from critical systems and encourage attacks against the themselves. These systems are created for the sole purpose of deceiving potential attackers. In Industry they are known as decoys, lures, and fly-traps.

When a collection of honey pots connects several honey pot systems on a subnet,it may be called a honey net.

In sum, honey pots are designed to

i) Divert an attacker from accessing critical systems.

ii) Collect information about the attacker‘s activity

iii) Encourage the attacker to stay on the system long enough for administrators to document the event and, perhaps ,respond.

A Padded Cell is a honey pot that has been protected so that it cannot be easily compromised. In otherwords, a padded cell is a hardened honey spot..

The advantages and disadvantages of using honey pot or padded cell approach

Advantages:

 Attackers can be diverted to targets that they cannot damage.

 Administrators have time to decide how to respond to an attacker.

Attackers action can be easily and extensively monitored

 Honey pots may be effective at catching insiders who are snooping around a network.

Disadvantages:

 The legal implication of using such devices are not well defined.

 Honey pots and Padded cells have not yet been shown to be generally useful security technologies.

 An expert attacker,once diverted into a decoy system,may become angry and launch a hostile attack against an organization‘s systems

 Admins and security managers will need a high level of expertise to use these systems.

Scanning and Analysis Tools

 Scanners, sniffers, and other analysis tools are useful to security administrators in enabling them to see what the attacker sees

 Scanner and analysis tools can find vulnerabilities in systems

 One of the preparatory parts of an attack is known as footprinting – collecting IP addresses and other useful data

 The next phase of pre-attack data gathering process is called fingerprinting – scanning all known addresses to make a network map of the target

How Scanning and Analysis tools are useful in enforcing Information Security?

Scanning and Analysis Tools

 Scanners, sniffers, and other analysis tools are useful to security administrators in enabling them to see what the attacker sees

 Scanner and analysis tools can find vulnerabilities in systems

One of the preparatory parts of an attack is known as footprinting – collecting IP addresses and other useful data

The next phase of pre-attack data gathering process is called fingerprinting – scanning all known addresses to make a network map of the target

Need of Intrusion Monitoring and detection

- It's a dire fact that while every enterprise has a firewall, most still suffer from network security problems. IT professionals are acutely aware of the need for additional protective technologies, and network equipment vendors are anxious to fill in the gap.
- Intrusion Prevention Systems have been promoted as cost-effective ways to block malicious traffic, to detect and contain worm and virus threats, to serve as a network monitoring point, to assist in compliance requirements, and to act as a network sanitizing agent.

IDPSs are primarily focused on:

- Identifying possible incidents, logging information about them, attempting to stop them, and reporting them to security administrators.
- Identifying problems with security policies
- Documenting existing threats
- Deterring individuals from violating security policies.

In addition, all types of IDPSs perform the following:

- **Recording information related to observed events.** Information is usually recorded locally, and might also be sent to separate systems such as centralized logging servers, security information and event management (SIEM) solutions, and enterprise management systems.
- **Notifying security administrators of important observed events.** This notification, known as an *alert*, may take the form of audible signals, e-mails, pager notifications, or log entries. A notification message typically includes only basic information regarding an event; administrators need to access the IDPS for additional information.

Producing reports. Reports summarize the monitored events or provide details on particular events of interest.

- An IDPS might also alter the settings for when certain alerts are triggered or what priority should be assigned to subsequent alerts after a particular threat is detected.
- IPSs respond to a detected threat by attempting to prevent it from succeeding. They use several response techniques:
- **The IPS stops the attack itself.** Examples:

  Terminate the network connection or user session that is being used for the attack. Block access to the target (or possibly other likely targets) from the offending user account, IP address, or other attacker attribute. Block all access to the targeted host, service, application, or other resource.

- **The IPS changes the security environment.** The IPS could change the configuration of other security controls to disrupt an attack. Such as reconfiguring a network device (e.g., firewall, router, switch) to block access from the attacker or to the target, and altering a host-based firewall on a target to block incoming attacks. Some IPSs can even cause patches to be applied to a host if the IPS detects that the host has vulnerabilities.
- **The IPS changes the attack's content.** Some IPS technologies can remove or replace malicious portions of an attack to make it benign. An example is an IPS removing an infected file attachment from an e-mail and then permitting the cleaned email to reach its recipient.
- **Most IDPSs also offer features that compensate for the use of common evasion techniques.** *Evasion* is modifying the format or timing of malicious activity so that its appearance changes but its effect is the same. Attackers use evasion techniques to try to prevent IDPSs from detecting their attacks.
- **For example:** an attacker could encode text characters in a particular way, knowing that the target understands the encoding and hoping that any monitoring IDPSs do not. Most IDPSs can overcome common evasion techniques by duplicating special processing performed by the targets. If the IDPS can "see" the activity in the same way that the target would, then evasion techniques will generally be unsuccessful at hiding attacks.

Virtual Private Network

Virtual private network technology is based on the idea of tunneling. **VPN tunneling** involves establishing and maintaining a logical network connection (that may contain intermediate hops). On this connection, packets constructed in a specific VPN protocol format are encapsulated within some other base or carrier protocol, then transmitted between VPN client and server, and finally de-encapsulated on the receiving side.
For Internet-based VPNs, packets in one of several VPN protocols are encapsulated within Internet Protocol (IP) packets. VPN protocols also support authentication and encryption to keep the tunnels secure.

Types of VPN Tunneling

VPN supports two types of tunneling - voluntary and compulsory. Both types of tunneling are commonly used.

In voluntary tunneling, the VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). Then, the VPN client application creates the tunnel to a VPN server over this live connection.

In compulsory tunneling, the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. From the client point of view, VPN connections are set up in just one step compared to the two-step procedure required for voluntary tunnels.

Compulsory VPN tunneling authenticates clients and associates them with specific VPN servers using logic built into the broker device. This network device is sometimes called the VPN Front End Processor (FEP), Network Access Server (NAS) or Point of Presence Server (POS). Compulsory tunneling hides the details of VPN server connectivity from the VPN clients and effectively transfers management control over the tunnels from clients to the ISP. In return, service providersmust take on the additional burden of installing and maintaining FEP devices.

VPN Tunneling Protocols

Several computer network protocols have been implemented specifically for use with VPN tunnels. The three most popular VPN tunneling protocols listed below continue to compete with each other for acceptance in the industry. These protocols are generally incompatible with each other.

Point-to-Point Tunneling Protocol (PPTP)

Several corporations worked together to create the PPTP specification. People generally associate PPTP with Microsoft because nearly all flavors of Windows include built-in client support for this protocol. The initial releases of PPTP for Windows by Microsoft contained security features that some experts claimed were too weak for serious use. Microsoft continues to improve its PPTP support, though.

Layer Two Tunneling Protocol (L2TP)

The original competitor to PPTP for VPN tunneling was L2F, a protocol implemented primarily in Cisco products. In an attempt to improve on L2F, the best features of it and PPTP were combined to create a new standard called L2TP. Like PPTP, L2TP exists at the data link layer (Layer Two) in the OSI model -- thus the origin of its name.

Internet Protocol Security (IPsec)

IPsec is actually a collection of multiple related protocols. It can be used as a complete VPN protocol solution or simply as the encryption scheme within L2TP or PPTP. IPsec exists at the network layer (Layer Three) of the OSI model.

#VPN Authentication#

The VPN server can be configured to use either Windows or Remote Authentication Dial-In User Service (RADIUS) as an authentication provider. If Windows is selected as the authentication provider, the user credentials sent by users attempting VPN connections are authenticated using typical Windows authentication mechanisms, and the connection attempt is authorized using the VPN client's user account properties and local remote access policies.

If RADIUS is selected and configured as the authentication provider on the VPN server, user credentials and parameters of the connection request are sent as RADIUS request messages to a RADIUS server.

The RADIUS server receives a user-connection request from the VPN server and authenticates and authorizes the connection attempt. In addition to a yes or no response to an authentication request,

RADIUS can inform the VPN server of other applicable connection parameters for this user such as maximum session time, static IP address assignment, and so on.
RADIUS can respond to authentication requests based on its own user account database, or it can be a front end to another database server, such as a Structured Query Language (SQL) server or a Windows domain controller (DC). The DC can be located on the same computer as the RADIUS server or elsewhere. In addition, a RADIUS server can act as a proxy client to a remote RADIUS server.

The RADIUS protocol is described in RFC 2865 and RFC 2866 in the IETF RFC Database.
The VPN server can be configured to use either Windows or RADIUS as an accounting provider. If Windows is selected as the accounting provider, the accounting information accumulates on the VPN server for later analysis. Logging options can be specified from the properties of the **Local File** or **SQL Server** objects in the **Remote Access Logging**folder in the Routing and Remote Access snap-in. If RADIUS is selected, RADIUS accounting messages are sent to the RADIUS server for accumulation and later analysis.

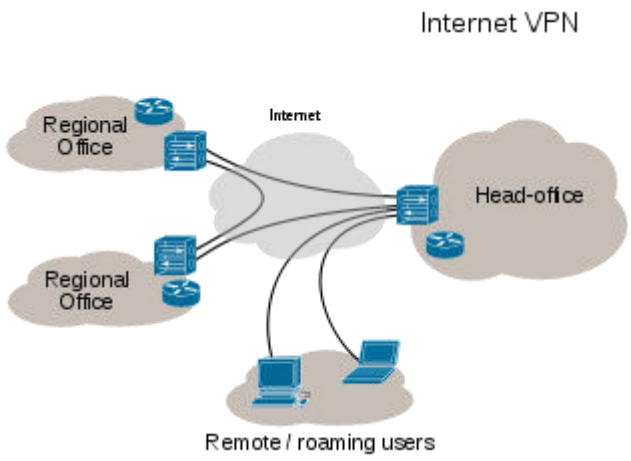
Most RADIUS servers can be configured to place authentication request records into an audit file. A number of third parties have written billing and audit packages that read RADIUS accounting records and produce various useful reports. For more information about RADIUS accounting, see RFC 2866 in the IETF RFC Database.

The VPN server can be managed using industry-standard network management protocols and infrastructure. The computer acting as the VPN server can participate in a Simple Network Management Protocol (SNMP) environment as an SNMP agent if the Windows Server 2003 SNMP service is installed. The VPN server records management information in various object identifiers of the Internet Management Information Base (MIB) II, which is installed with the Windows Server 2003 SNMP service. Objects in the Internet MIB II are documented in RFC 1213 in the IETF RFC Database.

Different Types of VPNs

Site-to-Site VPN

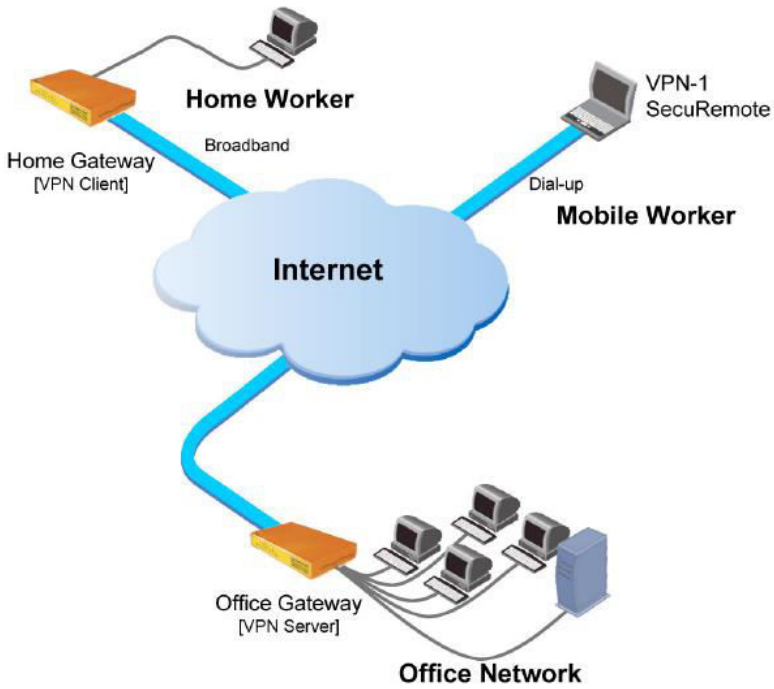
A **site-to-site VPN** allows two or more networks to be joined together. These networks use sophisticated encryption services to allow the connection to exist without hackers intercepting the traffic between the locations. Going back to our example, the connection between the branch office and its headquarters is an example of a site-to-site VPN. Users at both locations cannot tell that they are accessing network resources from another site because it is transparent to them.



Remote access VPN

A **remote access VPN** allows a user with a computer to access a private network. For example, I have a remote access VPN at my home that allows me to connect to my server, which stores all my music, documents from work, and photos of my family. I can access my VPN from my smart phone if I need something important.

A few years ago, I had to send my bank a copy of my home appraisal. At the time, I was located in California, and my home appraisal was stored on my computer, which was in Washington. Through my VPN, I was able to pull a copy of my appraisal and email it to the bank representative in a matter of minutes. With my remote access VPN, I saved a lot of money by not having to buy an airplane ticket to go back to Washington!



TYPES OF VPN PRODUCT

VPNs can be broadly categorised as follows2 :

1. A firewall-based VPN is one that is equipped with both firewall and VPN capabilities. This type of VPN makes use of the security mechanisms in firewalls to restrict access to an internal network. The features it provides include address translation, user authentication, real time alarms and extensive logging.

2. A hardware-based VPN offers high network throughput, better performance and more reliability, since there is no processor overhead. However, it is also more expensive.

3. A software-based VPN provides the most flexibility in how traffic is managed. This type is suitable when VPN endpoints are not controlled by the same party, and where different firewalls and routers are used. It can be used with hardware encryption accelerators to enhance performance.
4. An SSL VPN3 allows users to connect to VPN devices using a web browser. The SSL (Secure Sockets Layer) protocol or TLS (Transport Layer Security) protocol is used to encrypt traffic

between the web browser and the SSL VPN device. One advantage of using SSL VPNs is ease of use, because all standard web browsers support the SSL protocol, therefore users do not need to do any software installation or configuration.

#GENERAL VPN SECURITY CONSIDERATIONS#

The following is general security advice for VPN deployment:

1. VPN connections can be strengthened by the use of firewalls.

2. An IDS / IPS (Intrusion Detection / Prevention System) is recommended in order to monitor attacks more effectively.

3. Anti-virus software should be installed on remote clients and network servers to prevent the spread of any virus / worm if either end is infected.

4. Unsecured or unmanaged systems with simple or no authentication should not be allowed to make VPN connections to the internal network.

5. Logging and auditing functions should be provided to record network connections, especially any unauthorised attempts at access. The log should be reviewed regularly.

6. Training should be given to network/security administrators and supporting staff, as well as to remote users, to ensure that they follow security best practices and policies during the implementation and ongoing use of the VPN.

7. Security policies and guidelines on the appropriate use of VPN and network support should be distributed to responsible parties to control and govern their use of the VPN.

8. Placing the VPN entry point in a Demilitarised Zone (DMZ) is recommended in order to protect the internal network.

9. It is advisable not to use split tunnelling to access the Internet or any other insecure network simultaneously during a VPN connection. If split tunnelling is VPN Security Page 20 of 23 used, a firewall and IDS should be used to detect and prevent any potential attack coming from insecure networks.

10. Unnecessary access to internal networks should be restricted and controlled.

EXTRANET VPN SECURITY CONSIDERATIONS

The following are additional security considerations for extranet VPN deployment:

1. Strong user authentication mechanisms should be enforced.

2. The VPN entry point should be placed inside a DMZ to prevent partners from accessing the internal network.

3. Access rights should be granted on an as-needed basis. Only necessary resources should be available to external partners. Owners of these resources should review access permissions regularly.

CLIENT SIDE VPN SECURITY CONSIDERATIONS

The following are general security considerations for VPN users:

1. Strong authentication is required when users are connecting dynamically from disparate, untrusted networks, for example:

a) By means of certificates and/or smart cards, or tokens: A smart card is used to store a user profile, encryption keys and algorithms. A PIN number is usually required to invoke the smart card. A token card provides a one-time password. When the user authenticates correctly on the token by entering the correct PIN number, VPN Security Page 21 of 23 the card will display a one-time passcode that will allow access to the network.

b) By means of add-on authentication system, like TACACS+, RADIUS. This kind of central authentication system contains a profile of all VPN users, controlling the access to the private network.

2. Personal firewalls should be installed and configured properly on client VPN machines to block unauthorised access to the client, ensuring it is safe from attack. Many of the more recent remote access VPN clients include personal firewalls. Some may also include other configuration checks, such as the client not being able to connect to the network if anti-virus software is not running, or if virus signatures are out of date.

3. The client machine should have anti-virus software installed, with up-to-date signatures, to detect and prevent virus infections. 4. The user should remain aware of the physical security of the machine, in particular when authentication information is stored on the machine. 5. All users should be educated on good Internet security practices. Access from home should be considered an insecure channel, as traffic is routed over the Internet.

COMMON SECURITY FEATURES IN VPN PRODUCTS

The following are security features to look for when choosing a VPN product:

1. Support for strong authentication, e.g. TACACS+, RADIUS, smart cards / tokens.

2. Industry-proven strong encryption algorithms, with long key strength support to protect data confidentiality during transmission.

3. Support for anti-virus software, and intrusion detection / prevention features.

4. Strong default security for all administration / maintenance ports.

5. Digital certificate support, such as using certificates for site to site authentication

6. Address management support, such as the capability to assign a client address on the private network and ensuring all addresses are kept private.