Unit 1

Chp1.

INFORMATION SECURITY OVERVIEW

THE IMPORTANCE OF INFORMATION PROTECTION

* Data is nothing but a non-sorted content.
* Information is a sorted content.

INFORMATION :-

Q.1. What is Information? - 1M
what is its types? - 2M
explain its principle of Information Security - 2M

1. The Information is most important assets in organization & business.
2. The more information you have at your command, the better you can adapt to the world around you.
3. Information differentiaties companies and provides leverage that helps one company become more successful than another.
4. In order to control access to the information in different ways, depending on its importance, its sensitivity and its vulnerability to theft or misuse, organizations and businesses classify information in 2 types:-
   1. Unclassified Information / Unspecified Information - The information known to everyone.
   2. Top Secret - The Information to which only the most trusted people or parties have access.

5. Organizations classify information in different ways in order to differently manage aspects of its handling, such as labeling, distribution, duplication, release, storage, encryption, disposal and methods of transmission.
6. Information like internal memos, company announcements, meeting requests and general presentation materials is typically least restricted because spending a lot of time and money ~~are~~ on protecting it doesn't outweigh the value of the information or the risk of its disclosure.
7. Companies may have confidential information, this type of info is available to external audiences only for business-related purposes and only after entering a nondisclosure agreement (NDA) or equivalent obligation of confidentiality.
8. Specialized information or secret info may include trade secrets. It is usually restricted to only a few people or departments within a company and is rarely disclosed outside the company.
9. The principle of Information Security
   1. Confidentality -
      Only known users can access the resources & information.
      Only confidential person can communicate with each other.
   2. Integrity -
      The content of the message or information are

not changed or modified.
The content should be same at the sender as well as receiver side without modification is called as integrity.

3. Authentication -
The unique identity of the user. It's a mechanism to help to establish proof of identities.

4. Availability
Any services, information & resources are available at any time.

5. Non-repudiation
Once the user sends the message or information & later on refuse that message that he or she had sent.

10. CIA tried Model

Evolution Of Information Security

Q.3. Explain evolution of Information Security.

1. In networking, individual computers were connected together only in academic and government environments.
2. Thus, at the time, the networking technologies that were developed were specific to academic & government environments.

Academic Environment	Government Environment
1. Security model was "wide open".	1. Security model was "closed and locked".
2. Goal was to share info openly	2. Concerned with blocking access to computers, restricting internal access to confidential data.
3. It allows everything	3. It blocks everything.
4. Need More security as info is shared openly.	4. Needs less security as info is blocked.
5. Have full access from outsiders.	5. Have no access from outsiders.
6. Cost-effective	6. Less cost-effective.
7. Internet	7. Intranet
8. Network is vast	8. Network is small.

JUSTIFYING SECURITY INVESTMENT

1. First there was FUD - fear, uncertainty, debate & doubt. This didn't last long.
2. Thereafter, returns on investment (ROI) was used as an attempt to make security as an investment that "pays for itself".
3. This was a standard approach to justifying info technology budgets, but it never translated well to security. So, ROI was combined with annualized loss expectancy (ALE), a risk measurement strategy that combines a frequency of a loss with the cost of that loss, to produce a yearly expected monetary value, but ALE estimates were really not defensible.
4. The "insurance-analog" was developed as an alternative to value-based security justifications.
5. Business spend money on security because it's insurance against misuse of their assests.
6. Robust info security pratices not only reduce risks and costs, but also provide new opportunities for revenue.
7. Good security program allows companies to perform their operation in a more integrated manner especially with their customers.
8. Specific benefits of a strong security program are business agility, cost reduction and probability.

Y. IMP

Q4. Explain different security methodology.

SECURITY METHODOLOGY

1. Security is a paradigm, philosophy and a way of thinking.
2. Best approach to security is to consider every aspects asset in the context of its associated risk and its value, and also to consider its relationship among all assets and risks.
3. Info security is concerned with protecting information in all its forms, whether written, spoken, electronic, graphical or using other methods of communication.
4. Network security is concerned with protecting data, hardware and software on a computer network.
5. Basic concepts such as assets identification & valuation, threat definition & risk analysis, and processes & mechanism to protect assets apply equally well.
6. At its core, the pratice of security is all about reducing risks to assets to acceptable levels, so as that risk is still mitigated & controlled even when one control fails.
7. If you're trying to protect a network of computers a focus only on the security of those computers lead to vulnerabilities and/or risks that attackers might exploit to bypass your protective mechanisms.
8. The basic principles apply equally well to any

situation or environment, regardless whether you apply them to defend computers, networks, people, houses, or any other assets.

9. The basic assumption of security are as follows:
   - We want to protect our assets.
   - There are threats to our assets.
   - We want to mitigate those threats.

10. Three aspects of security which are considered as the three Ds of security can be applied to any situation
    1. Defense
    2. Defection Defensive Detection
    3. Deterrence./Detection

11. Defense – Defense is often the first part of security that comes to mind and usually it is the easiest aspect for people to understand. The desire to protect ourselves is instinctive, and defense usually precedes any other protective efforts.
Defensive measures reduce the likelihood of successful compromise of valuable assets, thereby lowering risk & potentially saving the expenses of incident.
Defensive controls on the network can include access control devices such as stateful firewalls, network access control, spam and malware filtering, web content filtering., and change control processes. These controls provide protection from software vulnerabilities, bugs, attack scripts, ethical & policy violations, accidental data damage.

However, defense is the only one part of a complete security strategy.

12. Detection -

Detective controls include :- video surveillance cameras, motion sensors, house or car alarm system.

Detective controls on the network include :- audio trails & log files, system & network intrusion detection and preventions system, and security information & event management alerts, reports and dashboards. and all controls are monitored by using SOC (security operation center).

13. Deterrence -

It is considered an effective method of reducing the frequency of security compromises & thereby the total loss due to security incidents. Deterrent controls include communication programs to employees about acceptable usage & security policies, monitoring of web browsing behaviour, training programs to employees & they signatures on agreement indicating that they understand & will compily with security policies. By using these controls, attackers may decide not to cause damage.

14. Each of the Ds is equally important and each complements the others.

15. A defensive strategy keeps attackers at bay and reduces internal misuse and accidents.

16. A detective strategy alerts decision makers to

violations of policy and other security events.

17. A Deterrent strategy discourages attempts to undermine the business goals & processes and keeps resource efficiently focused on productive efforts.

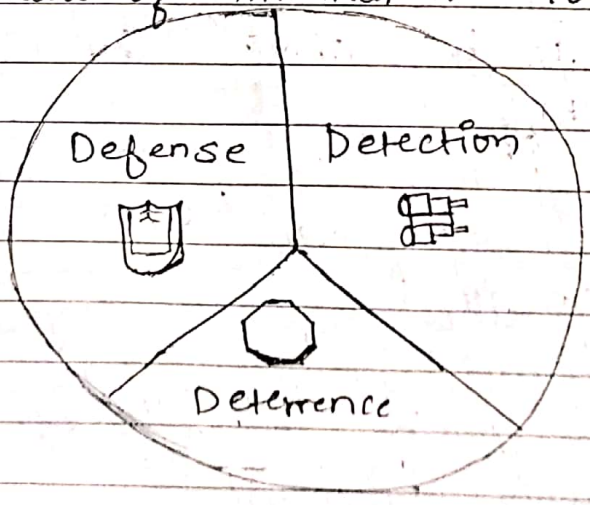
18. A security effort that employs all three Ds provides strong protection.

19. When only one or two of three aspects of security are applied to network, exposures can result.

20. A network that only use defense & detection without deterrence result in internal attacks, misuse & accidents.

21. A network that fails to employ a detection faces exposure to all failures of defensive and deterrent controls.

22. Employing no defensive controls on a network exposes that network to any of the well-known threats of internal or external origin.



23. Worms or Viruses will attack step by step:-
    1. Infection
    2. Replication
    3. Attack

V.IMP

Q.5. How to build Security program

BUILDING A SECURITY PROGRAM

Components:-

1. Authority
   1. The Security program must include the level of responsibility and authorization to be effective.
   2. A Security program charter defines the purpose, scope and responsibilities of the security organization and gives formal authority for the program.
   3. The responsibilities like physical security, information protection, risk management disaster-recovery & business-continuity plans etc varies by company, but should be clearly specified in security program charter which should be authorized by the company executive staff.
   4. A Resource plan is an ongoing strategy for providing the headcount needed to operate the security functions.
      It describes how the employees, contractors consultants, service providers & temporary workers will be leveraged to fuel the progress of security implementations, operations & improvement.
      - MRP - Manufacture Resource Planning
      - CRM - Customer Relation Mgmt

• SCM - Supply Change Mgmt.

2. Framework

1. A security framework provides a definsible approach to building the program.
2. The security policy provides a framework & also describes the intent of executive management with respect to what must be done to comply with the business requirements.
3. Standards are the appropriate place for product-spefic specific configurations to be detailed. These are doumented to provide continuity & consistency in the implementation & management of network resources.
4. Guidelines should be doumented clearly for the sake of the people who use these technologies: software, computer systems & nlw.

3. Assessment

1. Assessment - Assessing what needs to be protected, why, and how leads to a strategy for improving the security posture.
2. A risk analysis provides a perspective on current risk to the organization's assests. This result in a well-defined set of risks that the organization is concerned about that can be ~~mig~~ mitigated, transfered, or accepted
3. A gap analysis compares the desired state of the security program with the actual current state and identifies the differences.
4. Remediation planning takes into account the risks, gaps & other objectives to & puts them

together into a prioritized set of steps to move the security program from where it is today to where it needs to be at a future point.

4. Planning

1. Planning produces priorities and timelines for security initiatives.
2. A roadmap is a plan of action for how to implement the security remediation plan. It describes when, where & what is plan. Useful for managers who need the info to plan activities. Relatively a high-level docum
3. that contains - info about activities & upcoming milestones.
3. The security architecture documents how security technologies are implemented, at a relatively high-level. Driven by security po & identifies what goes where.
Good tool for architecture doc is block diagram - a diagram shows various com -ents at a relatively high level of security architecture. so the reader can see how com -nents work together.
4. The project plans detail the activities the individual contributors to the variou security implementations.
A good design project plan opens with analysis phase followed by design phase it the implementation phase is done done

5.

6.

followed by testing phase.

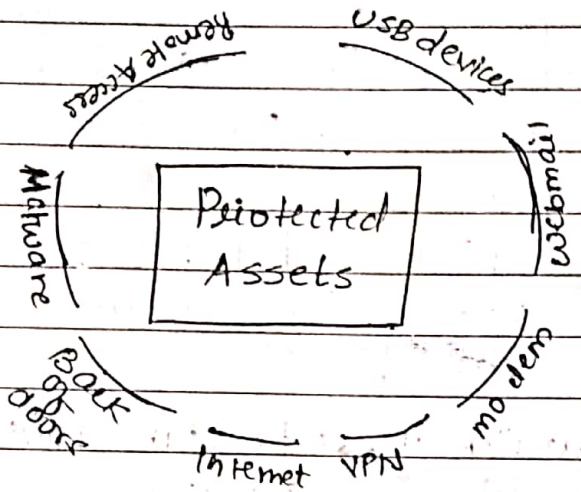
5. Action
1. The actions of the security team produces the desired results based on the plans.
2. Procedures describes how the processes are performed by people on an ongoing basis to produce the desired outcomes of the security program in a repeatable, reliable function. fashion.
3. ~~Maintaining~~ Maintenance & support are part of maintaining the ongoing operations of the security program and its associated technologies, as part of a normal life cycle of planning, updating, reviewing & improving.
4. The actions that should be taken when a security event occurs are defined in the incident response plan. Advanced planning helps shorten response time & provides repetable, reliable & effective actions to limit the scope & damage of an incident.

6. Maintenance
1. The end stage of the parts of the security program that have reached maturity ~~to~~ is to maintain them.
2. Policy enforcement is necessary to ensure that the intentions of management are carried out by the various people responsible for the behaviou and actions defined in the security policies.
3. Security awareness programs are used to

educate employees, business partners, and o
stakeholders about what behaviours are ex
of them, what actions they should take und
various circumstances and what consequen
may ensue if they don't follow the rules

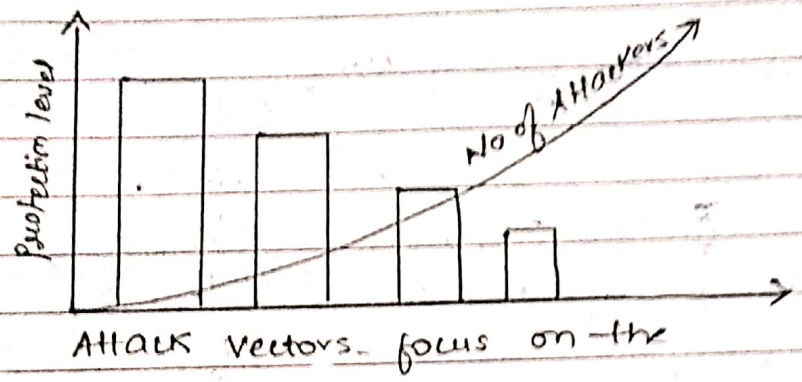
4. Ongoing guidance for business projects, daily operations & general walk-up questions is an important part of a security program. Someone should be available to advise the business on the best way to do things in a secure manner.

THE IMPOSSIBLE JOB



1. The job of attacker is always easier than the job of the defender because attacker needs only to find one weakness while the defender must try to cover all possible weakness of vulnerabilities.
2. The attacker has no rules, & can follow unused path, abuse the trust of the system & resort to destructive practice.
3. The defender must try to keep their assets intact, minimize damage & keep cost down.
4. The attackers have advanced knowledge of different tools technique as compared to every defender.
5. Defender can use 3 different process to perform the risk assessments.
   1. Mitigation is process of defense.
   2. Transference is process of insurance.
   3. Acceptance is deviding the risk that does not require any action.

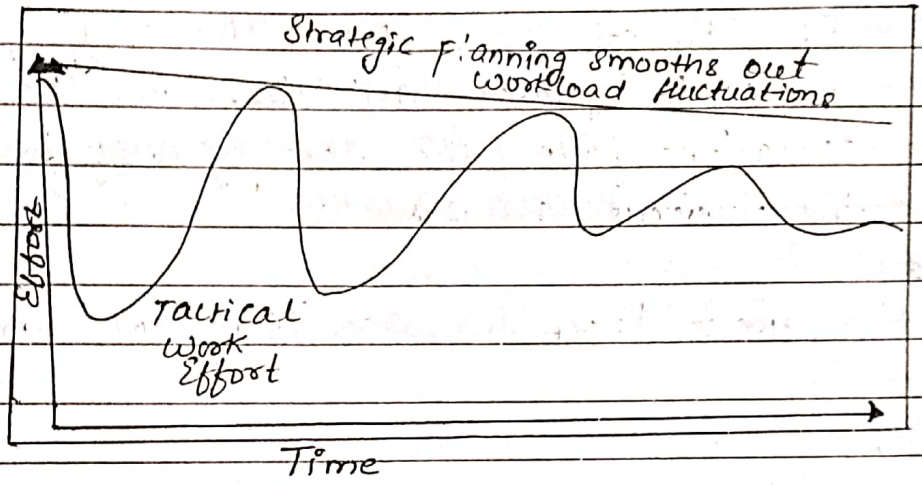
WEAKEST LINK



1. Every security infrastructure will drive an attacker to the weakest link.
2. The weakest link is a graph that source the attack the greatest number of attacks in the security infrastructure.
3. All security controls should complement each other & each should be equally as strong as th This principle is called equivalent security or transitive security.
4. In the computer network firewall are obtained the strongest point of defense.
5. Firewalls provides the security in different wa
   1. Scanning the port number.
   2. Scanning the IP address of package.
   3. Detecting the interface between the sourc & destination.
   4. Protecting the protocols with the port number.
6. In any case, weak points should be avoide and in situations where are neccessar due to business requirement then detective

deterrent security controls should focus on the areas where defensive weak point exist.
7. You can expect these weak points to attract attackers, and you should plan accordingly.

STRATEGY AND TACTICS



1. A security strategy is the definition of all the architecture and policy components that make up a complete plan for defense, detection & deterrence.
2. ~~Strateg~~ Security tactics are the day-to-day practices of the individuals and the technologies assigned to the protection of assets.
3. Strategies are proactive tatics are reactive.
4. A successful security program needs to be both strategic and tactical in nature
5. Strategic planning can be proceed weekly, monthly, quaterly & early basis whereas tactics are day to day basis.
6. The figure shows the interplay of strategic and tatics. As time progresses & strategic

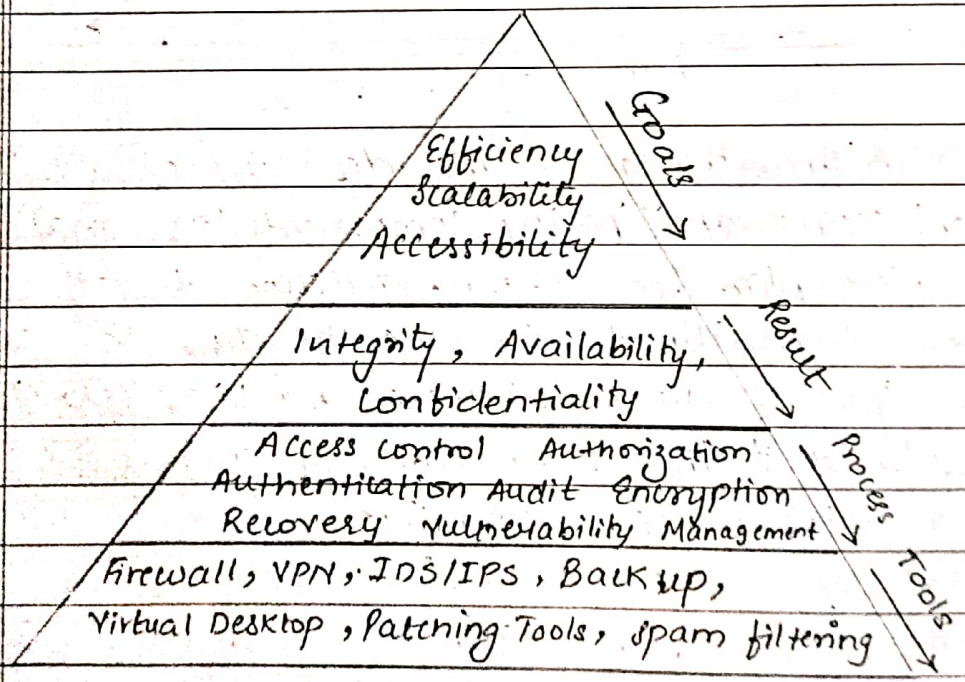
planning is employed, ~~then~~ tactical operati should begin to require less effort because the strategy should simplify the operation & business processes.

7. In ideal situation, strategy and tactics a at equilibrium.

8. The strategic focus paves the way for quater-to-quater activities, and the tactic operations follow the strategy set forth in the previous quaters.

9.

BUSINESS PROCESSES VS TECHNICAL CONTROLS



1. In security, there is no magic bullet. A magic bullet means a single security devi product, or technology that provides complete protection against all threats.

2. Some security products are marketed as

9.6

"security-in-box" solutions that provide all the security a company needs.

3. Security technologies need to be selected on the basis of business context, so they are targeted toward specifically identified risks with clear objectives.

4 ~~for Eg~~ :- ~~pv~~ The ~~tools~~ technical tools should be considered within a business process in order to be effective.
For Eg :- buying a database does not solve the problem of how to manage customer data.
Customer data management is a business process than can be faulitated by a database.

5. The figure above shows the principles of business objective priorities & processess drive to selection.

6. Any security implementation is a snapshot and as technology & business environment evolve over time, the technical controls that are part of this snapshot will become less and less appropriate.

7. Before selecting security product, the business process must be identified so that security products can be chosen that fit appropriately into business environment.

8. Make these assumption when considering security :-
1. You can never be 100 percent secure.
2. You can, however, manage the risk to your assets
3. You have many tools to choose from to manage risk.

Q.6 Explain the different business process with technical controls.

Explain different types of attacks?

Page No.
Date

12/12/18

Chp 2

RISK ANALYSIS

Migitating risk does not mean eliminating it means reducing them to an acceptable (IM)

Q.1. What is threat? Explain different types of threa

THREAT DEFINITION

1. Threat is a small kind of infected progra By identifying threats, you can give your security strategy focus & reduce the chan of over working imp stant areas of risk tha might otherwise remain unprotected.
2. The consideration should take into aboun into the following aspects of threats:-
   1. Threat Vector
   2. Threat Sources & Targets
   3. Types of Attacks
   4. Malicious Mobile Code
   5. APTs (Advanced Persistent Threats)
   6. Manual Attacks
3. Sewrity professionals know that many real- threats come from inside the organization.
4. Regardless of the breakdown for your partia organization, you need to make sure your security controls focus on the right threats.

1. THREAT VECTORS

1. A threat vector is a term used to describe where the threats originates and the path it

Write one example each for Trojan, Virus, Spam & worms.

Page No. 21
Date

takes to reach a target.

2. A good way to identify potential threat vectors is to create a table containing a list of threats you are concerned about, along with sources and targets.

3. Choosing different combinations of sources, threats and targets produces interesting varieties of threat vectors, which helps with the process of brainstorming & enumeration.

4. Many different analysis of threat vectors are published. One of the best publisher is computer security Institute (CSI) which identifies particular threat vectors and their frequency.

5. Eg. Insider a threat vectors take many forms:- For Eg:- trojan programmer & viruses compromise computers on trusted internal network.

6. Trojan - (i) Trojan programs are covertly installed pieces of software that perform functions with the privileges of authorized users, but unknown of those users.

(ii) Trojan functions include stealing data and passwords, providing remote access and/or monitoring to someone outside the trusted network, or performing specific function such as spamming.

(iii) Trojan are dangerouse because they can hide themselves in authorized communication channels such as web browsing.

(iv) Trojan may be installed by authorized internal staff, by unauthorized people who gain physical or network access to system, or by viruses.

7. Viruses - (i) Virus typically is a small infected program arrived in a document, executable files and e-mail.
eg:-
(ii) They may include trojan component that allows direct outside access or automatically sys private information to a reciver on Internet.

8. Spam - (i) It is the small email attachment that exploits the access rights of the person who opens the attachment to send confidential information out to the internet. eg:-

9. Worms - (i) A small infected program running on the unwanted website.
eg:- A girlfriend expolit attack which was coined by early attackers in the late 1980's, refers to a Trojan program planted by an unsuspecting employee who run a program provided by a trusted friend from a storage device like a disk or USB stick, that plants a backdoor also known as trap door inside the network.

10. A risk analysis that includes consideration of all major threat vectors helps ensure that the security controls will be effective against the real risks to the organization.

2 THREAT SOURCES AND TARGETS

(i) Security controls can be logically group into several categories:-

1. Preventive - Block security threats before they can exploit a vulnerability.

Q.2. Explain the different security controls in threat sources to protect against threat controls.

2. Detective - Discover and provide notification of attacks or misuse when they happen.
3. Deterrent - Discourage outsider attacks and insider policy violations.
4. Corrective - Restore the integrity of data or another asset.
5. Recovery - Restore the availability of a service.
6. Compensative - A layered security strategy, provide protection even when another control fails.

2. Each category of security control may have a variety of implementations to protect against different threat vectors. → (2½ M)

1. Physical - Controls that are physically present in the real world.
2. Administrative - Controls defined & enforced by management.
3. Logical / Technical - Technology controls performed by machines.
4. Operational - Controls that are performed in person by people.
5. Virtual - Controls that are triggered dynamically when certain circumstances arise.

TYPES OF ATTACKS

1. Any computer that is accessible from the Internet will be attacked.
2. 1. Malicious Mobile code

There are 3 malicious mobile code

1. Virus

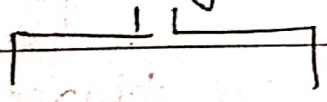
2. worms
3. trojan.

2. In addition many malware programs have components that act like 2 or more these types of threat, which are called as Hybrid threa mixed threat.

3. The lifecycle of malicious mobile code is
   1. find
   2. Exploit
   3. Infect
   4. Repeat

TYPES OF VIRUSES (Sneth publication) (Sir r

1. Non-resident virus
   If the virus executes, ~~then~~ does it the damage
2. Memory resident virus
3. Stealth virus
4. Boot sector virus
5. Over writing virus



Prepending virus Appending virus

6. Parasitic virus.

Page No.
Date

Q. Explain risk analysis with different approach.

Risk Analysis.

Qualitative ALE = SLE * ARO

ALE - Annual loss expectancy
SLE - Single loss expectancy
ARO - Annual Rate of occurrance

The Risk analysis process identifies the probable consequence or risk associated with ~~warranti~~ vulnerabilities or weakness & provides the basis or establishing the most effective program Risk management is the process of implementing & maintaning counter measures that reduces the effect of risk to an acceptable level.
Risk assessment in the process of calculating assests in the security program.
There are 2 main approach to risk analysis are quantitative & qualitative approach.

1. Qualitative Approach

Qualitative risk analysis typically mean assessing the likelihood that the risk will appear based on subjective quality & the impact it could have on an organization using predefined ranking scales. Eg. the perception is represented in scale such as low, medium or high as per the rating.

2. Quantitative Risk analysis

Quantitative risk assesment focuses on factual & measurable data & highly on mathematic &

Chp3 - Sir Notes.

Page No.
Date

computational bases to calculate probability impact value.

ALE = money expected to be loss in one year considering SLE & ARO

SLE = money expected to be loss if the incide to be one time.

ARO = How many times in 1 year intervals th incident is expected to occur.

ALE = SLE * ARO

Unit 2

Chp1

AUTHENTICATION & AUTHORIZATION

★ Authentication

Types of Authentication

★ Protocol / System in Authentication.

Q1. What is authentication & explain different types of authentication

Q2. Explain different types of protocols / system authentication.

Q3. Explain the authentication verification proce in Kerberos or SSL?

Page No.
Date

Protocol / system in authentication.

1. Local Storage & Comparison
In this system all the username & password were entered in the localized system database by administrator & were provided to users.
All the password were stored in the database in plain text format.
For eg:- In early unix system password were stored in file is called as /etc/passwd
Again after several highly publicized compromises, the system was re-designed to store the file in the encrypted file is known as /etc/shadow.
Today many off the shelf application use the central authentication system such as LDAP (Light weight directory access protocol).

2. Central Storage & Comparison
In this system centralized account databases that resides on remote host, sometimes the password entered by the user is encrypted, passed over the network & then compared by remote server to its stored encrypted password.
In this network applications, remote authentication algorithm is used such as PAP (password authentication protocol)

3. CHAP

The sending authentication credentials a the network can not be easily intercept replay is to used the challenge & respon authentication algorithm such as CHAP & M This both protocols used MD5 algorithm (message digest).

4. Kerberos

Kerberos is the protocol for authenticating service request between trusted host across untrusted network such as internet.

Kerberos is built in to all major operatin systems like microsoft windows, Mac OS, BSD & Linux

It is a network authentication system ba on the use of tickets.

5. OTP

It is also known as one time pin is a password that is valid for only one login session or transaction on a computer system or digital device.

Two current methods that use one-time passwords are:-

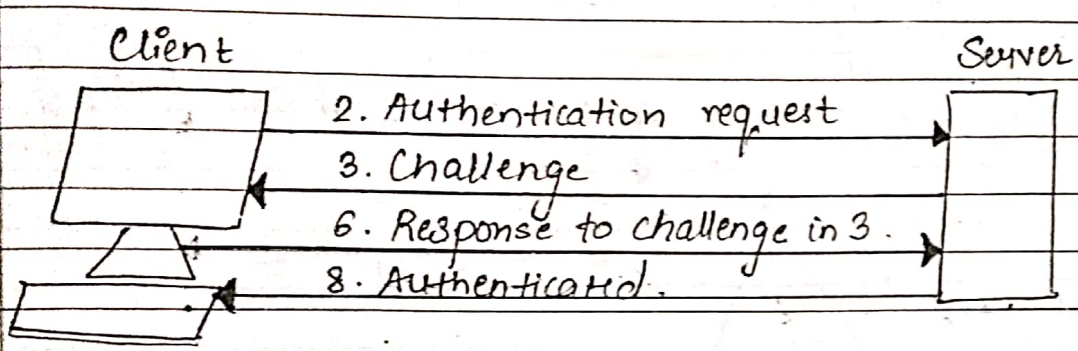
1. Time-based Keys
2. Sequential Keys

1. 1. Time-based Keys uses hardware or soft based authentication that generates a ran seed based on the current time of day.

Page No.
Date

2. Authentication code changes every 60 seconds so the password will also change each time it's used.
3. This system is a two-factor system since it combines the use of something you know, the PIN and something you have, the authenticator.

2. Sequential Keys provide a difense against passive eavesdropping and replay attacks.



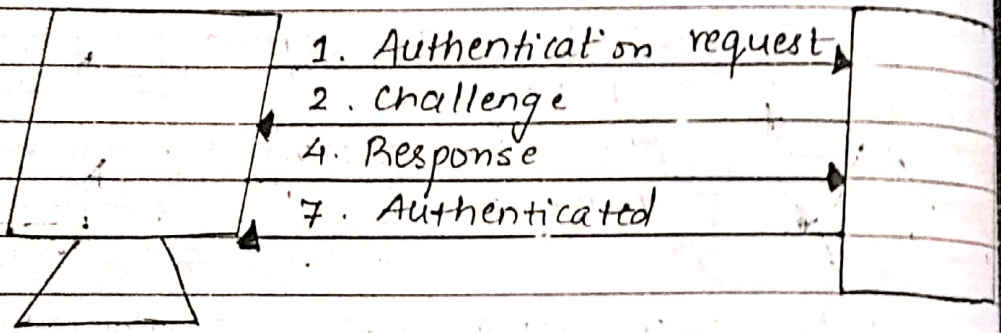
1. User enters passphrase
4. Generator generates password
5. Entry of password into the system encryption
4. Generator generates password
7. Evaluation of response.

The Sequential Key one-time password process is a modified challenge and response authentic-ation system.

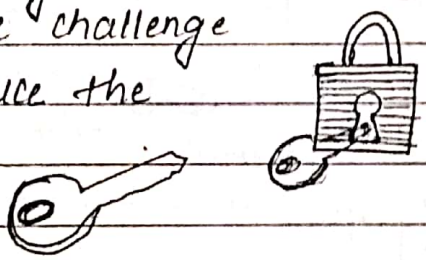
Certificate - Based Authentication

1. A certificate is a collection of information that binds an ~~identify~~ identity to the public key of a public/

private key pair.
2. It includes information about the Iden & specifies the purpose for which the cert maybe used.
3. The certificate is digitally signed by the Issuing authority, the certificate authority
4. The infrastructure used to support certific in an organization is called the Public Key infrastructure (PKI)



3. Private Key used to encrypt the challenge and produce the response



5. Public Key of clie to decrypt
6. Response com to challenge.

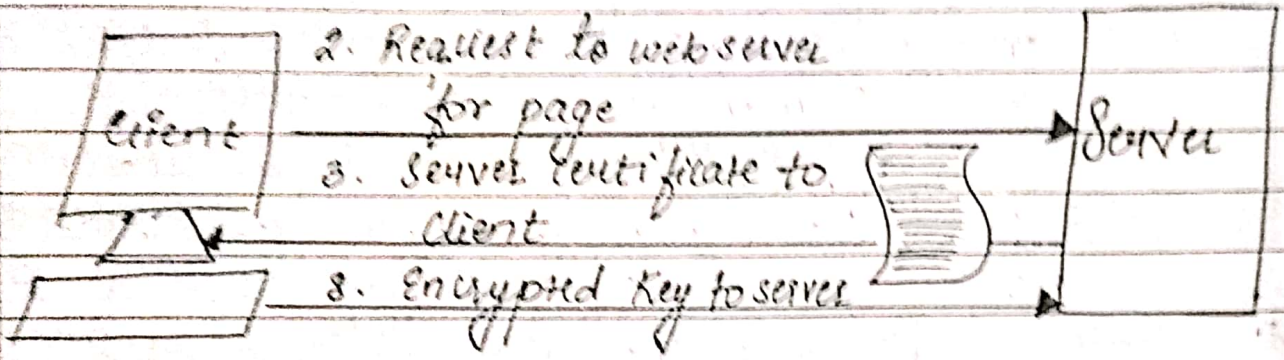
Certificate Authentication uses public & private keys.

SSL / TLS

Secure Socket Layer (SSL) is a certificate- system that is used to provide authenticati of secure web servers and clients and

share encryption keys between servers and clients.

Transport Layer Security (TLS) is the Internet standard version of the proprietary SSL.



1. URL entered in browser
4. Browser looks for certificate in store
5. Checks signature on cert using public key of CA.
6. Accepts
7. Generate symmetric key using server's public key
5. Public key of client used to decrypt response
9. Symmetric key decrypted using own private key

SSL can be used for server authentication and to provide secure communications between a web server and a client.

Page No.
Date

Q4. Explain the following terms in Authentication
1. Biometric 2. EAP.

BIOMETRIC

1. It is a security mechanism used to authen and provide access to a facility or system ba on the automatic and instant verification of an individual's physical characteristics.
For eg:- ~~fingerprints~~, voice regonization, Hand Bitte
2. Biometric security is mainly implemented in environments with critical physical securit requirements, this include fingerprints, eye texture, voice & face recognization etc

EAP Extensible Authentication Protocol

1. It was develop to allow pluggable module be incorporated in and overall Authenticatio process.
2. EAP is currently implemented in several remote access system including RADIUS (Remote Authentication dial in user service)
3. Two different models in EAP #1
1. EAP/TLS 2. EAP/MD5-CHAP.

EAP/TLS - Uses the TLS authentication protoc and provides ability to use smart cards for remote authentication.

EAP/MD5-CHAP - Allows the use of username passwords by organizations.

AUTHORIZATION

Q. What is authorization ? Explain different types of authorization.

Authentication establishes who the user is; authorization specifies what the user can do. It is security mechanism used to determine user/client privileges or permission and access levels related to the system resources that including computer programs files, information or data, services, application features.
There are 4 different types of authorization

1. User Rights

User rights management is a security mechanism that controlling which resource that the user can access and what kind of action that the user will perform on those resource.

2. Role Based

Role based authorization is used RBAC approach (Role Based Access Control) in the computer system security that sometimes refer to as role based security.
RBAC is a policy neutral control mechanism i.e define _ and previliges of the users.

3. Rule Based

It requires the development of rules that stipulate what the specific user can do on the

System.

For eg :- User A can access the resource x but cannot access the resource y.

4. ACL (Access Control List)

It is a table that tells the computer os which access rights that each user has to a particular system object such as file directory or individual file.

Page No.
Date

Ch 5 ENCRYPTION

Q.1 What is cryptography? Explain different types of cryptography.

Cryptography is the science of data protection via encryption.
It protects the integrity of data while the data is carried from one place to another.
Contents of data would be rearranged in order or replaced or substituted with other symbols, characters, numbers or even pictures.
Two types of cryptography are:-
1. Symmetric -Key
2. Public -Key

1. Symmetric - Key Cryptography
1. It uses the same algorithm and key to both encrypt and decrypt digital data.
2. The unencrypted data is called as plaintext & the encrypted data is called as ciphertext.
3. The key must be known to both the sender and receiver that is the secret.
4. Secret Key ~~con~~ cryptography schemes are categorized in 2 types:-
1. Stream cipher
2. Block cipher
1. Stream cipher - The plain text is processed one bit at a time.

Q2]. Explain PKI with different components.

Page No.
Date

Steam cipher is mainly two forms:-

1. Self-synchronizing stream cipher → calculates each bit in the keystream as a function of the previous n bits in the keystream.
2. Synchronous stream cipher → generates the keystream in a fashion independent of the message stream but by using the same keystream generation function at sender and receiver.

2. Block cipher - The plain binary text is processed in blocks of bits at a time.
The no of bits in a block is fixed.
It operates in one of several modes
1. (ECB) Electronic Codebook.
2. Cipher Block chaining (CBC)
3. Cipher Feedback (CFB)
4. Output Feedback (OFB)
5. Counter (CTR)

2. Public Key Cryptography
1. It involves a pair of key known as public key and a private key.
2. In PKC, one of the keys is designated as public key & may be advertised as widely as the owner wants. The other key is designated as private key and is never revealed to another party.
3. PKC enables the following:-
1. Encryption and Decryption

2. Non Repudiation which prevents:-
   - Sender of the data from claiming, at a late date, that the data was never sent.
   - The data from being altered.
3. How freely public key data can be distribute so that only the owner of private key can read data that was encrypted with the public key.
4. Most important properties of PKC Schemes:-
   1. Different keys are used for encryption and decryption.
   2. Each receiver possesses a unique decryption key, referred as private key.
   3. Receiver needs to publish an encryption key, referred to as public key.
   4. Encryption algorith ~~mt~~ is complex enough to prohibit attacker from deducing plaintext.
   5. It is not feasible to calculate the private key from public key.
5. Two Best-known uses of PKC are:-
   1. Public Key encryption
   2. Digital signatures

Public Key Infrastructure

1. It is a database server or a security infrastructure that provides private public keys and digital signature services.
2. It is the framework in which the entire process of managing keys, ~~certificate~~ creating and distributing digital certificates takes place.

3. It is the system or server for storing & maintaining encryption / decryption Key.

4. PKI consist of :-

1. Registeration authority (RA) - It is used to identify identity of entities that requ their digital certificates to be stored at CA.

2. Certificate authority (CA) - It is used to cr issues and signs the digital certificates.

3. Certificate Mgr. it System - It is used to ma things like the access to store certificates the delivery of the certificate to be issued.

4. Central directory - It is a secure location used to store private / public keys.

5. Policy - It is a set of rules and regulati that stating the PKI requirements concer its procedure.

It's purpose is to allow outsiders to ana the PKI trust worthiness.

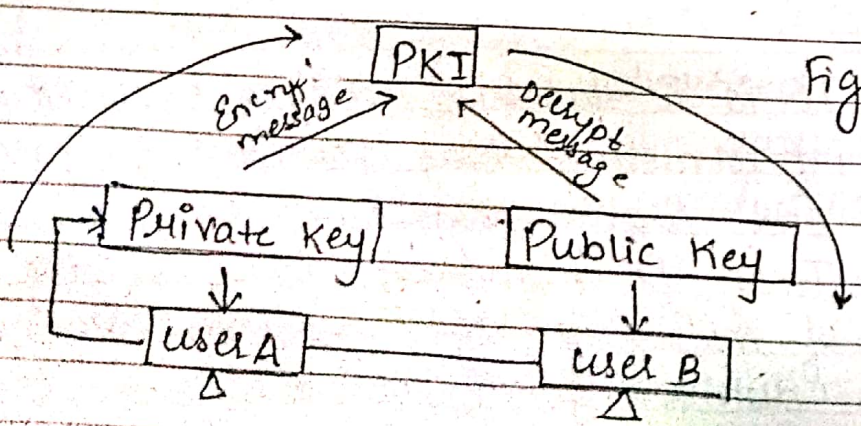


Fig :- PKI overvie

Page No.
Date

Q. Explain the following terms in PKI

1. Digital Certificates
2. CA's Hierarchy
   ① Root CA ② Intermediate CAs
   ③ Issuing CA
3. CRLs.

Benefits of PKI
1. Security Advantage
2. Non-Repudiation Advantage
3. Administrative Advantage

Risks of PKI
1. Protection of CA's Private Key.
2. Protection of Individual Private Keys.

Q.5] What is PKI & Explain advantages & disadvantages.

Q.6] Explain the difference between symmetric & assymetric types of cryptography.

Chp6

STORAGE SECURITY

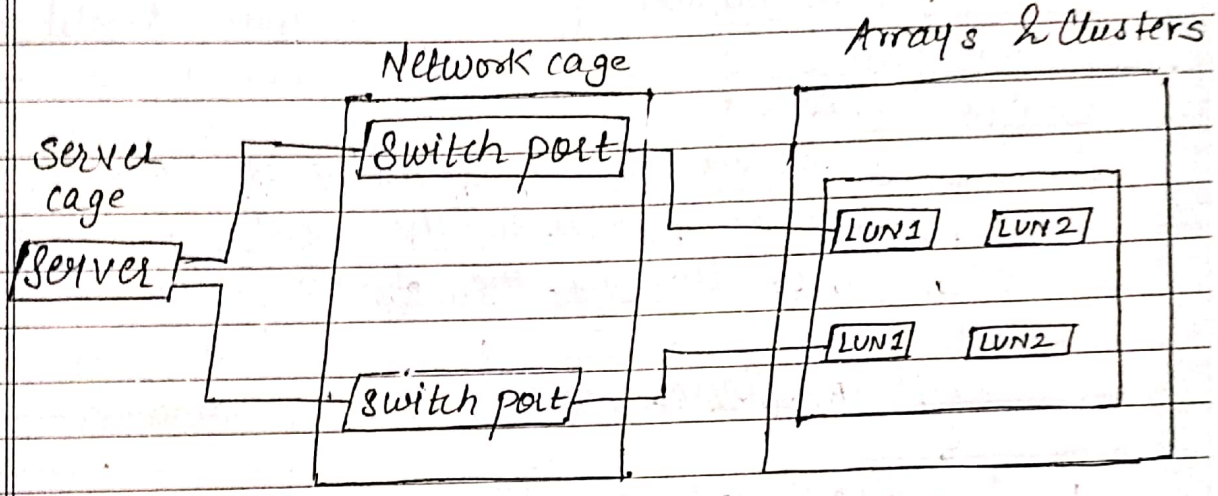
Q. Explain the Storage Infrastructure

1. There are two models storage network h moved away from end point computers to the network i.e.
   1. network attached storage
   2. Storage area network that consits of large ~~nu~~ harddisk drive arrays & clusters with controllers.
   - NAS can be accessed by most of the compu & other devices on the network whereas S is typically used by server to provide the storage services.
   These both storage system have many bui security capabilities to choose from.
3. Storage infrastructure can broadly divid in three primary categories:-
   1. Storage network
   2. Arrays
   3. Servers

1. Storage Network

Seperation of duties should be apply o the storage infrastructure.
So all storage devices are connected physicall either over the network or through a storag connection protocol, seperating access to the

physical servers to prevent a storage administrator from connecting a rougue server into the environment with the restricted access of LUN's is called as storage network



2. LUN

A LUN is the ~~network~~ number mechanism that is used by arrays & clusters to present its storage to a host operating system.

3. Storage Network is broadly divided into 2 types of zoning.

1. Port zoning

Port zoning is that the accessibility of the host to the LUN's that is defined by switch port.

2. WWN Zone (World Wide Web)

1. WWN zone are created relatively to the ports that are connected to the servers on the switch
2. It defines the individual zone based on the WWN id of the host bust adapter (HBA).

2. Arrays

It is a set of components, devices peripher... that are connected to the server through the switch port.

Every devices or components has its own LUN number.

3. Server

Server is the system that provide the storage services to the user's & this services is handled by the system administrator's.

RISK REMEDIATION

1. Confidentality Risk

Confidentality risk are associated with vulne-lities and threats pertaining to the privac... and control of information.

a) Data Leakage

Data Leakage is the risk of loss of informat... such as confidentional data and intellectu... property through intentional or unintentio... means.

There are 4 major thread vectors for data leakage.

1. Theft by outsiders
2. Malicious to sabotage by insiders
3. Inadvertant misuse by authorized users
4. Mistakes created by unclear policies.

b)

c)

b) Espionage

Espionage refers to the unauthorized interception of network traffic or messages for the purpose of gaining information intentionally.

Packet Sniffing / Spoofing

Using the different tools to capture the network packet is called as packet sniffing.

Packet Replay

Using the different tools to reproduce the traffic and the data was previously sent on the network is called as packet replay.

c) Inappropriate Administrator Access.

If the users are getting the privilages levels usually that reserve from the system administrator that provides full access to the system and all the data on the system has access too, then they will be able to view the data or make the changes without being properly restricted through the system authorization process.

Storage Persistence

Data remains in storage devices is stored for longtime but it is no longer we needed and even after it is deleted is called as storage persistence.

d) Misuse of data
People who have authorized access to d
can do this things with the data that
they are not suppose to ~~data~~ do.

e) Fraud
A person who illegally gain access to th
information that they are not authorized to
acuss ~~that~~ commits fraud.

f) Phishing
It is an attempt to trick a victim into
disclosing personal information.

g) Hijacking
It refers to the exploitation of a valid com
session - sometimes also called a session key
gain unauthorized acuss to information or beh
in a computer system.

2. Integrity Risk

a) Malfunctions
Different types of malware program is
to corrupt your data or information and
damage the data or the integrity.

b) Data deletion and data loss.
Data can be accidentally or intentionally
destroyed due to computer system failures or

mishandling.

c) Data Corruption and Data Tampering
Changes to data caused by malfunction in computer or storage systems, or by malicious individuals or malware, can damage the integrity of that data.

d) Accidental Modification
It occurs either when a user intentionally make changes to data but makes the changes to the wrong data or when user inputs data incorrectly.

3. Availability & Risks.
Associated with vulnerabilities & threats pertaining to pose a low risk & to have a low incidence of outage.

a) Denial of Service
A DOS attack or a distributed DOS attack is an attempt to make a computer resource unavailable to its intended users.

b) Outage
It is any unexpected down downtime or unreachability of a computer system or network.

c) Instability and Application Failure
Problems, such as bugs, in software or firmware

can cause freezing, locking or crashing of applications, making them unresponsive and resulting in loss of functionality or fail of an entire computer or network.

d) Slowness

When the response time of a computer or network is considered unacceptably slow, its availability is affected.

e) High Availability Failure

A device that is supposed to fail over in the event of a problem with one device to other, functioning devices may not actually fail over properly.

f) Backup Failure

When you discover that those backups you were relying on aren't actually any good, either because the media is damaged or the backup data is corrupted or missing data is lost.

IMP

Best Practices

1. Zoning
2. Arrays
3. Servers
4. Offsite Data Storage

Page No.
Date

Chp7 DATABASE SECURITY

Q. What is database & explain various capacities used where database can be used?.

General Database Security Concepts.

1. Application Support - Ranging from simple employee list to enterprise-level tracking software, relational databases are the most commonly used method for storing data.
2. Secure Storage of sensitive information
3. Online transaction processing (OTLP) services are functions of db in many organization.
4. Data Warehousing

IMP Database Security Layers.

1. Server-Level Security
   Buisness data security begins at server level
   A db appln is only secure as the server it is running on.
   First step to secure the server is to determine which users and applications should have access to it.

2. Network Level Security
   Four steps to protect your network:-
   1. Implement - 1st step is to create & implement

a network security system.

2. Analyze - Once created & implemented, the system needs to be analyzed to determine the current security system is appropriate. network it is protecting.

3. Test - After analyze step it is time to to to make sure all securities are working & will protect your n/w.

4. Modify - After tests, collect data & enha your protections.

3. Data Encryption.
Another method for ensuring the safety of db information. is to use encryption.

4. Operating System Security.
It is the process of ensuring OS integrity. confidentiality and availability.

MPS. Object-Level Security
Types of Object:-
1. SELECT - Retrieves information from db
2. INSERT - Adds a new row to table.
3. UPDATE - Changes the values in an existing
4. DELETE - Deletes rows from a table.
5. GRANT - Particular user will have a right perform a specific action.

Q. How database provide security in web application? OR How appln security works in db?

Page No. Date

6. REVOKE - Removes any current permissions settings for specified users.

7. DENY - Prevents a user or role from performing a specific action.

APPLICATION LAYER SECURITY

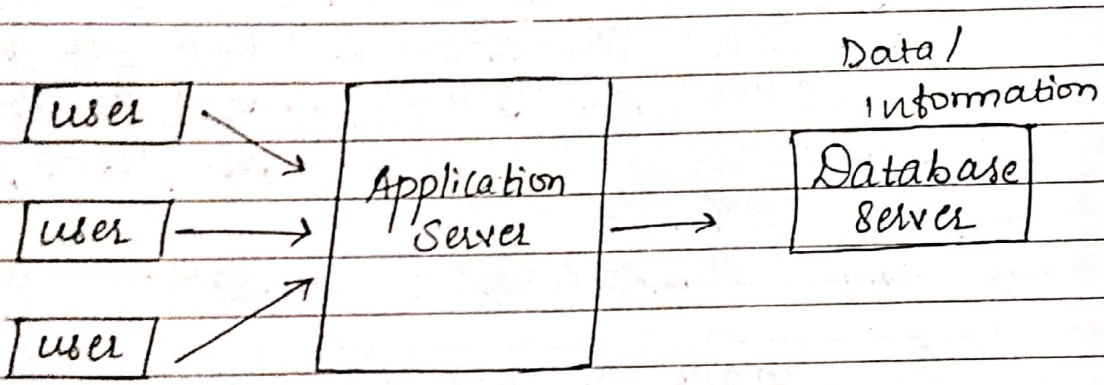
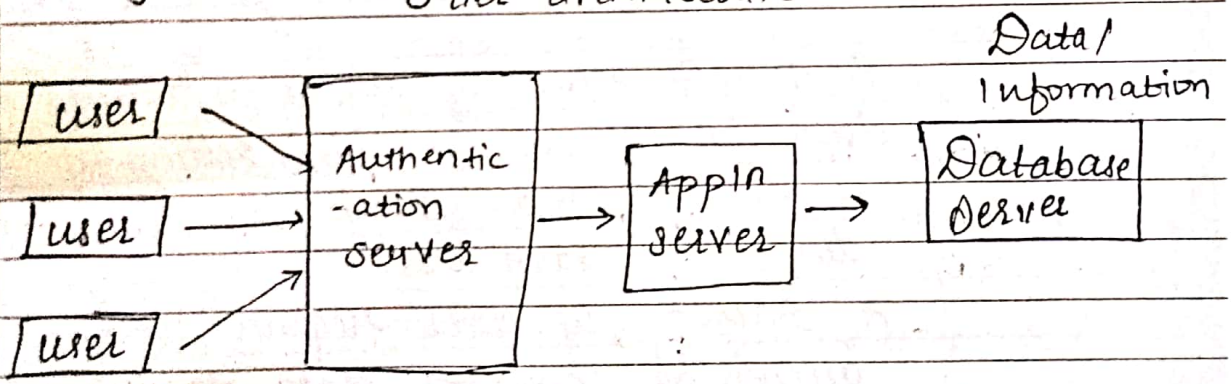


Fig:- Appln layer security for a database 3 tier architecture.



Four tier architecture

Many modern database system implement appln level security by using 3-tier architecture. In this architecture a single db account is used by an application. This user account provides the application with

access to all of you the databases, informati & operation that might be required by any user of the appln.

The appln server is responsible for enfo all user level security rules.

The figure provides a simplified example of how application security works in db.

Application security allows you to limit the number of database accounts & does by limiting the number of actual account tha have database acces.

Li it your exposure to external hacking att

Q. Explain different types of Backup.

Database Backup & Recovery

1. Backup & recovery refers to process of backu data in case of loss of setting up system permission that allow the data recovery due to the data loss.
2. Backing up data requires copying & archeiving computer data to that it is accusible in case of deletion or corruption of data.
3. There are 4 types of backups in db.
   1.
   2.
   3.
   4.

Page No.
Date

1. Full Backup
It is a basic & complete type of backup protection operation.
This type of backup makes a copy of all data to another set of media which can be disk or dvd.
Advantage :- 1. It will take full copy of the data is available with the single set of media.
2. This result in minimial type to restore data that metric is known as RTO (Recovery Time Objective)
Disadvantage :- 1. It requires more store space & more duplication of data in backup process.
Thus full backups are typically run only periodically

2. Incremental Backup
It copy only data that has change since the last backup operations of any time.
The modified timestamp file is typically used & compare to the timestamp of the last backup.
Advantage :- 1. It requires low resources & fewer resources.
2. It can be carried out only the change data as obtained as needed.
Disadvantage :- Lowest data recovery time.

3. Discremental Backup
It consits of copying all the data that has change since the last full backup.

The differential backup contains only changed data, the recovery process involved:-

1. Restoring latest full backup
2. Restoring latest differential backup.

Advantage:- 1. It provides a way of backing up changed data.

Disad - 1. It requires more time & space to comple

4. Transaction Log backups.

RDBMS are design to support multiple concurrent objects to the data.

Advantage - 1. Periodically the transaction that have been logged are then committed to the actual database.

Disadvantage - 1. To implementing transaction log backup in order to recovery database that the last full backup must be restore.

Q. Write a short note on auditing & monitoring db security.

Unit 3 Chp 8

Security Network Design

Computers and information networks are critical to the success of businesses when they are connect the people, support different application & services and provide access to resources that keep the businesses running properly.

To design the secure network to handling this multiple task, we required the following steps

1. Acceptable Risk
2. Designing Security into a Network.
3. Best Network design model
4. Designing an appropriate network.
5. Overall cost of the security.

Acceptable Risk

Risk acceptance is the process that is defined as the organization capability to accept the level of risk associated with the given activity or process.

Designing security into a network

To building different security feature over an existing network is expensive and difficult as it has dedicated zones that allows an organization to use small no of security devices such as firewall, IDS / IPS (Intrusion Detection System / Intrusion Prevention system) and multiple

application system to secure and monitor the network.

There are various factors for designing security in the network such as Budgets, Availability requirements, Network size & scope, future growth expectations, capacity requirements & management tolerance of risk impact on the network.

3. Network Design Model

In network security, you have the three types of network to consider

1. Inside
2. Outside
3. Optional

These all three is called as Demilitarized zone. It is the best network design model can be used in organization.

For eg:- Shopping mall, airports, etc.

4. Design an appropriate network

The overall network design must provide the ability and support future network requirements. The best way to design and maintain a network that supports the need of its user that involves into the network architect and engineers in the application development process.

5. The cost of security

The different security control mechanism has

expenses associated with their purchase, deployment, maintainance and implementing this secure systems in a redundant fashion can increase cost significantly.

Factors of Network.

INP

Q2] Explain the CHI Models for Network Design.

1. Performance.

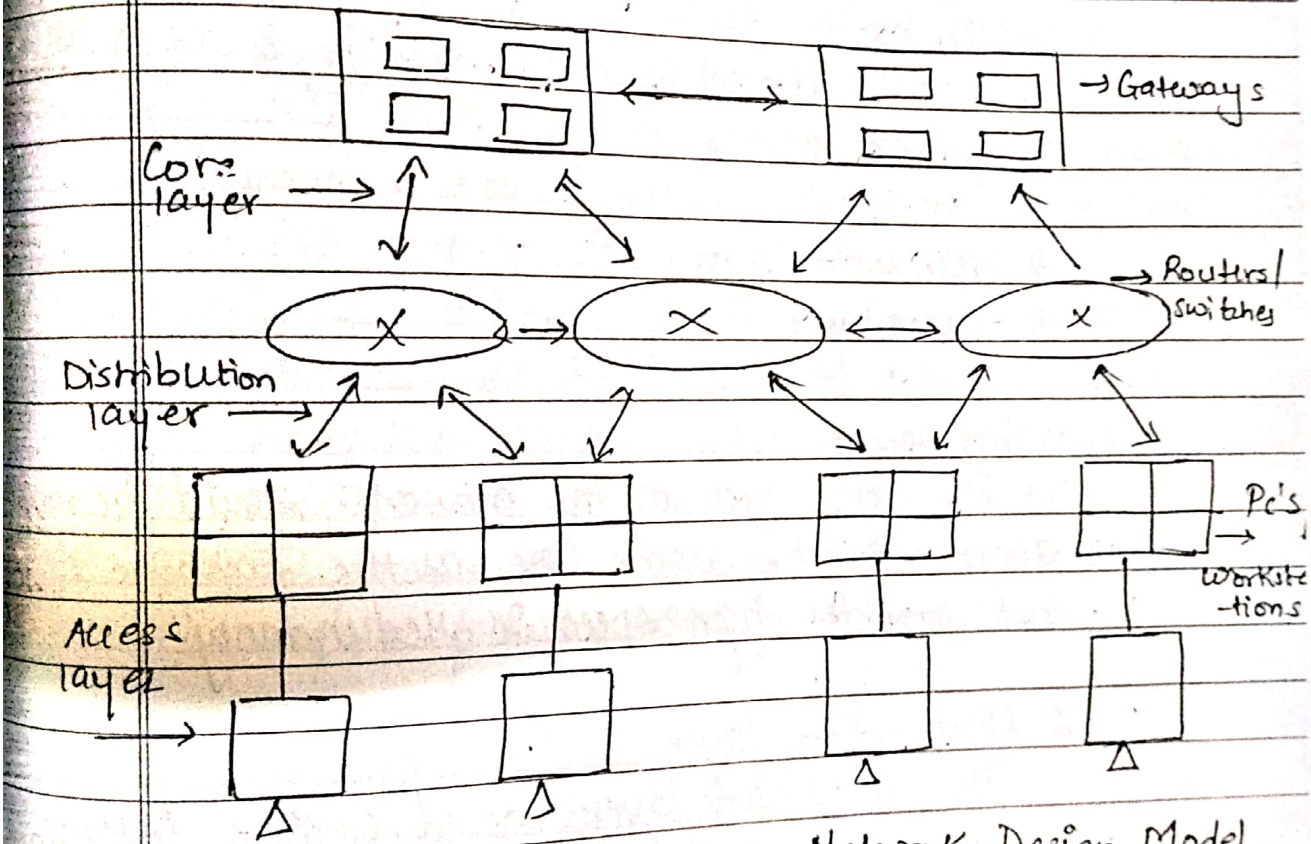


Fig: Cisco Heirarchical Network Design Model

1. The CHI Model is a common network design model to implement the large scale network or campus network.
2. This model support emerging technologies like:-

1. Class fabir
2. loss. less ethernet
3. layer to bridging & other data center-centric technology.
5. The cisco 3 mad model is derived from PSTN network (Public switch telephone network). which we will use for much of the worlds telephone infrastructure.
4. It is a blueprint of network which defines how network should be designed in different layers. each having its own their roles & responsibilities
5. The CHI model is made up of 3 main layer known as :-
1. Core layer
2. Distribution layer
3. Access layer

1. Core layer
The core layer of the network would be consi along with the same line as the backbone netw that provides high speed & redundancy.

2. Distribution layer
The distribution layer would contain intermedi router and switches such as those use to rout between the subnets or Vlan (Virtual LAN).

3. Access layer
The access layer is litral where user's pc workstations are plug plugged into the local sw

It is the simplified view of network. It provides a general high level overview.

2. Availability

3. Security

1. Each component on the network performs the different job & it contains data of different security requirements.
2. Some of the components contains highly sensitive information that could damage of an organization.
   If distributed to unauthorized users such as payroll record, customer list & event internal job costing documents.
3. When designing & implementing security in the network & the system architectures, it is helpful to identify critical security controls & consequences of failure in your control.
4. To provide the security in the network we require following security controls:-

1. Firewall

A firewall is a networking device (hardware as well as software) is used to protect host by limiting what services that the users can connect to on the given network.
The firewall can be use to prevent unauthorized users, non-administrative users & unauthorized application that running over the network.

The network designers can increase the security by segregating servers from each other by using firewall.

Firewall is a network perimeter (boundary) that consits of all the external-most points of the internal ~~do~~ network, each connection to the another network, whether to the internet or to any external third party, creates an entry point that must be secured for physical network.

2. VPN (Virtual Private Network)

VPN consits of group of the users that are integrated ~~from~~ & interconnected to access the internal services.

The VPN network is normally designed for intrnal users for security example :- dialup connection.

VPN's used to protect organization network for remote user access, security administrator ~~network for remote~~ should ensure that adequate protection that implemented over the network or end points.

VPN network connects remotely connected people to the organization network & it protects the data while it travels over an untrusted network.

3. Intranet, Internet (Extranet), DMZ

Intranet -

~~Itran~~ Intranet is a network made up of ~~for~~ internal users of the organization that include

in all workstations & server but not share with the outside world.
The Intranet is typically under the one administrative authority & operates under a common security plan.

Internet (Extranet)
It is a public network that can be used by the outsider to access the external resources from the internet.
When the internal users access the resources from the internet with the administrative authority then it is called as extranet.

DMZ
It is also called as screened subnets is made up of one or more isolated LAN network that contains shared server resources such as web, DNS & Email server.
The shared servers are connected to the network ~~that~~ in device is called as Bastion host.
A screened subnet is really an isolated network that is only available through firewall interface & it is not directly connected to the internal network.

Remote Access considerations

Q) Explain the OSI Model.

Page No.
Date

Unit 3 Chp 9

NETWORK DEVICE SECURITY

Routers & Switches Basics

Switch

1. Switch is a networking device is used to fi & forward the packets between the LAN segments and it operates at the datalink layer of the OSI model.
2. LAN's uses the switch to connect the different fragments are known as switch l or switch ethernet in the physical network.

Router

1. Router is the networking device that used to forward the packets along the network & it operates at the network layer of the OSI model
2. It is connected to atleast 2 LAN's or WAN at its highest peak network that are located at gateway.
3. Routers are used header & forwarding table should determine the best part of for the packet and they use different protocol to communicate with each others.
4. Parameters

Q.2]. Explain the parameters of switch & routers used the to forward packets.

1. Media Access Control (MAC)
1. It is the globally unique identity number that assign network devices (NIC cards) & therefore it is often refer to as physical address or hardware address.
2. They are 6 bytes in length.
The first 3 bytes are Id number of the manufacturer which is assigned by IETF (Internet Engineering Task Force) & the second 3 bytes are serial number assign by the manufacturer.

2. IP address
1. The MAC address supports implementation of hardware into the device where as software implementation is supported by IP address.
2. It consits of 4 bytes of information & is also called as logical address of the network & host.

3. ARP
1. ARP is a protocol ~~is used to~~ for address mapping into the network.
2. ARP protocol is used to mapping the logical address to physical address of the host.

4. TCP / IP protocol
1. TCP/IP is used for establishing the connection oriented service for a communicating through the network.
2. TCP is a connection oriented transport protocol

Q4. Explain the routing with its types.
Q.3. Difference between TCP & OSI Model

Page No.
Date

for transmitting unstructured stream of bytes.

IMP Comparison of TCP/IP Model & OSI Model

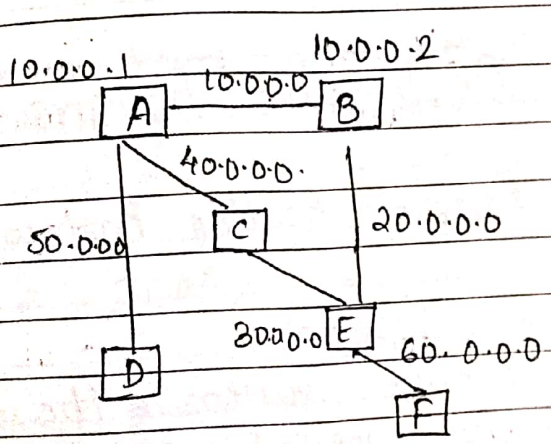
	Parameters	TCP/IP	OSI Model
1.	No of Layers	4 layers (network, internet, transport, Appln)	7-layers (physical, Data network, transp Session, presenta Appln).
2.	Developed by	DOD (Department of Defense)	ISO (Internati Standard Orga
3.	Tangible	Yes	No
4.	Usage	Widely Used	Not Used
5.	Meaning	Also called Client-Server model	Also called theoretical used for com -uting syste
6.	Purpose	used for data transmission	

Routing

Routing is the process that plays an impo roles to transmitting the routing table informa from router to router on the network.

When the router receive the data it determines the destination address by reading the header of the packet.
Once the address is determine it searches in its routing table to get to knowledge how to reach the destination & then forward the packet as per the routing.
There are 2 types of routing:-
1. Static
2. Dynamic

1. Static Routing



1. In static routing the routing table information is fed into the routing tables manually.
2. The network administrator manually configure the static routing on the routers by using IP route command.
Thus static routing is feasible for small environment with minimum of one or 2 routers.

Q.5]. Explain Heirarchy of Dynamic Routing Protocol with diagram.

Page No.
Date

2. Dynamic Routing

1. In the dynamic routing, the routing table information is fed into the routing table dynamically by using the different dynamic protocols i.e. rip, ospf, bgp.
2. The purpose of this protocols is to enable the other routers to transfer the routing information about to other routers, so that the other routers can build their own routing tables. Thus dynamically routing can be used their own for large environment with maximum of 2 or more routers.

IMP **HEIRARCHY OF DYNAMIC ROUTING PROTOCOL**

Dynamic Routing Protocol →

1. Autonomous System

An autonomous system is the collection of routes that are connected to each other in one particular area or boundary under a common administration such as company or an organization.

For. eg:- companies internal network, an ISP's network.

2. IGP -

Internal Gateway Protocol

IGP protocol is use for sharing the routing tab

information from router to router within an autonomous system.
It is also refer to as Intra-domain routing protocols.
2. IGP includeds RIP, IGRP, EIGRP, OSPF, IS-IS

Dynamic Routing Protocol

Interior Gateway Protocol

Exterior Gateway Protocol

Distance Vector Routing

Link State Routing

Path Vector Routing

RIP IGRP Open Shortest path first IS-IS BGP

Routing Info Protocol

Interior Gateway Routing Protocol

Intermediate System - Intermediate System

Border Gateway Protocol

RIPv2 Enhance IGRP

3. BGP
BGP is used for sharing routing table info -rmation router to router between the autonom -ous system.

It is also refer to as interdomain router.

4. Distance Vector Routing & Linkstate

It is used for sharing the routing table information from one router to another to calculate the best path. Reach to the destination.

The RIP & IGRP protocol supports distance vector routing where ospf & IS-IS supports linkstate routing.

5. Path - vector

It is used for sharing the routing table Information from one ~~router to another to calculate~~ border routers to another border routers between an autonomous system. BGP supports path vector routing.

IMP Network Hardening.

1. Patches.
2. Switches Security → port security functions
3. ACL.
4. Disabling unused services.
5. Network Discovery Protocol.
6. Proxy ARP.
7. AAA
8. SNMP → DHCP
   → WINS

Q Explain the different layers of Protections in the network?

→ Network Hardening defin - 1Mark
8 Factor - 4Mark

Page No.
Date

Network hardening is the process that helps in improving the security of network through deploying security solutions on making changes in the network configuration.
It includes the activities of applying firmware updates & managing configuration issues.
Network hardening is a set of layers of protections to the network :-

1. Patche:
Patches is the first step to help hardened the network & computing systems that is applying by vendors.
It add security hardening features to protect your devices on the one hand against a number of well-known problems & potential unknown vulnerabilities within the application.

2. Switches Security
The nodes in the networks are not directly aware about the switches which handles the network traffic effectively and make the switches silent workhouse workhorse of a network.
Port security functionality is used to provide the security on the switches and it is helpful when physical acess ores the network.

3. ACL
Access Control List can be configured to permit or deny TCP & UDP traffic that based on the

VSNP Q. Short note on ICNP / Explain ICMP with its unreachable message type?

Page No.
Date

Source & destination address or both.
ACL are used to protect the routers itself which permits the host on the network used by administrative staff that authorized to login to the network devices to connect to the network services on the routers such as Telnet, SSH, HTTP.

4. Disabling unused services.
The routers run different services that are not required for processing of the packets which can be disable by network administrator.

5. Networking Discovery Protocol
DHCP is a network discovery protocol to dynamically assign IP address & that used the cisco routers & switches to locate the neighbouring routers & switches.

6. Proxy ARP
Proxy ARP allows one host to respond to ARP request on behave of the host which is used by proxying traffic for protecting host.

7. AAA
It is a centralizing account management software that is used in large environment. The local account management can be simplify by configuring network devices & system to

8.

Authenticate against control account repositories with the Help of AAA.

SNMP

It is a management software which is used to monitor any network device which is install through SNMP agent software.

SNMP is used in local area network to monitor network nodes such as servers, workstations, routers, bridges, printers & hubs as well as services such as DHCP & WINS (Windows Internet name services)

ICMP (Internet Control Message Protocol)

Unreable Message Types

0 - Network unreachable
1 - Host unreachable
2 - Protocol unreachable
3 - Port unreachable

ICMP gives the notifiation about the send messages to the users.

It provides mechanism for reporting

TCP IP communicates problem & utilities for testing IT layer connectivity.

It consists of two type of messages.

1. Query Message ⇒ successfull
2. Error Message ⇒ unsuccessfull.

Code No	Description
0	Network unreachable
1	Host unreachable
2.	Protocol unreachable
3	Port unreachable
4	Data gram is too big
5	Source Routes failed error
6	Destination Network unknown
7	Destination Host unknown error
8	Source Host Isolated error
9	The destination network is administratively prohibited.
10	Destination Host is administratively prohibited.
11	Network is unreachable for TOS [Types of service].
12	Host is unreachable for TOS
13	Communication administratively prohibited.
14	Host Precedence violation.
15	Precedence cutoff in the effect

NAT: Network Address Translation

Q1. Explain Evolution of firewall / 2 same Page No.
Q2. Explain types of firewall Answer Date

Chp 3 FIREWALLS

1. Types →
   Packet filtering, Stateful Inspection.
   #ppln Level, Circuit Level.

2. Functions →
   NAT
   Auditing & logging

3. Benefits

EVOLUTION OF FIREWALL

Firewall categories based on generations of the firewall :-

1st Generation - Packet filtering

1. It was developed in 1980's.
2. It is used to examine source & destination IP addresses, source & destination port numbers & protocols (Interfaces).
3. It monitors the network addresses & port numbers of inbound & outbound network traffic & filters them as per some pre determined rules.
4. It works on 3 layers of OSI Model.
   1. Physical layer
   2. Network layer
   3. Transport layer.

Pa
Date

2nd Generation - Stateful Inspection fi
1. It was developed in early 1990's.
2. It is used to determine whether the pack
a part of existing connection or not &
the traffic and forwards that packet.
3. It operates upto 4 layers of OSI model
works with TCP stream i.e. byte to byte.

3rd Generation - Application Level Firewall.
1. It is also known as Proxy server can m
& filter the packets on any OSI layer.
2. It has ability to block specific content & a
recognize certain application & protocols like
HTTP, FTP are being misuse.

4th Generation - Circuit Level Firewall
Next Generation Firewall
1. It is recently deployed, integrated net
platform that consits of deep packet
inspection, application inspection & SSL-SS
inspection and other security system fun
-alities.
2. It can examine the data network packet
for protocol non-compliance, visuses and
enforce security from these modern threats

Q.3. Explain the working of NAT in the public
network.

Q.4. Explain the core functions of firewall.

Q. Explain

CORE FUNCTIONS OF FIREWALL

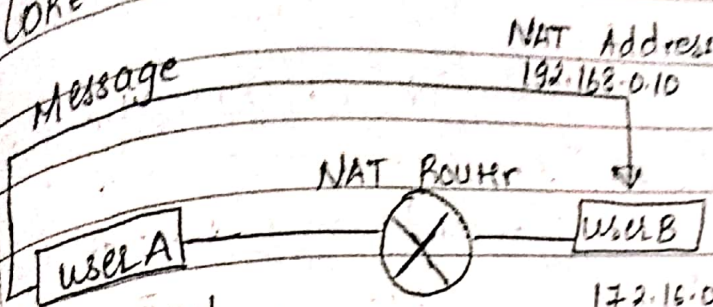


Fig:- NAT

NAT

Types of NAT

1. Static
   1. It is a one to one mapping of a private IP address to a public IP address.
   2. It is useful when the network device (router) inside the private network a ~~SSH~~ VPN to be accessible from internet.

2. Dynamic NAT
   1. It is a one to many mapping of a private IP address to a multiple ~~IP Address~~ public IP addresses.
   2. It is useful when public IP address is taken from pool of IP addresses that configured on

end of the NAT browser.

3. Dynamic NAT establish one to many mapping of IP addresses or a group of public IP addresses is called as NAT pool.

3. PAT (Port Address Translation)

1. It is a many to one mapping of many private IP addresses can be translated to single public IP address.
2. Port numbers are used to ~~distrib~~ distinguish the traffic and its is cost effective as thousand of users can be connected to the internet.

Benefits / Advantages of NAT

1. Security
   Keeping the internet private IP addresses hidden
2. Flexibility
   internal IP addressing scheme or private IP addresses can be changed without affecting the public IP addresses that available external.
3. IP routing solution
   Overlapping of IP addresses are not a problem when NAT is used.
4. Translating between IPv4 & IPv6.
   NAT is used to translate IP addresses between IPv6 network to an IPv4 network.

Q5. Explain the benefits of the firewall → Sheth qsb.

Page No.
Date

2. Auditing & Logging

1. In the process of filtering internet traffic, all firewalls have some types of features of logging that documents how the firewall handle various types of traffic with private IP addresses & public IP addresses.
2. This logs can be provide & maintain valuable information like source & destination IP address, source & destinate Port numbers & protocols.

Benefits

Q. Explain the spread spectrum

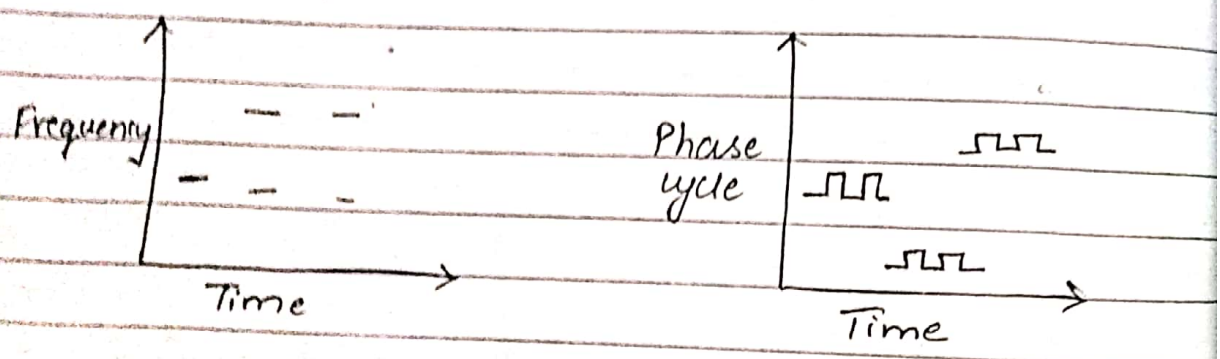
Page No.
Date

Unit 3

WIRELESS NETWORK SECURITY

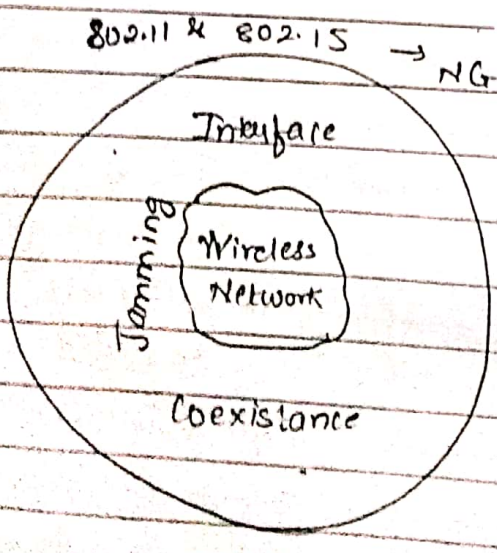
RF Signal
↳ Proper network design
↳ Compliance with FCC Regulation
↳ Principle of least access
↳ Largest Security
↳ Distinguishing security solutions from malfunctions.

Spread Spectrum.



FHSS

DSSS



The basic concept of spread spectrum communication are neccessary for understanding concept of

1. Interferences
2. Jamming.
3. Coexistence of devices on wireless network.

Spread spectrum refers to the ~~wide~~ wide frequency band, low power transmission as oppose to narrow band transmission.

There are two IEEE standards define the wireless network

1. 802.11
2. 802.15 that employ spread spectrum band technology.

There are two ways to implement spread spect-rum communication.

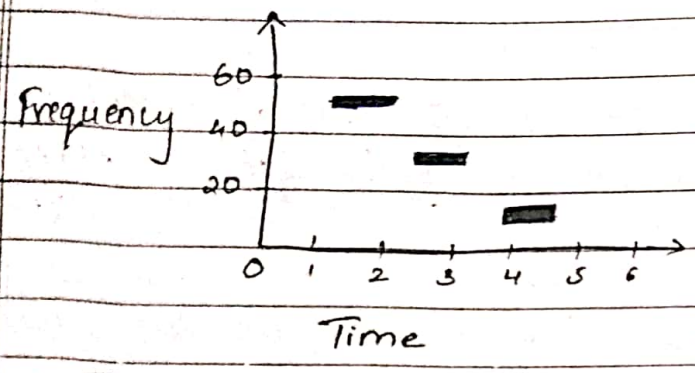
1. FHSS → Frequency hopping Spread Spectrum
2. DSSS → Direct sequence Spread Spectrum

1. FHSS

1. It ~~operates~~ define in 2.4GHz band and operates in around 79 frequencies that ranging from 2.402 to 2.480 GHz.
2. It is the method of transmitting radio signals by shifting carriers across numerous channels with pseudo random order which is already known by sender and receiver.
3. FHSS is a robust technology with only very little influence from reflection, noise and other environmental factors.

9. Explain the IDS & IPS -> 5 marks

Page No.
Date



4. In FHSS a pseudorandom sequency of frequency hops is followed by all host that participate in the wireless network as shown in the figure.

5. The carrier remains are same at a given frequency for a ~~dwell~~ dwell timed period and then hops to another frequency sequence is repeated. When the list of frequencies to the hop through is exhausted.

LMP

Q.1. Explain the IDs & IPs - 5marks
Q.2. Explain different types of threa on IDS

Page No.
Date

Unity

Neural Networks are intended to simulate the behaviour of

IDS & IPS

An intruder detection system is used to another monitor the network traffic that flowing across the different network and assess every packets against known issues & attack & it creates the alert based on those results.
It is a network security technology originally design for or build for detecting vulnerabilities that exploits against the web application, computers, networking devices & needs only to detect threats.
The key functionality of IDS are
1. Recording information related to the events.
2. Producing reports
3. Notifying administator of important observe events.

An IDS & IPS supports defense in depth security principle & can be used to detect & prevent wide range of rogue events such as impersonation attempts, password cracking Attacks, protocols attacks & buffer overflow.
There are 6 different types of IDS system :-
1. Host based

2. Network Based
3. Anamoly Based
4. Signature Based
5. Policy Based
6. HoneyPot Server

IPS

IPS is the system of both detecting intrusion activities of threats & managing responsive action on those detected intrusion activities throughout the network.

It is a network security prevention technology which examines & filter network traffic to detect & prevent different weakness exploits on the network.

Types of Threats

1. Attacks or Misuse of data
2. Application Attack
3. Data Normalization
4. Fragmentation & Reassembly attack
5. Flag exploits.

Q3. SIEM - Security Information Event Management

Q: What is VOIP? Componets of enterprise IP network?
List of Protocols of enterprise IP

Page No.
Date

Unit 4
Chp 2

VOIP

It is a set of controls that allows you to perform voice communication, data communication, instant messaging over the IP telephony network instead of dedicated switch network.
VOIP is used to provide the different services like voice call service, videocall service, messaging service by using voice channels & trunk circuits over the ISDN network.

Common Components of enterprise IP network.

1. Call Control Element (Call Agent)
It is also called as call agent
It includes appliance, IPPBX, soft, switches, proxy, session border controller, server based call controls.

2. Gateways
It has a dialt peer (server is responsible to provide the services.
It includes MCUs (Multi Conference Unit) is responsible for individual & dedicated service.

POTS - Plane Old Telephone Service
PSTN - Public Switch Telephone Network
ISDN - Integrated

Page No.
Date

3. Hardware endpoints
It includes ~~dns~~ smartphones, PDAs (Personal Digital Assistance) and other devices.

4. Software endpoints
It includes IP telephone software unified messaging integrated chat & videoclients, desktop based video clients & IP based smartphones client.

5. Contact Center Component
It includes interactive voice response system call recording system & call center workflow solution.

PROTOCOLS

1. COPS - Common Open Policy Service Protocol
2. H.248 → Megaco H → Hardware
3. MGCP - Multimedia Gateway Component Protocol
4. SIP - Session Initiation Protocol
5. DS - Differentiated services
6. RTP - Real Time Protocol
7. RTSP - Real Timie Streaming Protocol
8. SRTP - Secure Real Time Transport Protocol
9. IAX - Inter Ansterisk Exchange.
10. XMPP - Extensible Messaging & presence protocol
11. T-38 & T-125
12. ISDN -
13. SMS - Short Messaging Service
14. SS7 - Signal System No 7.

Page No.
Date

Q.2. Explain the components of VOIP

1. IPPBX / Call processing Server
(Internet Protocol Private Branch Exchange)

2. Gateways VOIP

3. User End Points

4. IP Network.

Q.3. Write a short note on PBX & PLC TEM.
(Telecom ~~Exchange~~ Expense Manager)