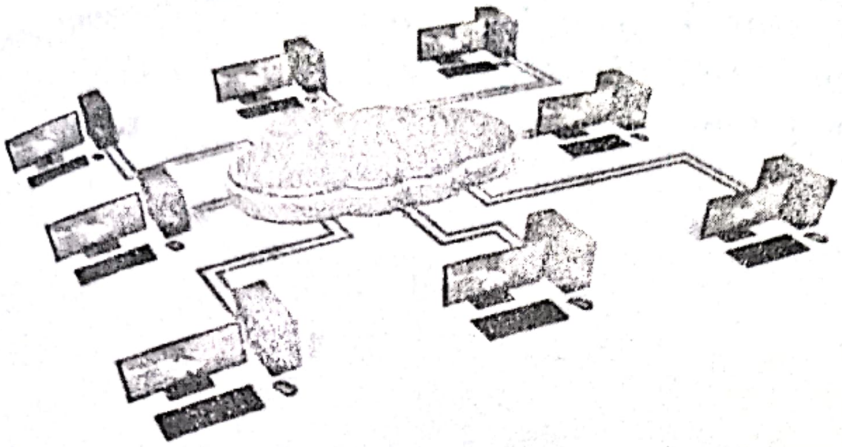


9

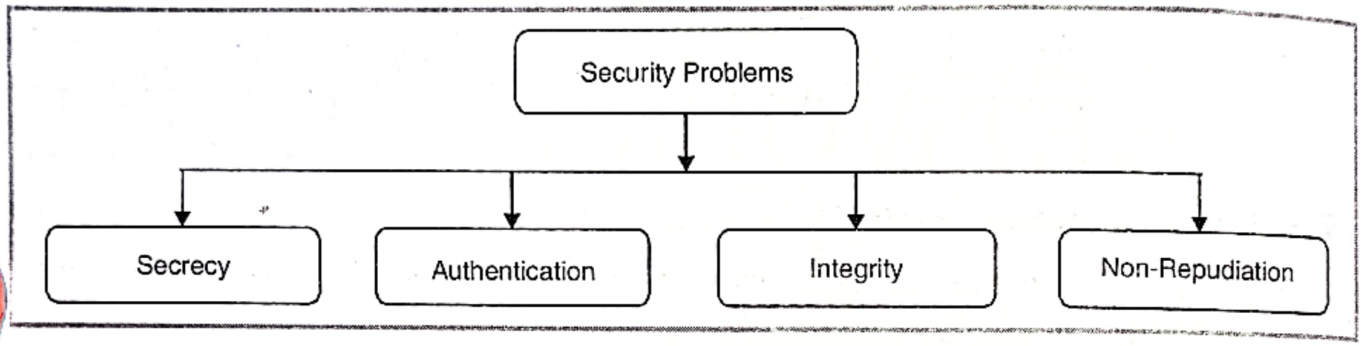
NETWORK SECURITY

Introduction

- When we talk about "security" we know what want, but describing it and making it happen can be different matters altogether.
- Network security has a natural conflict with network connectivity.
- The more an autonomous system opens itself up, the more risk it takes on.
- This, in turn, requires that more effort be applied to security enforcement tasks.
- Network security is a complicated subject, historically only tackled by well-trained and experienced experts. However, as more people become "wired", an increasing number of people need to understand the basics of security in a networked world.
- In simple words security means to protect data or meaningful information from unauthorized users or malicious user which can harm you data.
- Network security takes care that people can not read or edit the data of some other user without their permission.
- Most security related problems are caused by various types of users just to take the benefit in one or in another form, to harm someone or to threat someone etc.
- The problem associated with network security and their producers are like

"A student just for fun, Hacker to steal meaningful information. A spy to take an information about enemy's secrets etc. Network security is not a simple task rather it is a big game which require smartness, intelligence and lot of experience."

- So network security must be required in every case to avoid any type of problem.
- Network security problems are normally divided into four closely areas like Secrecy, Integrity control, Authentication and non-repudiation as shown below :



- Secrecy is associated with confidentiality. It has to do with keeping information out of the hands of unauthorized users.
- Authentication deals with checking whether a true user is working on data or not.
- Not repudiation deals with the signature for verification.
- Integrity control is associated with transferring correct and original data safely from one location to another.

9.1 TYPES OF NETWORK SECURITY

- There are two kinds of network security.
- One kind is enforced as a background process not visible to user; the other is in your face. These are as follows :
  1. **Traffic-based security** Controls connections requested by a network application, such as a web browser or an FTP download.
  2. **User-based security** Controls admission of individuals to systems in order to start applications once inside, usually by user and password.
- One kind of traffic-based security is the use of firewalls to protect autonomous systems by screening traffic from authorized hosts.

- The other kind of traffic-based security is router access lists, used to restrict traffic and resources within an autonomous system.
- User-based security is concerned with people, not hosts.
- This is the kind of security with which we're all familiar – login-based security that asks you for a username and password.
- The two types complement one another yet operate at different levels.
- Traffic-based security goes into action when you click a button in a web browser, enter a command into an FTP screen, or use some other application command.
- User-based security, on the other hand, assets itself when an individual tries to log into a network, device, or service offered on a device.

9.1.1 Traffic-Based Security :

- The Traffic-based in normally implemented by using restricted mechanism such as firewalls or router access lists.
- This style of security focuses mainly on source and destination IP addresses, application port numbers, and other packet-level information that can be used to restrict and control network connections.
- Until recently, firewalls have focused strictly on guarding against intruders from outside the autonomous system.
- They are now coming into use in more sophisticated shops to restrict access to sensitive assets from the inside.
- Access lists have been the traditional tool used to enforce intramural security.

9.1.1.1 Access List Traffic-Based Security :

- Routers can be configured to enforce security in much the same way firewalls do.
- All routers have access lists, and they can be used to control what traffic may come and go through the router's network interfaces and what applications may be used if admitted.
- What exactly an access list does is left to how it's configured by the network administrator.
- A view of a packet from the source to destination location is as shown in the figure 9.1 below :

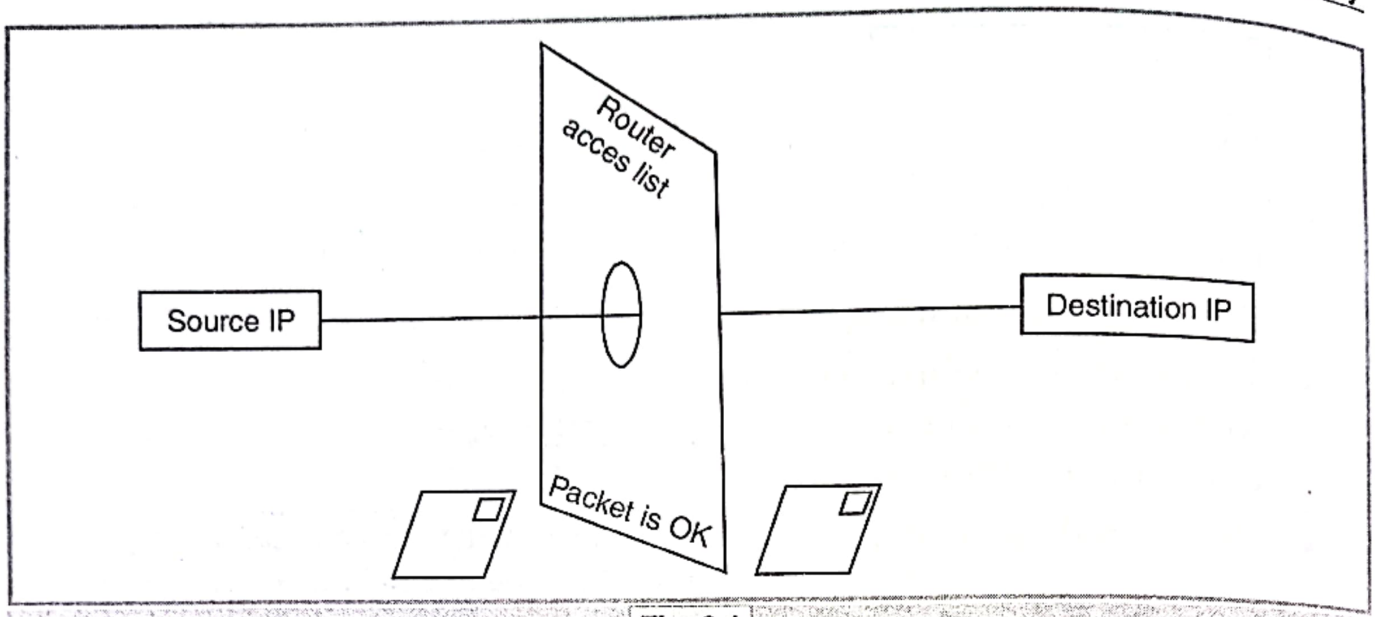


Fig. 9.1

- Mostly, access lists are used to improve network performance by isolating traffic in its home area, but a heavily configured access list can pretty much behave like an internal firewall, restricting traffic among departments.

9.1.1.2 Firewall Traffic-Based Security :

- Firewalls are basically beefed-up routers that screen processes according to strict traffic management rules.
- They use all sorts of tactics to enhance security : address translation to hide internal network topology from outsiders; application layer inspection to make sure only permitted services are being run; even high/low counters that watch for any precipitous spikes in certain types of packets to ward off Denial-of-Service attacks such as SYNflood and FINwait.
- Firewalls intentionally create a bottleneck at the autonomous system's perimeter.
- As traffic passes through, the firewall inspects packets as they come and go through the networks attached to its interfaces.
- A view of a packet from the source to destination location is as shown in the figure 9.2 below :
- Firewalls read source and destination host addresses and port numbers (for example, port numbers (for example, port 80 for HTTP), and establish a context for each permitted connection.
- The context comes in the form of a session, where packets with a certain address pair and port number must belong to a valid session.

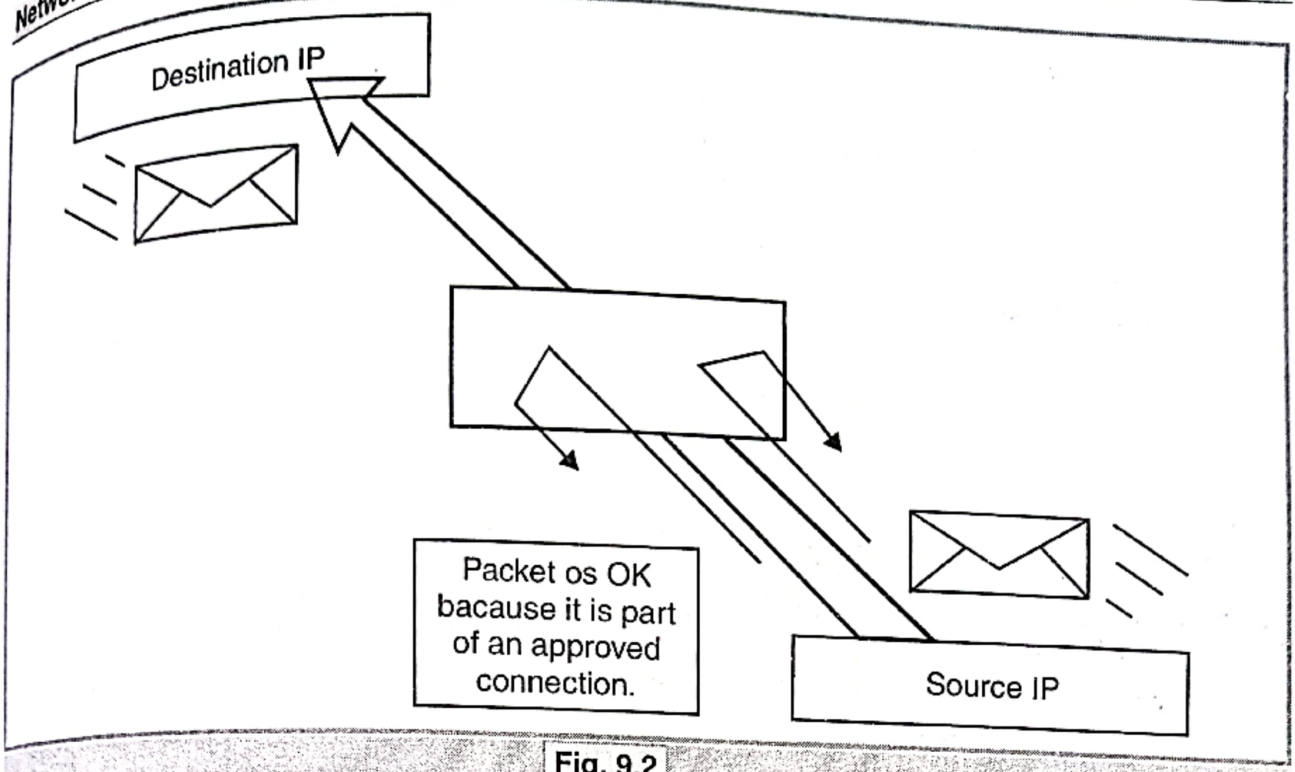


Fig. 9.2

- For example, if a user tries to connect to a web server to download a file, the firewall will check the user's source IP address and the application service requested before permitting the packets to pass.

9.1.2 User-Based Security :

- User-based security brings to mind a different picture having a gate with sober security guard standing and the post.
- The guard will ask you question regarding you identity and challenge you to prove your identity.
- If you qualify, you get to go in.
- More sophisticated user-based security systems also have the guard ask what you intend to do one inside and issue you a coded visitor's bage giving you access to some areas, but no other.
- Thus, user-based security is implemented where a person must log into a host, and the security comes in the form of a challenge for your username and password.
- In internetworking, this kind of security is restrict unauthorized user from entering network devices such as routers or switches, as it is to restrict access to payload devices, such as servers.
- Unlike firewalls, however, user-based security is nearly as concerned with insiders as outsiders.

- That security guard at the gate has colleagues on the inside, there to make sure nobody goes into the wrong area.
- You know the routine—there are employee badges and there are visitor badges, but the employee badges let you go more places.
- A view of a packet from the source to destination location is as shown in the figure 9.3 below :

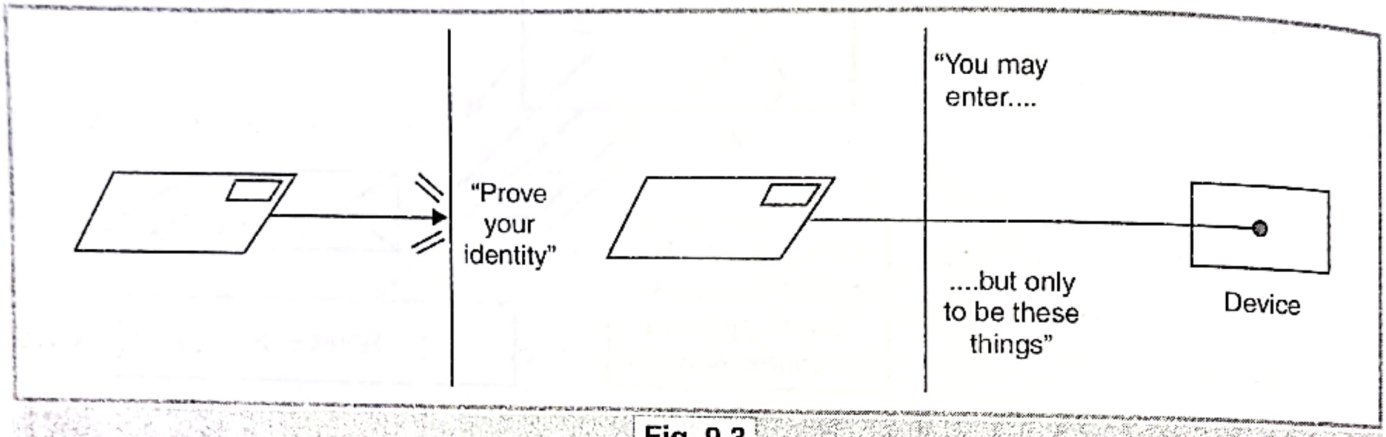


Fig. 9.3

- Login/password points are generally placed on every network device and all servers. Because user-based security mechanisms are software, not hardware, they can be deployed at will within an internetwork with little impact on performance or budget.
- The trade-off is how much inconvenience you're willing to put network users through, having to log in to gain access to various services. User-based security has four major applications :
  - To grant remote employees access to the enterprise network.
  - To grant onsite employees access to protected hosts and services within the internetwork.
  - To let network administrators log into network devices.
  - To let ISPs grant subscribers access to their portals.

Because most user-based security involves remote dial-in connec-tions, WAN technologies play an important role.

9.2 TYPES AND SOURCES OF NETWORK THREATS

Differact protect yourself against various threats.

Types of Threat

(i) Data Destruction :

- Some of those are responsible for attacks are simply twisted jerks who like to delete things.

- It can drastically effect your data and hence your business like any catastrophic event such as fire, flood, earthquake etc.

(ii) Data Editing :

- Another threat on network regarding data security is data editing.
- With data editing somebody can change your data and making data useless.
- Data editing is likely the worst sort, since the fact of a break-in might not be immediately obvious.
- Perhaps he's toying with the numbers in your spreadsheets, or changing the dates in your projections and plants.
- May be he is changing the account numbers for the auto-deposit of certain paychecks.
- In any case, rare is the case when you'll come in to work one day, and simply know that something is wrong.
- An accounting procedure might turn up a discrepancy in the books three or four months after the fact.
- Trying to track the problem down will certainly be difficult, and once that problem is discovered, how can any of your numbers from that time period be trusted ? How far back do you have to go before you think that your data is safe ?

(iii) Unauthorized Access :

- Unauthorized access means accessing the data which does not come in your range.
- It is a very high-level term that can refer to a number of difference types of attacks.
- The goal of these attacks is to access some resource that your machine should not provide the attacker.
- For example, a host might be a web server, and should provide anyone with requested web pages. However, that host should not provide command shell access without being sure that the person making such a request is someone who should get it, such as a local administrator.

(iv) Digital signature :

- This type of problem is normally associated in E-commerce or in E-Business *i.e.* you are not sure about the person who is selling or purchasing an item online.

- He or she can make use of your digital signature which selling or purchasing on web.

(v) Denial-of-Service :

- Another horrible attack on network security is DoS (Denial-of-Service) attacks, these are normally the most difficult to address.
- These are the most horrible, because they're very easy to launch, difficult (sometimes impossible) to track, and it isn't easy to refuse the requests of the attacker.
- The theory of a DoS attack is simple that is it sends more requests to the machine than it can handle.
- There are various tool kits available in the underground community that make this a simple matter of running a program and telling it which host to blast you're you requests.
- The attacker's program simply makes a connection on some service port, perhaps fake the packet's header information that says where the packet came from, and then dropping the connection.
- If the host is able to answer 20 requests per second, and the attacker is sending 50 per second, obviously the host will be unable to service all of the attacker's requests.
- Such attacks have created a problem in late 1996 and early 1997, but are now becoming less popular.
- Some things that can be done to reduce the risk of being stung by a denial of service attack include
  - Keeping up-to-date on security-related patches for your hosts' operating systems.
  - Not running your visible-to-the-world servers at a level too close to capacity.
  - Using packet filtering to prevent obviously forged packets from entering into your network address space.

(vi) Executing Commands Illegally :

- It's obviously undesirable for an unknown and untrusted person to be able to execute commands on your server machines.
- There are two main classifications of the severity of this problem : normal user access, and administrator access.
- A normal user can do a number of things on a system (such as read files, mail them to other people, etc.) that an attacker should not be able to do.

- This might, then, be all the access that an attacker needs.
- On the other hand, an attacker might wish to be make configuration changes to a host (perhaps changing its IP address, putting, a start-up script in place to cause the machine to shut down every time it's started, or something similar). In this case, the attacker will need to gain administrator privileges on the host.

9.3 PROTECTION OF THREAT

(i) Where Do They Come From :

- It should be noted that all of these attack come from normally one source that is most common example of Wide Area Networking *i.e.* an internet.
- It is an internet that provides assistance to an attacker gain access to your equipment.
- From looking at the sorts of attacks that are common, we can divide a relatively short list of high-level practices that can help to prevent security disasters, and to help control the damage in the some unwanted events.

(ii) Backups :

- Backup is made of two words back and up that means an additional support in case of risk.
- But this isn't just a good idea from a security point of view.
- Operational requirements should dictate the backup policy, and this should be closely coordinated with a disaster recovery plan, such that if an airplane crashes into your building one night, you'll be able to carry on your business from another location.

(iii) Do not put data at insecure place :

- Although this *should* go without saying, this doesn't occur to lots of persons.
- As a result, information that doesn't need to be accessible from the outside world sometimes is, and this can needlessly increase the severity of a break-in dramatically.

(iv) Avoid systems with single points of failure :

- Any security system that can be broken by breaking any one component isn't really very strong. In security, a degree of redundancy is good, and can help you protect your organization from a minor security breach becoming a catastrophe.

(v) Stay current with relevant operating system patches :

- Be sure that someone who knows what you've got is watching the vendor's security advisories.
- Exploiting old bugs is still one of the most common and most effective means of breaking into systems.

(vi) Watch for relevant security advisories :

- In addition to watching what the vendors are saying, keep a close watch on groups like CERT and CIAC Make sure that at least one person (preferably more) is subscribed to these mailing lists.

(vii) Have someone on staff be familiar with practices :

- There should be some person in your organization that is well versed in network security techniques that is you should have at least one person who is charged with current or latest security tips and tricks.
- This need not be a technical wizard, but could be someone who is simply able to read advisories issued by various incident response teams, and keep track of various problems that arise.
- Such a person would then be a wise one to consult with on security related issues, he'll be the ne who knows if web server software version such-and-such has any known problems, etc.

9.4 DEVELOPING YOUR SECURITY DESIGN

The design of the perimeter network and security policies requires the following subjects to be addressed.

1. Know Your Enemy :

- Knowing your enemy means knowing attackers or intruders.
- Consider who might want to circumvent your security measures, and identify their motivations.
- Determine what they might want to do and the damage that they could cause to your network.

Security measures can never make it impossible for a user to perform unauthorized tasks with a computer system : they can only make it harder. The goal is to make sure that the network security controls are beyond the attacker's ability or motivation.

2. Count the Cost :

- Security measures usually reduce convenience, especially for sophisticated users. Security can delay work and can create expensive administrative and educational overhead.

- Security can use significant computing resources and require dedicated hardware. When you design your security measures, understand their costs and weigh those costs against the potential benefits.
- To do that, you must understand the costs of the measures themselves and the costs and likelihood of security breaches.
- If you incur security costs out of proportion to the actual dangers, you have done yourself a disservice.

3. Identify Any Assumptions :

- Every security system has underlying assumptions. For example, you might assume that your network is not tapped, that attackers know less than you do, that they are using standard software, or that a locked room is safe.
- Be sure to examine and justify your assumptions. Any hidden assumption is a potential security hole.

4. Control Your Secrets :

- Most security is based on secrets. Passwords and encryption keys, for example, are secrets.
- Too often, though, the secrets are not all that secret.
- The most important part of keeping secrets is in knowing the areas that you need to protect. What knowledge would enable someone to know your system ? You should jealously guard that knowledge and assume that everything else is known to your adversaries.
- The more secrets your have, the harder it will be to keep them all.
- Security systems should be designed so that only a limited number of secrets need to be keep.

5. Human Factors :

- Many security procedures fail because their designers do not consider how users will react to them.
- For example, because they can be difficult to remember, automatically generated nonsense passwords often are written on the undersided of keyboards.
- For convenience, a secure door that leads to the system' only tape drive is sometimes propped open.
- For expendiency, unauthorized modems are often connected to a network to avoid dial-insecurity measures.

- If your security measures interfere with essential use of the system, those measures will be resisted and perhaps circumvented.
- To get compliance, you must make sure that users can get their work done, and you must sell your security measures to users.
- Users must understand and accept the need for security.
- Any user can compromise system security, at least to some degree.
- For instance, passwords can often be found simply by calling legitimate users on the telephone, claiming to be a system administrator and asking for them.
- If your users understand security issues, and if they understand the reasons for your security measures, they are far less likely to make an intruder's life easier.
- At a minimum, users should be taught never to release passwords or other secrets over unsecured telephone lines (especially cellular telephones) or e-mail.
- User should be wary of people who call them on the telephone and ask questions.
- Some companies have implemented formalized network security training so that employees are not allowed acess to the Internet until they have completed a formal training program.

6. Know Your Weakness :

- Every security system has vulnerabilities. You should understand your system weak points and know how they could be exploited.
- You should also know the areas that present the greatest danger and should prevent access to them immediately.
- Understand the weak point is the first step toward turning them into secure areas.

7. Limit the Scope of Access :

- You should create appropriate barriers in your system so that if intruders access one part of the system, they do not automatically have access to the rest of the system.
- The security of a system is only as good as the weakest security level of any single host in the system.

8. Understand Your Environment :

- Understanding how your system normally functions, knowing what is

expected and what is unexpected, and being familiar with how devices are usually used with help you detect security problems.

- Noticing unusual events can help you catch intruders before they can damge the system. Auditing tools can help you detect those unusual events.

9. Limit Your Trust :

- You should know exactly which software you rely on, and your security system should not have to rely on the assumption that all software has unusual events.

10. Remember Physical Security : Physical access to a computer (or a router) usually gives a sufficiently sophisticated user total control over that computer.

- Physical access to a network link usually allows a person to tap that link, jam it, or inject traffic into it.
- It makes no sense to install complicated software security measures when access to the hardware is not controlled.

11. Make Security Pervasive :

- Almost any change that you make in your system may have security effects.
- This is especially true when new service are created.
- Administrators, programmers, and users should considers the security implications of every change they make. Understanding the security implications of a change take practice; it requires lateral thinking and a willingness to explore every way that a service could potentially be manipulated.

9.5 CRYPTOGRAPHY

- Cryptography, word with Greek origins, means "secret writing". However. We use the term refer to the science and art of transforming messages to make them secure and immune to attack.
- Network security is mostly achieved through the use of cryptography : a science based on the abstract algebra.

Definition

Cryptography means **"Writing secret code or Text"**. It refers to science and art of transforming the message to certain code and then retransform it to the original message.

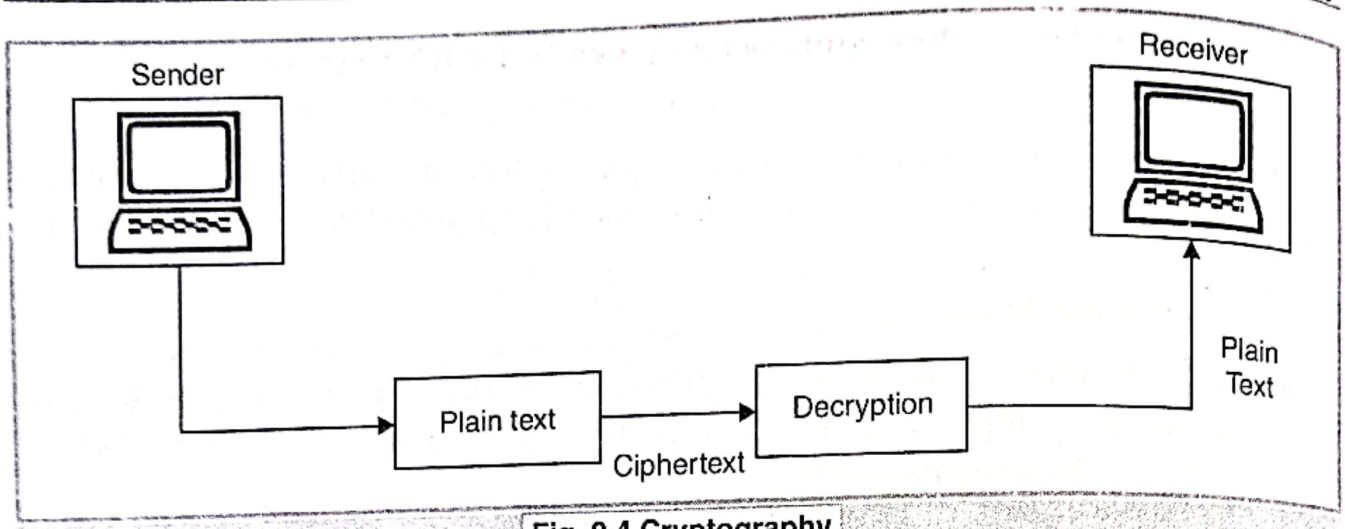


Fig. 9.4 Cryptography

9.5.1 Basic Terminology used in Cryptography

(i) Plain Text. The original message, being transformed is called plain text.

(ii) Cipher Text. The message is transformed into certain code is cipher text.

(iii) Encryption Algorithm. An encryption algorithm transform the plain text into cipher text.

(iv) Decryption Algorithm. It transform the cipher text back into the plain text. The sender uses an encryption algorithm but the receiver uses a decryption algorithm.

(v) Cipher. Encryption and decryption refer to cipher. The term cipher is also used to refer to different categories of algorithm in cryptography.

(vi) Key. A key is number (or set of number) that the cipher, an on algorithm operates on. To encrypt a message, we need an encryption algorithm, an encryption algorithm, and the plain text. These create a cipher text. To decrypt a message we need a decryption algorithm.

(vii) Alice, Bob and Eve. In cryptography, we use three character:

Alice : Alice is person who need to send secure data.

Bob : Bob is the recipient data.

Eve : is the person who want to disturb the communication between Alice and Bob.

9.5.2 Substitution Cipher

- A substitution cipher substitute one symbol with other. If the symbol in the plain text are alphabetic character we replace one character with another.

A substitution cipher replaces one symbol with another.

Example : We can replace S with A and K with B.

If symbols are digits (0 to 9) we can replace 3 with 7; and 2 with 6. Substitution cipher can be categorised into two part.

1. **Mono alphabetic Cipher :**

- A character (or a symbol) in the plain text is always changed to the same characters (or symbol) in the cipher text regardless of its position in the text. When one latter are group fillet is replace by another later called.

Example : If S is replace with A character. Then every character in the word is replaced. This relationship is called one to one relationship.

Plain text : S. SIMAR Singh Sabharwal

Cipher text : A. AIMAR Aingh Aabharwal

Plain Text : KHALSA (A → S)

Cipher Text : KHSLSS

2. **Polyalphabetic Cipher :**

- Each occurrence of a character can have different substitution.
- The relationship between a character in the plain text to a character into the cipher text is one to many relationship. When is replaed by group of letter.

Example : Character A could be changed to D in the beginning of text but it could be changed to M at the middle.

AMAR : Plain Text

DMMR : Cipher Text

Plain text : HELLO

Cipher text : A B N Z F

Here each occurence of L is encrypted by different character. The First is replaced with N and Second is replaced with Z.

9.5.3 Transposition Cipher

- In the Transposition cipher is related with the position or Location changes.
- A character in the first position of the plain text may be may appear in the tenth portion of the cipher text.
- In simple words, a Transposition cipher reorder the symbols in a block of symbols.

A Transposition symbol reorders permutes the symbols.

In transposition cipher, the key is mapping between the position of the symbols in the plain text and cipher text.

Example :

Plain text	2	4	1	3
Cipher text	1	2	3	4

In Encryption we move the character at position

$2 \longrightarrow 1$

$4 \longrightarrow 2$

$1 \longrightarrow 3$

$3 \longrightarrow 4$

This is the Rule (Key)

Example

Plain text 2 4 1 3 4 3 2 1 1 1 2 3 3 2 1 3

We make the Block of

2413 4321 1123 3213

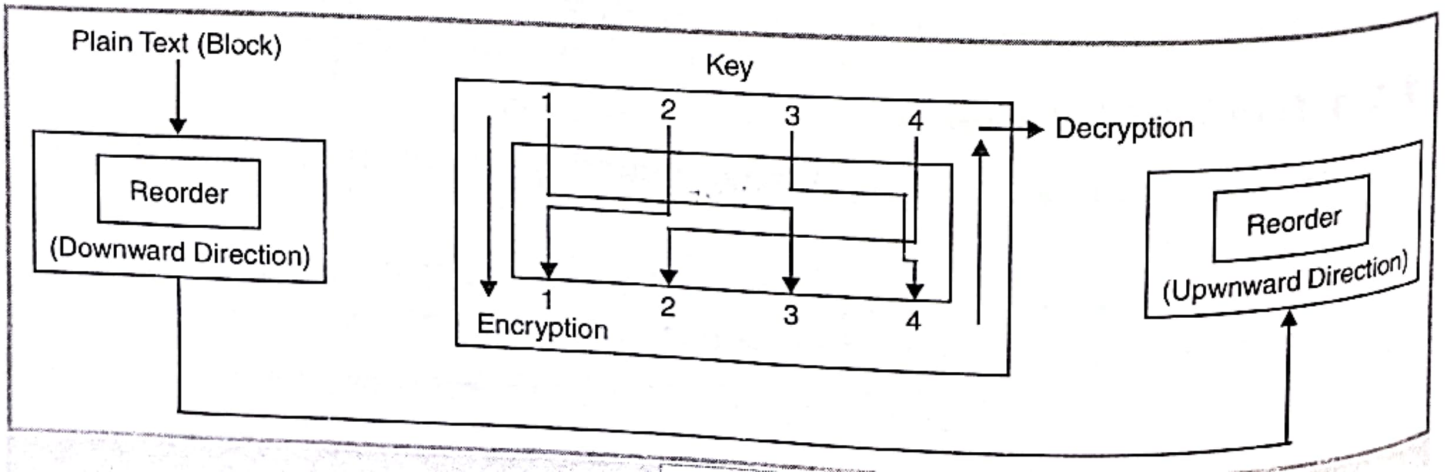
Our key works like :

(1)	4	3	1	2	[2nd $\longrightarrow$ 1st]
(2)	43	31	13	23	[4th $\longrightarrow$ 2nd]
(3)	432	314	131	233	[1st $\longrightarrow$ 3rd]
(4)	4321	3142	1312	2331	[3rd $\longrightarrow$ 4th]

This is encrypted Transposition cipher.

Cipher Text : 4321 3142 1312 2331

Transposition Cipher



9.5.4 One Time PADS

- Constructing an unbreakable cipher is actually quite easy; this technique has been known for decades.
- First choose a random bit string; by using ASCII code representation.
- Finally, compute XOR (exclusive OR) of these two string bit by bit. The resulting cipher text can not be broken because in a sufficiently large sample of cipher text, each letter will occur equally often, as will every dicyram every trigram an so on.
- This method is known as one time pad is to all present and future attacks no matter how much computational power this intruder has.
- The reason drives from the information theory : there is simply no information in the message because all possible plain texts of given length are equally present.

Example : Message "I Love you" is converted to 7 bit ASCII.

One Time Pad in choose as XoRed with the message to set the cipher text.

Message 1					
1001001	0100000	1101100	1101111	1110110	1100101
0100000	1111001	1101111	1110101	0101110	
Pad 1					
1010010	1001011	1110010	1010101	1010010	1100011
0001011	0101010	1010111	1100110	0101011	
Cipher text					
0011011	1101011	0011110	0111010	0100100	
0000110	0101011	1010011	0111000	0010011	0000101

9.5.5 Two Fundamental Cryptographic Principles

Fundamental Principles of Cryptography :

1. Redundancy

- The first principle is that all the encrypted messages must contain some redundancy, that is, information not needed to understand the message.

Cryptographic principle 1 : Message must contain some redundancy.

- The redundancy is need to prevent the active intruder from sending the garbage and tricking the receiver into decrypt the garbage and acting on the "Plain text".
- However this same redundancy make it much easier for passive intruders to break the system so there is some tenision here.
- Further more, the redundancy should never be in the form of *n* zeros at the start or at the end of message; since running such messages through some cryptographic algorithm gives more predictable results making the crypt analysts, job easier.
- A CRC polynomial is much better than a run of OS such that receiver can easily verify it, but it generate more work for cryptanalyst. It is better to use cryptographic hash.

2. Freshness

- The second cryptographic principle is that some measure must be taken to ensure that each message received can be verified as being fresh that is sent very recently.
- This message is needed to prevent active intruders from playing back old message.
- If no such messages were taken, our ex-employed could tap TCP's phone line and keep just repealing previously sent valid messages.

Cryptographic Principle-2 : Some method is needed to foil replay attack.

- One such message is including in every message a timestamp valid for say 10 seconds.
- After every 10 second message is refreshed.

9.6 PUBLIC KEY

- Public key cryptography was invented in 1976 by Whitfield Diffie and Martin Hellman.
- For this reason, it is sometime called *Diffie-Hellman encryption.*
- A cryptographic system that uses two keys -- a **public key** known to everyone and a **private *or* secret key** known only to the recipient of the message.

- When Simar wants to send a secure message to Aekam, Simar uses the public key to encrypt the message. Aekam then uses Simar's private key to decrypt it.
- An important element to the public key system is that the public and private keys are related in such a way that only the public key can be used to encrypt messages and only the corresponding private key can be used to decrypt them.
- Moreover, it is virtually impossible to deduce the private key if you know the public key.
- Public-key systems, such as Pretty Good Privacy (PGP), are becoming popular for transmitting information via the Internet.
- They are extremely secure and relatively simple to use.
- The only difficulty with public-key systems is that you need to know the recipient's public key to encrypt a message for him or her.
- It is also called *asymmetric encryption* because it uses two keys instead of one key (*symmetric encryption*)

9.7 RSA ALGORITHM

- RSA is an Internet encryption and authentication system that uses an algorithm developed in 1977 by Ron Rivest, Adi Shamir, and Leonard Adleman.
- RSA is the first character of last name of the developrs *i.e.* Rivest – R, Shamir – S, Adleman-A.
- The RSA algorithm is the most commonly used encryption and authentication algorithm and is included as part of the Web browsers from Microsoft and Netscape.

9.7.1 Working of RSA Algorithm

1. Multiplying two large prime numbers (a prime number is a number divisible only by that number and 1)
2. Through additional operations deriving a set of two numbers that constitutes the public key and another set that is the private key. Once the keys have been developed, the original prime numbers are no longer important and can be discarded.
3. Both the public and the private keys are needed for encryption/ decryption but only the owner of a private key ever needs to know it.

Using the RSA system, the private key never needs to be sent across the Internet.

4. The private key is used to decrypt text that has been encrypted with the public key.

- Hence, if I send you a message, I can find out your public key (but not your private key) from a central administrator and encrypt a message to you using your public key. When you receive it, you decrypt it with your private key.

9.7.2 Key Generation Algorithm

1. Choose two very large random prime integers:
   p and q
2. Compute n and φ(n):
   $n = pq$ and $\varphi(n) = (p-1)(q-1)$
3. Choose an integer e, $1 < e < \varphi(n)$ such that:
   $\gcd(e, \varphi(n)) = 1$(where gcd means greatest common denominator)
4. Compute d, $1 < d < \varphi(n)$ such that:
   $ed \equiv 1 \pmod{\varphi(n)}$
   - the public key is (n, e) and the private key is (n, d)
   - the values of p, q and φ(n) are private
   - e is the public or encryption exponent
   - d is the private or decryption exponent

(i) Encryption

The cyphertext C is found by the equation '$\mathbf{C = M^e \bmod n}$' where M is the original message.

(ii) Decryption

The message M can be found form the cyphertext C by the equation '$M = \mathbf{C^d \bmod n}$'.

A simple example

This is an extremely simple example and would not be secure using primes so small, normally the primes p and q would be much larger.

1. Select the prime integers q=11, q=3.
2. n=pq=33; φ(n)=(p-1)(q-1)=20
3. Choose e=3
   - Check gcd(3,20)=1

4. Compute d=7
   - $(3)d \equiv 1 \pmod{20}$

Therefore the public key is (n, e) = (33, 3) and the private key is (n, d) = (33, 7).

Now say we wanted to encrypt the message **M=7**

- $C = M^e \bmod n$
- $C = 7^3 \bmod 33$
- $C = 343 \bmod 33$
- $C = 13$

So now the cyphertext C has been found. The decryption of C is performed as follows.

- $M' = C^d \bmod n$
- $M' = 13^7 \bmod 33$
- $M' = 62{,}748{,}517 \bmod 33$
- $M' = 7$.
- The value of M and M′ is same *i.e.* 7.
- As you can see after the message has been encrypted and decrypted the final message M' is the same as the original message M.
- A more practical way to use the algorithm is to convert the message to hexadecimal and perform the encryption and decryption steps on each octet individually.

9.8 TYPES OF ENCRYPTION

(i) Symmetric Encryption

- Symmetric encryption is the oldest and best-known technique.
- A secret key, which can be a number, a word, or just a string of random letters, is applied to the text of a message to change the content in a particular way.
- This might be as simple as shifting each letter by a number of places in the alphabet.
- As long as both sender and recipient know the secret key, they can encrypt and decrypt all messages that use this key.

(ii) Asymmetric Encryption

- The problem with secret keys is exchanging them over the Internet or

a large network while preventing them from falling into the wrong hands.

- Anyone who knows the secret key can decrypt the message.
- One answer is asymmetric encryption, in which there are two related keys--a key pair.
- A public key is made freely available to anyone who might want to send you a message.
- A second, private key is kept secret, so that only you know it.
- Any message (text, binary files, or documents) that are encrypted by using the public key can only be decrypted by applying the some algorithm, but by using the matching private key.
- Any message that is encrypted by using the private key can only be decrypted by using the matching public key.
- This means that you do not have to worry about passing public keys over the Internet (the keys are supposed to be public).
- A problem with asymmetric encryption, however, is that it is slower than symmetric encryption.
- It requires far more processing power to both encrypt and decrypt the content of the message.

9.9 DIGITAL SIGNATURE

- We are all familiar with the concept of a signature.
- We sign a document to show that it originated from us or was approved by us.
- The signature is proof to the recipient that the document comes from the correct entity. When a customer signs a check to himself, the bank needs to be sure that the check is issued by that customer and nobody else.
- In other words, a signature on a document, when verified, is a sign of authentication that the document is authentic.
- When Alice sends a message to Bob, Bob needs to check the authenticity of the sender; he needs to be sure that the message comes from Alice and not Eve.
- Bob can ask Alice to sign message electronically.

- In other words, an electronic signature can prove the authenticity of Alice as the sender of the message.
- We refer to this type of signature as a digital signature.
- Basically there are two types of signatures:
  1. Conventional Signature
  2. Digital Signature

1. Conventional Signature

- A conventional signature is included in the document; it is part of the document.
- When we write a check, the signature is on the check ; it is not a separate document.
- In conventional signature, when the recipient receives a document, it compares the signature on the document with the signature on file.
- If they are the same, the document is authentic.
- The recipient needs to have a copy of this signature on file for comparison.
- In this a copy of the signed document can be distinguished from the original one on file.
- In this , there is normally a one-to-many relationship between a signature and documents.
- A person, for example, has a signature that is used to sign many checks, many documents, etc.
- In conventional signature a signature is like a private "key" belonging to the signer of the document.
- The signer uses it to sign a document; no one else has this signature.
- The copy of the signature is on file like a public key; anyone can use it to verify a document, to compare it to the original signature.

2. Digital Signature

- In Digital Signature, we send the signature as a separate document. The sender sends two documents: the message and the signature.
- The recipient receives both documents and verifies that the signature belongs to the supposed sender.
- If this is proved, the message is kept; otherwise, it is rejected.

- In digital signature, the recipient receives the message and the signature.
- A copy of the signature is not stored anywhere.
- The recipient needs to apply a verification technique to the combination of the message and the signature to verify the authenticity.
- In digital signature, to compare the signed and the original signature there is a factor of time (such as a timestamp) on the document.
- For example, suppose Alice sends a document instructing Bob to pay Eve.
- If Eve intercepts the document and the signature, she can resend it later to get money again from Bob. In digital signature, there is a one-to-one relationship between a signature and a message.
- Each message has its own signature.
- The signature of one message cannot be used in another message.
- If Bob receives two messages, one after another, from Alice, he cannot use the signature of the first message to verify the second.
- Each message needs a new signature. In digital signature, the signer uses her private key, applied to a signing algorithm, to sign the document.
- The verifier, on the other hand, uses the public key of the signer, applied to the verifying algorithm, to verify the document.
- Can we use a secret (symmetric) key to both sign and verify a signature? The answer is no for several reasons.
- First, a secret key is known only between two entities (Alice and Bob, for example).
- So if Alice needs to sign another document and send it to Ted, she needs to use another secret key.
- Second, as we will see, creating a secret key for a session involves authentication, which normally uses digital signature.
- We have a vicious cycle. Third, Bob could use the secret key between himself and Alice, sign a document, send it to Ted, and pretend that it came from Alice.
- A digital signature needs a public-key system.

9.9.1 Procedure for Digital Signature

- Digital signature can be achieved in two ways: signing the document and signing a digest of the document.

A. Signing the Document

- The easier, but less efficient way is to sign the document itself.
- Signing a document is encrypting it with the private key of the sender; verifying the document is decrypting it with the public key of the the sender.
- In digital signature public and private keys as used for confidentiality.
- In the latter, the private and public keys of the receiver are used in the process.
- The sender uses the public key of the receiver to encrypt; the receiver uses his own private key to decrypt.
- In digital signature, the private and public keys of the sender are used.
- The sender uses her private key; the receiver uses the public key of the sender.
- In a cryptosystem, we use the private and public keys of the receiver;
- In digital signature, we use the private and public key of the sender.

B. Signing the Digest

- Public key is very inefficient in a cryptosystem if we are dealing with long messages.
- In a digital signature system, our messages are normally long, but we have to use public keys.
- The solution is not to sign the message itself; instead, we sign a digest of the message.
- As we learned, a carefully selected message digest has a one-to-one relationship with the message.
- The sender can sign the message digest, and the receiver can verify the message digest. The effect is the same.
- A digest is made out of the message at Alice's site. The digest then goes through the signing process using Alice's private key.
- Alice then sends the message and the signature to Bob.

9.9.2 Advantages of Digital Signature

For a security purpose A digital signature provide the following services

1. Message Integrity
2. Message Authentication
3. Non repudiation.

1. Message Integrity

- The integrity of the message is preserved even if we sign the whole message because we cannot get the same signature if the message is changed.
- The signature schemes today use a hash function in the signing and verifying algorithms that preserve the integrity of the message.
- A digital signature today provides message integrity.

2. Message Authentication

- A secure signature scheme, like a secure conventional signature (one that cannot be easily copied), can provide message authentication.
- Bob can verify that the message is sent by Alice because Alice's public key is used in verification.
- Alice's public key cannot create the same signature as Eve's private key.
- Digital signature provides message authentication.

3. Message Non repudiation

- If Alice signs a message and then denies it, can Bob later prove that Alice actually signed it?
- For example, if Alice sends a message to a bank (Bob) and asks to transfer ₹10,000 from her account to Ted's account, can Alice later deny that she sent this message? With the scheme we have presented so far, Bob might have a problem.
- Bob must keep the signature on file and later use Alice's public key to create the original message to prove the message in the file and the newly created message are the same.
- This is not feasible because Alice may have changed her private/public key during this time; she may also claim that the file containing the signature is not authentic.
- One solution is a trusted third party.

- People can create a trusted party among themselves.
- Alice creates a signature from her message (SA) and sends the message, her identity, Bob's identity, and the signature to the center.
- The center, after checking that Alice's public key is valid, verifies through Alice's public key that the message comes from Alice.
- The center then saves a copy of the message with the sender identity, recipient identity, and a timestamp in its archive.
- The center uses its private key to create another signature (ST) from the message.
- The center then sends the message, the new signature, Alice's identity, and Bob's identity to Bob. Bob verifies the message using the public key of the trusted center.
- If in the future Alice denies that she has sent the message, the center can show a copy of the saved message.
- If Bob's message is a duplicate of the message saved at the center, Alice will lose the dispute.

EXERCISE

1. What is the role of cryptography in the security of networking.
2. Explain the following terms :
   (i) Plain Text (ii) Cipher Text
   (iii) Key (iv) Encryption
   (v) Decryption (vi) Key Generation Algorithm
3. What are the two principle of cryptography?
4. Explain one Time Pad.
5. Explain the following :
   1. Transposition Cipher
   2. Substitution Cipher
6. Describe the working of RSA algorithm with the help of example.
7. Differentiate between symmetric Encryption and Asymmetric Encryption.
8. Illustrate the concept of digital signature by taking the suitable example.
9. What is the procedure for digital signature ? Write the advantages of digital signature.
10. Explain Public key and Private key.

□□□□□