Network Security

Course outline:

Introduction to Network Security (Client-Server Security and Data-Message Security)

Client/Server Security

Firewalls and its Types

Data and Message Security (Private or Secret and Public Key Cryptography)

Digital Signature

Digital Certificate

Certificate Authority

Third Party Authentication, SSL,VPN, SET.

Introduction to Network Security

A network security is defined as a circumstance, condition with the potential to cause economic hardship to data or network resources in the form of destruction, disclosure, modification of data, denial of service, and/or fraud, waste, and abuse.

The discussion of security concerns in electronic commerce can be divided into two broad types:
Client/server security uses various authorization methods to make sure that only valid user and programs have access to information resources such as databases. Access control mechanisms must be set up to ensure that properly authenticated users are allowed access only to those resources that they are entitled to use. Such mechanisms include password protection, encrypted smart cards, biometrics, and firewalls.

Data and transaction security ensures the privacy and confidentiality in electronic messages and data packets, including the authentication of remote users in network transactions for activities such as on-line payments. The goal is to defeat any attempt to assume another identity while involved with electronic mail or other forms of data communication. Preventive measures include data encryption using various cryptographic methods.

Client/Server Network Security

Client/server network security is one of the biggest headaches system administrators face as they balance the opposing goals of user maneuverability and easy access and site security and confidentiality of local information. According to the National Center for Computer Crime Data, computer security violations cost U.S. businesses half a billion dollars each year.

Network security on the Internet is a major concern for commercial organizations, especially top management. Recently, the Internet has raised many new security concerns. By connecting to the Internet, a local network organization may be exposing itself to the entire population on the Internet. As figure below illustrates, an Internet connection opens itself to access from other networks comprising the public Internet.

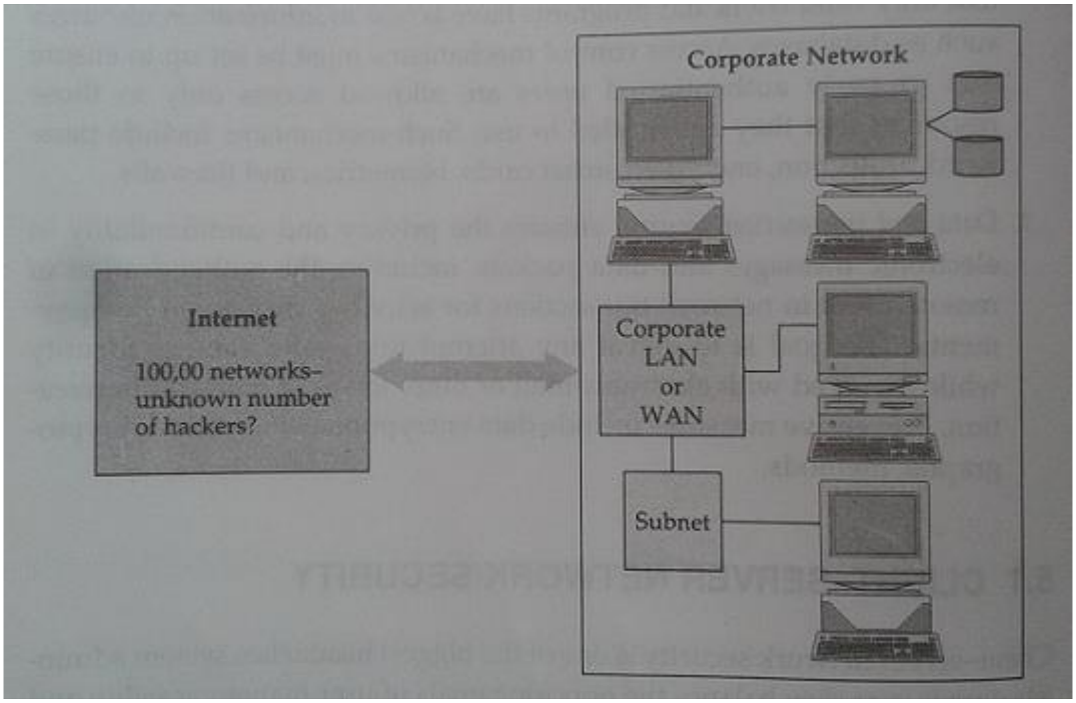


Fig: Unprotected Internet Connection

That being the case, the manager of even the most relaxed organization must pay some attention to security. For many commercial operations, security will simply be a matter of making sure that existing system features, such as passwords and privileges, are configured properly. They need to audit all access to the network. A system that records all log-on attempts—particularly the unsuccessful ones—can alert managers to the need for stronger measures. However, where secrets are at stake or where important corporate assets must be made available to remote users, additional measures must be taken. Hackers can use password guessing, password trapping, security holes in programs, or common network access procedures to impersonate users and thus pose a threat to the server.

Client–server network security problems manifest themselves in three ways:

1) **Physical security holes** result when individuals gain unauthorized physical access to a computer. A good example would be a public workstation room, where it would be easy for a wandering hacker to reboot a machine into single-user mode and tamper with the files, if precautions are not taken. On the network, this is also a common problem, as hackers gain access to network systems by guessing passwords of various users.

2) **Software security holes** result when badly written programs or "privileged" software are "compromised" into doing things they shouldn't. The most famous example of this category is the "sendmail" hole, which brought the Internet to its knees in 1988. A more recent problem was the "rlogin" hole in the IBM RS-6000 workstations, which enabled a cracker (a malicious hacker) to create a "root" shell or superuser access mode. This is the highest level of access possible and could be used to delete the entire file system, or create a new account or password file.

3) **Inconsistent usage holes** result when a system administrator assembles a combination of hardware and software such that the system is seriously flawed from a security point of view. The incompatibility of attempting two unconnected but useful things creates the security hole. Problems like this are difficult to isolate once a system is set up and running, so it is better to carefully build the system with them in mind. This type of problem is becoming common as software becomes more complex.

To reduce these security threats, various protection methods are used. At the file level, operating systems typically offer mechanisms such as access control lists that specify the resources various users and groups are entitled to access. Protection—also called authorization or access control—grants privileges to the system or resource by checking user-specific information such as passwords. The problem in the case of e-commerce is very simple: If consumers connect a computer to the Internet, they can easily log into it from anywhere that the network reaches. That's the good news. The bad news is that without proper access control, anyone else can too.

Over the years, several protection methods have been developed, including trust-based security, security through obscurity, password schemes, and biometric systems.

Trust-Based Security: Quite simply, trust-based security means to trust everyone and do nothing extra for protection. It is possible not to provide access restrictions of any kind and to assume that all users are trustworthy and competent in their use of the shared network. This approach assumes that no one ever makes an expensive breach such as getting root access and deleting all files (a common hacker trick). This approach worked in the past, when the system administrator had to worry about a limited threat. Today, this is no longer the case.

Security through Obscurity: Most organizations in the mainframe era practiced a philosophy known as security through obscurity (STO)—the notion that any network can be secure as long as nobody outside its management group is allowed to find out anything about its operational details and users are provided information on a need-to-know basis. Hiding account passwords in binary files or scripts with the presumption that "nobody will ever find them" is a prime case of STO (somewhat like hiding the housekey under the doormat and telling only family and friends). In short, STO provides a false sense of security in computing systems by hiding information.

Password Schemes: One straightforward security solution, a password scheme, erects a first-level barrier to accidental intrusion. In actuality, however, password schemes do little about deliberate attack, especially when common words or proper names are selected as passwords. For instance, network administrators at a Texas air force base discovered that they could crack about 70 percent of the passwords on their UNIX network with tools resembling those used by hackers. The simplest method used by most hackers is dictionary comparison— comparing a list of encrypted user passwords against a dictionary of encrypted common words EGCN941. This scheme often works because users tend to choose relatively simple or familiar words as passwords. To beat the dictionary comparison method, experts often recommend using a minimum of eight-character length mixed-case passwords containing at least one non-alphanumeric character and changing passwords every 60 to 90 days.

Biometric Systems: Biometric systems, the most secure level of authorization, involve some unique aspect of a person's body. Past biometric authentication was based on comparisons of fingerprints, palm prints, retinal patterns, or on signature verification or voice recognition. Biometric systems are very expensive to implement: At a cost of several thousand dollars per reader station, they may be better suited for controlling physical access—where one biometric unit can serve for many workers—than for network or workstation access. Many biometric devices also carry a high price in terms of inconvenience; for example, some systems take 10 to 30 seconds to verify an access request.

Firewalls and Its Types

The most commonly accepted network protection is a barrier—a firewall between the corporate network and the outside world (untrusted network). The term firewall can mean many things to many people, but basically it is a method of placing a device—a computer or a router—between the network and the Internet to control and monitor all traffic between the outside world and the local network. Typically, the device allows insiders to have full access to services on the outside while granting access from the outside only selectively, based on log-on name, password, IP address or other identifiers as shown in figure below.

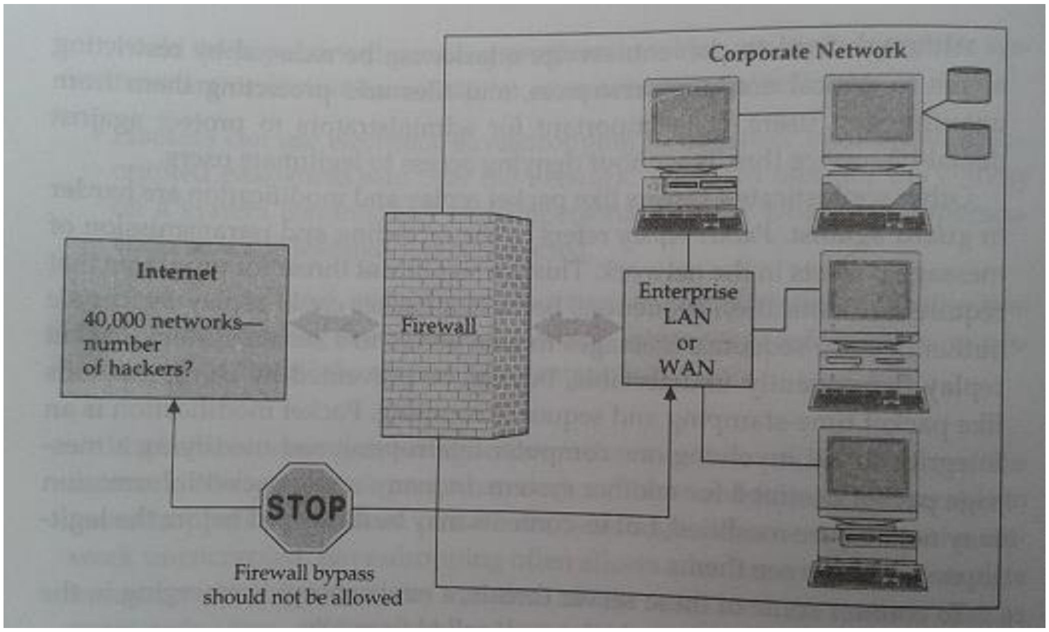


Fig: Firewall-secured Internet Connection

Generally speaking, a firewall is a protection device to shield vulnerable areas from some form of danger. In the context of the Internet, a firewall is a system—a router, a personal computer, a host, or a collection of hosts—set up specifically to shield a site or subnet from protocols and services that can be abused from hosts on the outside of the subnet. A firewall system is usually located at a gateway point, such as a site's connection to the Internet, but can be located at internal gateways to provide protection for smaller collection of hosts or subnets.

Firewalls come in several types and offer various levels of security. Generally, firewalls operate by screening packets and/or the applications that pass through them, provide controllable filtering of network traffic, allow restricted access to certain applications, and block access to everything else. The actual mechanism that accomplishes filtering varies widely, but in principle, the firewall can be thought of as a pair of mechanisms: one to block incoming traffic and the other to permit outgoing traffic. Some firewalls place a greater emphasis on blocking traffic, and others emphasize permitting traffic.

In short, the general reasoning behind firewall usage is that, without a firewall, network security is a function of each host on the network and all hosts must cooperate to achieve a uniformly high level of security. The larger the subnet, the less manageable it is to maintain all hosts at the same level of security. As mistakes and lapses in security become more common, break-ins can occur not as the result of complex attacks, but because of simple errors in configuration and inadequate passwords.

Types of Firewall (Firewalls in Practice)

Firewalls range from simple traffic logging systems that record all network traffic flowing through the firewall in a file or database for auditing purposes to more complex methods such as IP packet screening routers, hardened fire-wall hosts, and proxy application gateways. The simplest firewall is a packet- filtering gateway or screening router. Configured with filters to restrict packet traffic to designated addresses, screening routers also limit the types of services that can pass through them.

More complex and secure are application gateways. They are essentially PCs or UNIX boxes that sit between the Internet and a company's internal network to provide proxy services to users on either side. For example, a user who wants to FTP in or out through the gateway would connect to FTP software running on the firewall, which then connects to machines on the other side of the gateway. Screening routers and application gateway firewalls are frequently used in combination when security concerns are very high.

IP Packet Screening Routers: This is a static traffic routing service placed between the network service provider's router and the internal network. The traffic routing service may be implemented at an IP level via screening rules in a router or at an application level via proxy gateways and services. Figure below shows a secure firewall with an IP packet screening router.

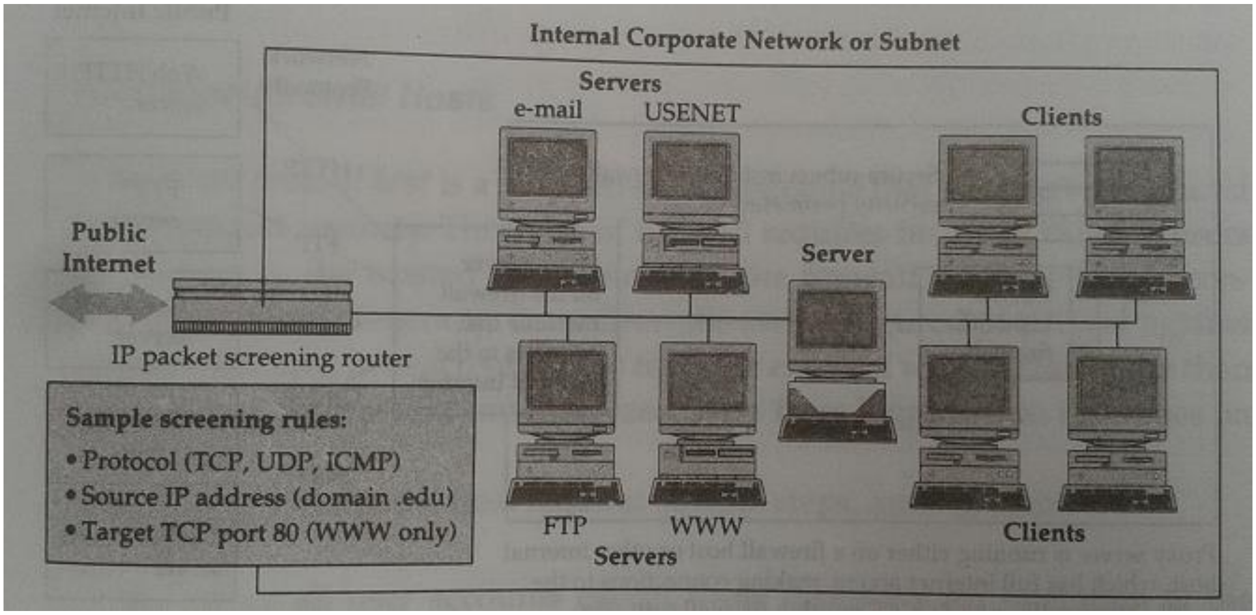
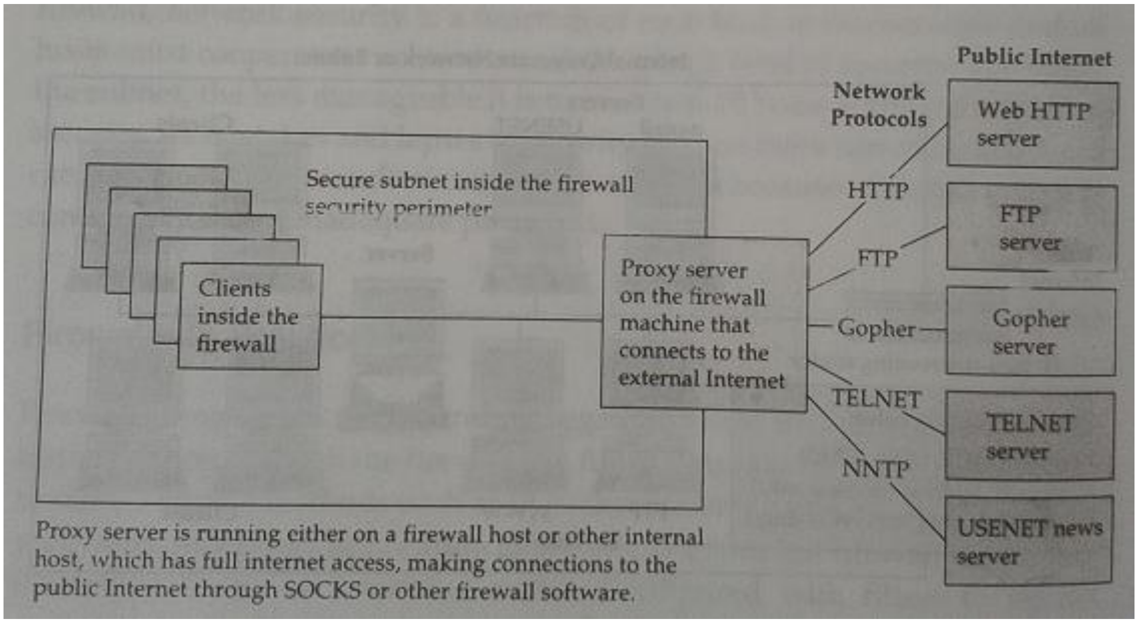

Internal Corporate Network or Subnet
Servers
e-mail
USENET
Clients
Public Internet
Server
IP packet screening router
Sample screening rules:
• Protocol (TCP, UDP, ICMP)
• Source IP address (domain .edu)
• Target TCP port 80 (WWW only)
FTP
WWW
Servers
Clients

Fig: Secure firewall with IP packet screening router

The firewall router filters incoming packets to permit or deny IP packets based on several screening rules. These screening rules, implemented into the router are automatically performed. Rules include target interface to which the packet is routed, known source IP address, and incoming packet protocol (TCP, UDP, ICMP). ICMP stands for Internet Control Message Protocol, a network management tool of the TCP/IP protocol suite.

Although properly configured routers can plug many security holes, they do have several disadvantages. First, screening rules are difficult to specify, given the vastly diverse needs of users. Second, screening routers are fairly inflexible and do not easily extend to deal with functionality different from that preprogrammed by the vendor. Lastly, if the screening router is circumvented by a hacker, the rest of the network is open to attack.

Proxy Application Gateways: A proxy application gateway is a special server that typically runs on a firewall machine. Their primary use is access to applications such as the World Wide Web from within a secure perimeter as shown in figure below. Instead of talking directly to external WWW servers, each request from the client would be routed to a proxy on the firewall that is defined by the user. The proxy knows how to get through the firewall. An application-Level proxy makes a firewall safely permeable for users in an organization, without creating a potential security hole through which hackers can get into corporate networks. The proxy waits for a request from inside the firewall, forwards the request to the remote server outside the firewall, reads the response, and then returns it to the client. In the usual case, all clients within a given subnet use the same proxy. This makes it possible for the proxy to execute efficient caching of documents that are requested by a number of clients. The proxy must be in a position to filter dangerous URLs and malformed commands.


Public Internet
Network Protocols
Web HTTP server
Secure subnet inside the firewall security perimeter
HTTP
FTP server
FTP
Proxy server on the firewall machine that connects to the external Internet
Clients inside the firewall
Gopher
Gopher server
TELNET
TELNET server
NNTP
USENET news server

Proxy server is running either on a firewall host or other internal host, which has full internet access, making connections to the public Internet through SOCKS or other firewall software.

Fig: Proxy servers on the World Wide Web

Hardened Firewall Hosts: A hardened firewall host is a stripped-down machine that has been configured for increased security. This type of firewall requires inside or outside users to connect to the trusted applications on the firewall machine before connecting further. Generally, these firewalls are configured to protect against unauthenticated interactive log-ins from the external world. This, more than anything, helps prevent unauthorized users from logging into machines on the network.

The hardened firewall host method can provide a greater level of audit and security, in return for increased configuration cost and decreased 'level of service (because a proxy needs to be developed for each desired service).

Data and Message Security (Private or Secret and Public Key Cryptography)

The lack of data and message security on the Internet has become a high- profile problem due to the increasing number of merchants trying to spur commerce on the global network. For instance, credit card numbers in their plain text form create a risk when transmitted across the Internet where the possibility of the number falling into the wrong hands is relatively high. Would you be willing to type in your credit card number knowing the risk? Even worse, would you expose your customers to that risk? In short, the lack of business transaction security is widely acknowledged as a major impediment to widespread e- commerce.

Historically, computer security was provided by the use of account passwords and limited physical access to a facility to bona fide users. As users began to dial in from their PCs and terminals at home, these measures were deemed sufficient. With the advent of remote users on internetworks, commercial transactions, mobile computers, and wireless technologies, simple password schemes are not sufficient to prevent attacks from sophisticated hackers.

Interestingly, the security problems plaguing network administrators resemble the problems facing transaction-based electronic commerce. Credit card numbers are similar to passwords in many ways. A growing threat on today's public (and sometimes even private) networks is the theft of passwords and other information that passes over them. Today's hacker has an array of tools to reach and manipulate information from remote sites as well as to engage in unauthorized eavesdropping. Unsuspecting and amateur users logging into remote hosts are the most vulnerable.

Transaction security issues can be divided into two types: **data** and **message** security. These are discussed below.

Data Security: Electronic data security is of paramount importance at a time when people are considering banking and other financial transactions by PCs. Also, computer industry trends toward distributed computing, and mobile computers, users face security challenges. One major threat to data security is unauthorized network monitoring, also called packet sniffing.

Sniffer attacks begin when a computer is compromised and the cracker installs a packet sniffing program that monitors the network to which the machine is attached. The sniffer program watches for certain kinds of network traffic, typically for the first part of any Telnet, FTP, or rlogin sessions— sessions that legitimate users initiate to gain access to another system. The first part of the session contains the log-in ID, password, and user name of the person logging into another machine, all the necessary information a sniffer needs to log into other machines. In the course of several days, the sniffer could gather information on local users logging into remote machines. So, one insecure system on a network can expose to intrusion not only other local machines but also any remote systems to which the users connect.

The fact that someone can extract meaningful Information from network traffic is nothing new. Network monitoring can rapidly expand the number of systems intruders are able to access, all with only minimal impact on the systems on which the sniffers are installed and with no visible impact on the systems being monitored. Users whose accounts and passwords are collected will not be aware that their sessions are being monitored, and subsequent intrusions will happen via legitimate accounts on the machines involved.

Message Security: Threats to message security fall into three categories:

1. confidentiality,
2. integrity, and
3. authentication.

1. **Message Confidentiality**- Confidentiality is important for uses involving sensitive data such as credit card numbers. This requirement will be amplified when other kinds of data, such as employee records, government files, and social security numbers, begin traversing the network. Confidentiality precludes access to, or release of, such information to unauthorized users.

   The environment must protect all message traffic. After successful delivery to their destination gateways, messages must be removed (expunged) from the public environment. All that remains is the accounting record of entry and delivery, including message length, authentication data, but no more. All message archiving must be performed in well-protected systems.

The vulnerability of data communications and message data to interception is exacerbated with the use of distributed networks and wireless links. The need for securing the communications link between computers via encryption is expected to rise.

2. **Message and System Integrity**- Business transactions require that their contents remain unmodified during transport. In other words, information received must have the same content and organization as information sent. It must be clear that no one has added, deleted, or modified any part of the message.

   While confidentiality protects against the passive monitoring of data, mechanisms for integrity must prevent active attacks involving the modification of data. Error detection codes or checksums, sequence numbers, and encryption techniques are methods to enhance information integrity. Encryption techniques such as digital signatures can detect modifications of a message.   .

3. **Message Sender Authentication/Identification**- For e-commerce, it is important that clients authenticate themselves to servers, that servers authenticate to clients, that both authenticate to each other. Authentication is a mechanism whereby the receiver of a transaction or message can be confident of the identity of the sender and/or the integrity of the message. In other words, authentication verifies the identity of an entity (a user or a service) using certain encrypted information transferred from the sender to the receiver.

   Authentication in e-commerce basically requires the user to prove his or her identity for each requested service. The race among various vendors in the e-commerce today is to provide an authentication method that is easy to use, secure, reliable, and scalable. Third-party authentication services must exist within a distributed network environment where a sender cannot be trusted to identify itself correctly to a receiver. In short, authentication plays an important role in the implementation of business transaction security.

Encryption Techniques for Data and Message Security

(Private and Public Key Cryptography)

The success or failure of an e-commerce operation depends on different key factors, including but not limited to the business model, the team, the customers, the investors, the product, and the security of data transmissions and storage. Data security has taken on heightened importance since a series of high-profile "cracker" attacks have humbled popular Web sites, resulted in the impersonation of Microsoft employees for the purposes of digital certification, and the misuse of credit card numbers of customers at business-to-consumer e-commerce destinations. Security is on the mind of every e-commerce entrepreneur who solicits, stores, or communicates any information that may be sensitive if lost. Technologists are building new security measures while others are working to crack the security systems. One of the most effective means of ensuring data security and integrity is **encryption**.

Encryption is a generic term that refers to the act of encoding data, in this context so that those data can be securely transmitted via the Internet. Encryption can protect the data at the simplest level by preventing other people from reading the data. In the event that someone intercepts a data transmission and manages to deceive any user identification scheme, the data that they see appears to be gibberish without a way to decode it. Encryption technologies can help in other ways as well, by establishing the identity of users (or abusers); control the unauthorized transmission or forwarding of data; verify the integrity of the data (i.e., that it has not been altered in any way); and ensure that users take responsibility for data that they have transmitted.

Encryption can therefore be used either to keep communications secret (defensively) or to identify people involved in communications (offensively). Encryption Provide Following Security:

- **Message Integrity**: provides assurance that the message has not been altered.
- **No repudiation**: prevents the users from denying he/she sent the message
- **Authentication**: provides verification of the identity of the person (or machine) sending the message.

- **Confidentiality**: give assurance that the message was not read by others.

There are two types of encryption: **symmetric key** encryption and **asymmetric key** encryption. Symmetric key and asymmetric key encryption are used, often in conjunction, to provide a variety of security functions for data and message security in e-commerce.

Symmetric Key Encryption (Private or Secret Key Encryption):

Encryption algorithms that use the same key for encrypting and for decrypting information are called symmetric-key algorithms. The symmetric key is also called a secret key because it is kept as a shared secret between the sender and receiver of information. Otherwise, the confidentiality of the encrypted information is compromised. Figure below shows basic symmetric key encryption and decryption.

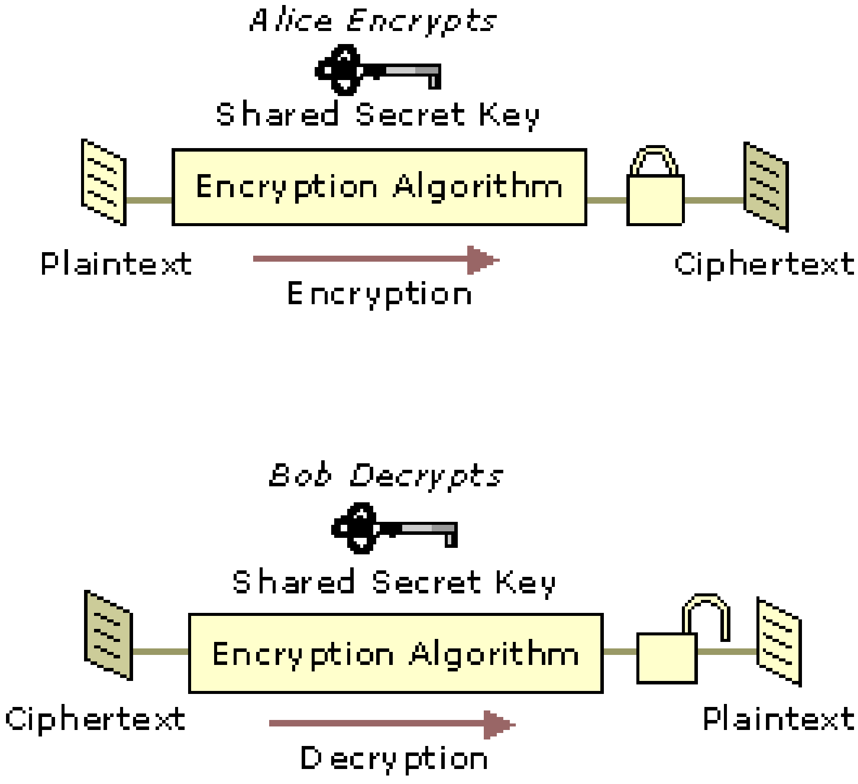


Fig: Encryption and Decryption with a Symmetric Key

Symmetric key encryption is much faster than public key encryption, often by 100 to 1,000 times. Symmetric key technology is generally used to provide secrecy for the bulk encryption and decryption of information.

Cryptography-based security technologies use a variety of symmetric key encryption algorithms to provide confidentiality. Symmetric algorithms have the advantage of not consuming too much computing power. People can use this encryption method as either a "**stream**" cipher or a "**block**" cipher, depending on the amount of data being encrypted or decrypted at a time. A stream cipher encrypts data one character at a time as it is sent or received, while a block cipher processes fixed block (chunks) of data. Common symmetric encryption algorithms include Data Encryption Standard (**DES**), Advanced Encryption Standard (**AES**), and International Data Encryption Algorithm (**IDEA**).

Asymmetric Key Encryption(Public Key Encryption):

Encryption algorithms that use different keys for encrypting and decrypting information are most often called public-key algorithms but are sometimes also called ***asymmetric key algorit***. Public key encryption requires the use of both a private key (a key that is known only to its owner) and a public key (a key that is available to and known to other entities on the network). A user's public key, for example, can be published in the directory so that it is accessible to other people in the organization. The two keys are different but complementary in function. Information that is encrypted with the public key can be decrypted only with the corresponding private key of the set. Figure below shows basic encryption and decryption with asymmetric keys.

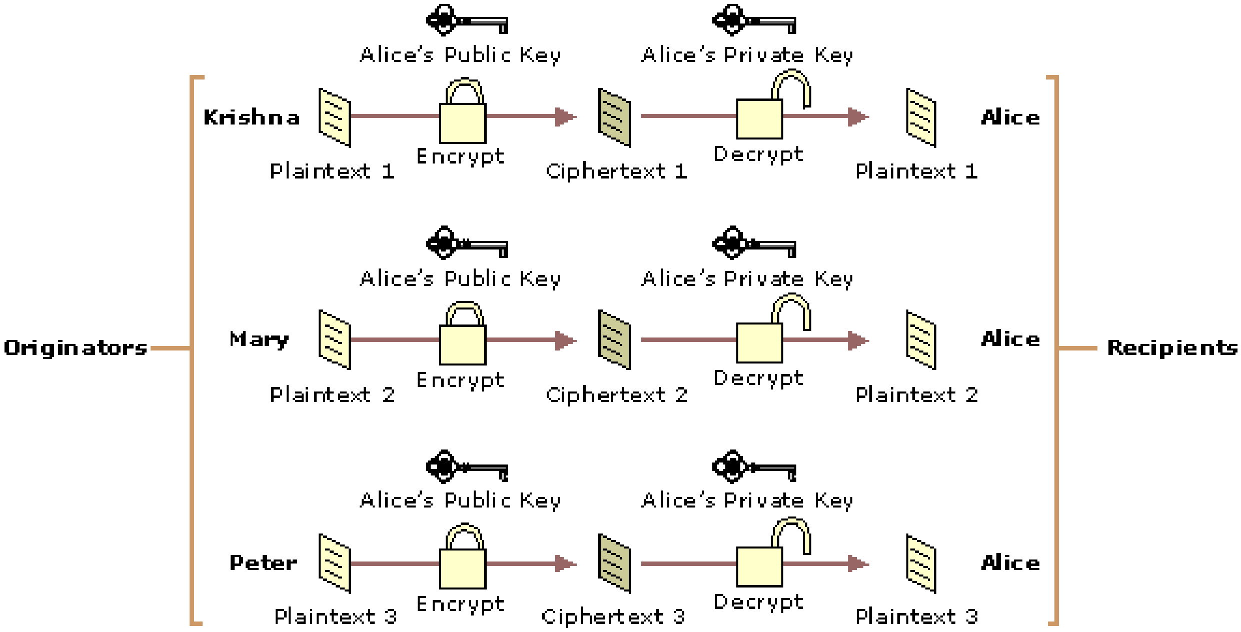


Fig: Encryption and Decryption with Asymmetric Keys

Today, public key encryption plays an increasingly important role in providing strong, scalable security on intranets and the Internet. Public key encryption is commonly used to perform the following functions:

- Encrypt symmetric secret keys to protect the symmetric keys during exchange over the network.
- Create digital signatures to provide authentication and non-repudiation for online entities.
- Create digital signatures to provide data integrity for electronic files and documents.

Algorithms that use public key encryption methods include RSA and Diffie-Hellman.

Common Cryptosystems

a) **RSA Algorithm**: RSA is the most commonly used public key algorithm, although it is vulnerable to attack. Named after its inventors, Ron Rivest, Adi Shamir and Len Adleman, of the MIT, RSA was first published in 1978. It is used for encryption as well as for electronic signatures (discussed later). RSA lets you choose the size of your public key. The 512-bit keys are considered insecure or weak. The 768-bit keys are secure from everything but 1024-bit keys are secure from virtually anything.

b) **Data Encryption Standards (DES)**: DES was developed by IBM in1974 in response to a public solicitation from the US Department of Commerce. It was adopted as a US federal standard in1977 and as a financial industry standard in1981. DES uses a 56-bit key to encrypt.

c) **3DES**: A stronger version of DES, called 3DES or Triple DES, uses three 56-bit keys to encrypt each block. The first key encrypts the data block, the second key decrypts the data block, and the third key encrypts the same data block again. The 3DES version requires a 168-bit key that makes the process quite secure and much safer than plain DES.

d) **RC4**: RC4 was designed by Ron Rivest RSA Data Security Inc. this variable-length cipher is widely used on the Internet as the bulk encryption cipher in the SSL protocol, with key length ranging from 40 to 128 bits. RC4 has a repudiation of being very fast.

e) **IDEA**: IDEA (International Data Encryption Algorithm) was created in Switzerland in1991. it offers very strong encryption using 1 128-bit key to encrypt 64-bit blocks. This system is widely used as the bulk encryption cipher in older version of Pretty Good Privacy(PGP)

Digital Signature

Just as handwritten signatures or physical thumbprints are commonly used to uniquely identify people for legal proceedings or transactions, so digital signatures are commonly used to identify electronic entities for online transactions. A digital signature uniquely identifies the originator of digitally signed data and also ensures the integrity of the signed data against tampering or corruption.

One possible method for creating a digital signature is for the originator of data to create the signature by encrypting all of the data with the originator's private key and enclosing the signature with the original data. Anyone with the originator's public key can decrypt the signature and compare the decrypted message to the original message. Because only someone with the private key can create the signature, the integrity of the message is verified when the decrypted message matches the original. If an intruder alters the original message during transit, the intruder cannot also create a new valid signature. If an intruder alters the signature during transit, the signature does not verify properly and is invalid.

However, encrypting all data to provide a digital signature is impractical for following two reasons:

- The ciphertext signature is the same size as the corresponding plaintext, so message sizes are doubled, consuming large amounts of bandwidth and storage space.
- Public key encryption is slow and places heavy computational loads on computer processors.

Digital signature algorithms use more efficient methods to create digital signatures. The most common types of digital signatures today are created by signing **message digests** with the originator's private key to create a digital thumbprint of the data. Because only the message digest is signed, the signature is usually much shorter than the data that was signed. Therefore, digital signatures place a relatively low load on computer processors during the signing process, consume insignificant amounts of bandwidth. Two of the most widely used digital signature algorithms today are the **RSA digital signature** process and the **Digital Signature Algorithm** (DSA).

RSA Data Security Digital Signature Process: In the RSA digital signature process, the private key is used to encrypt only the message digest. The encrypted message digest becomes the digital signature and is attached to the original data. Figure below illustrates the basic RSA Data Security digital signature process.

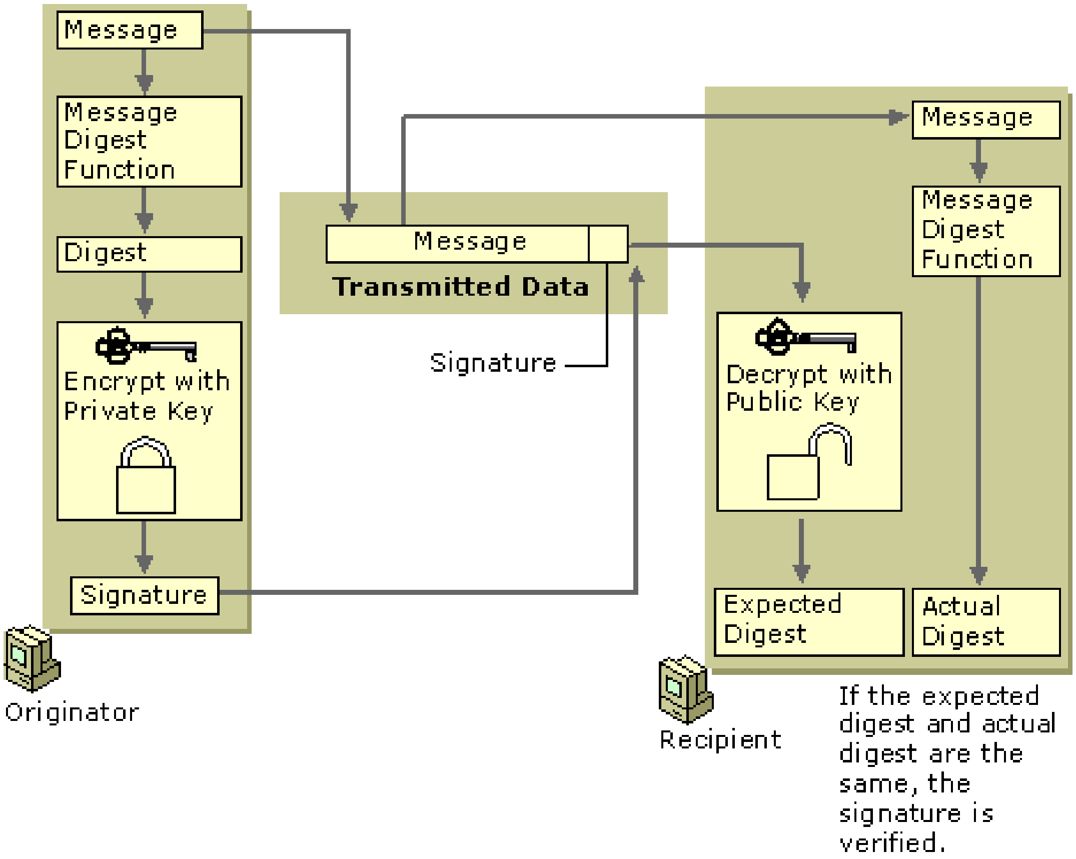


Fig: Basic RSA Data Security Digital Signature Process

To verify the contents of digitally signed data, the recipient generates a new message digest from the data that was received, decrypts the original message digest with the originator's public key, and compares the decrypted digest with the newly generated digest. If the two digests match, the integrity of the message is verified. The identification of the originator also is confirmed because the public key can decrypt only data that has been encrypted with the corresponding private key.

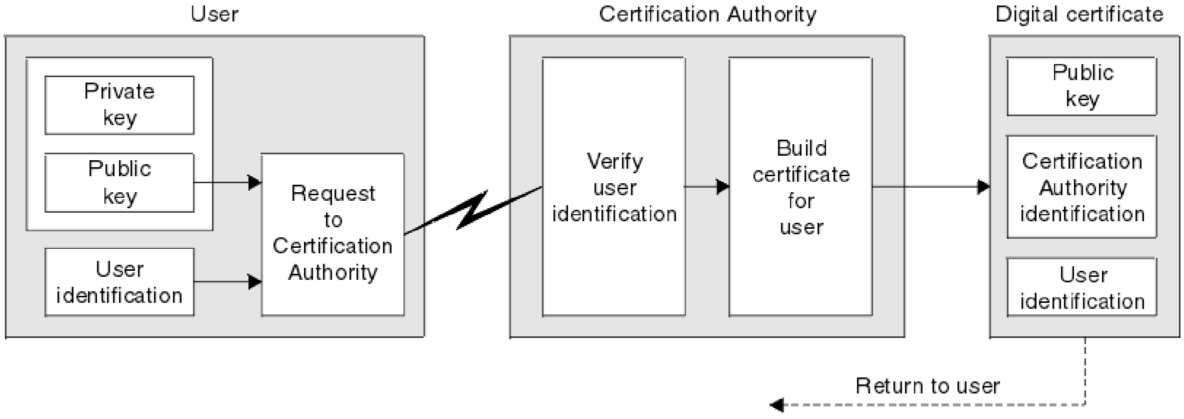
Digital Certificate and Certification Authority

Digital certificates are electronic credentials that are used to assert the online identities of individuals, computers, and other entities on a network. **Digital certificates** function similarly to identification cards such as passports and drivers licenses. Most commonly they contain a public key and the identity of the owner. They are issued by certification authorities (CAs) that must validate the identity of the certificate-holder both before the certificate is issued and when the certificate is used. Common uses include business scenarios requiring authentication, encryption, and digital signing.

Most certificates in common use today are based on the X.509v3 certificate standard. X.509v3 stands for version 3 of the International Telecommunication Union Telecommunication Standardization Sector (ITU-T) recommendation X.509 for certificate syntax and format. Typically, certificates contain the following information:

- The subject’s public key value
- The subject’s identifier information, such as the name and email address
- The validity period (the length of time that the certificate is considered valid)
- Issuer identifier information
- The digital signature of the issuer, which attests to the validity of the binding between the subject’s public key and the subject’s identifier information

Process to obtain a Certificate From CA: One can obtain a certificate for your business from commercial CAs. The Issuing entities of commercial CAs provide certificate with a cost. User can generate a Key pair of its own and generate a Certificate Signing Request (CSR) and then send the CSR to Issuing CA for a certificate. CSR contains the public key of the user and user identity information in a format that issuing CAs would normally expect as shown in figure below.



A **Certificate Authority (CA)** issues digital certificates that contain a public key and the identity of the owner. The matching private key is not made available publicly, but kept secret by the end user who generated the key pair. The certificate is also a confirmation or validation by the CA that the public key contained in the certificate belongs to the person, organization, server or other entity noted in the certificate. A CA's obligation in such schemes is to verify an applicant's credentials, so that users and relying parties can trust the information in the CA's certificates. CAs use a variety of standards and tests to do so. In essence, the Certificate Authority is responsible for saying "yes, this person is who they say they are, and we, the CA, verify that".

If the user trusts the CA and can verify the CA's signature, then he can also verify that a certain public key does indeed belong to whoever is identified in the certificate. Browsers maintain list of well known CAs root certificates. Aside from commercial CAs, some providers issue digital certificates to the public at no cost. Large institutions or government entities may have their own CAs.

Third Party Authentication

In third-party authentication systems, the password or encryption key itself never travels over the network. Rather, an "authentication server" maintains a file of obscure facts about each registered user. At log-on time, the server demands the entry of a randomly chosen fact—mother's maiden name is a traditional example—but this information is not sent to the server. Instead, the server uses it (along with other data, such as the time of day) to compute a token. The server then transmits an encrypted message containing the token, which can be decoded with the user's key. If the key was properly computed, the user can decrypt the message. The message contains an authentication token that allows users to log on to network services.

There are many variations on this theme. For example, users can tell the authentication server with which remote computer they want to converse.

> **Kerberos**: Kerberos is a popular third-party authentication protocol. Kerberos is an encryption-based system that uses secret key encryption designed to authenticate users and network connections. It was developed at MIT's Project Athena in the 1980s and is

named after the three-headed dog of Greek mythology that guards the entrance to Hades. Like its namesake, Kerberos is charged with preventing unauthorized access and does it so well that it is now a de facto standard for effecting secure, authenticated communications across a network.

The assumption of Kerberos is that the distributed environment is made up of unsecured workstations, moderately secure servers, and highly secure key-management machines. Kerberos provides a means of verifying the identities of requestor (a workstation user or a network server) on an unprotected network. The goal is to accomplish security without relying on authentication by the host computer, without basing trust on the IP addresses, without requiring physical security of all the hosts on the network, and under the assumption that IP packets on the network can be read, modified, and inserted at will. Kerberos performs authentication under these conditions as a trusted third-party authentication service by using conventional cryptography (secret key).

The authentication process proceeds as follows: Client A sends a request to the Kerberos authentication server (KAS) requesting "credentials" for a given server, B. The KAS responds with the following information, which is encrypted in A's key:

- A "ticket" for the server. This ticket contains B's key.
- A temporary encryption key (often called a "session key").

A then transmits—the client's identity and a copy of the session key, both encrypted in B's key—to B.

The session key (now shared 'by the client and server) is used to authenticate the client and used to authenticate the server in future transaction. The session key is then used to encrypt further communication between the two parties or to exchange a separate sub-session key to be used to encrypt further communication.

Using Certificates for Secure Web Communications (SSL)

Secure Sockets Layer (SSL) and **Transport Layer Security** (TLS) are protocols that are used to provide secure Web communications on the Internet or intranets. TLS is the standardized (on the Internet Engineering Task Force—IETF—level) version of SSL. TLS is also referred to as SSL version 3.1, whereas the most commonly used SSL version is 3.0. Both protocols can provide the following basic security services:

- **Mutual authentication.** Verifies the identities of both the server and client through exchange and validation of their digital certificates.
- **Communication privacy.** Encrypts information exchanged between secure servers and secure clients using a secure channel.
- **Communication integrity.** Verifies the integrity of the contents of messages exchanged between client and server, which ensures that messages haven’t been altered en route.

Sample Scenario Example: Here’s an example of an environment using SSL/TLS. When you use the Internet for online banking, it’s important to know that your Web browser is communicating directly and securely with your bank’s Web server. Your Web browser must be able to achieve Web server authentication before a safe transaction can occur. That is, the Web server must be able to prove its identity to your Web browser before the transaction can proceed. Microsoft IE uses SSL to encrypt messages and transmit them securely across the Internet, as do most other modern Web browsers and Web servers.

Computer Authentication in VPNs

The use of certificates for authentication of VPN connections is the strongest form of authentication available with the Windows Server 2003 family. You must use certificate-based authentication for VPN connections.

Sample Scenario Example: Here’s a short example of the use of certificates in a VPN scenario. When an employee logs in to the organization’s network from home using a VPN, the VPN server can present a server certificate to establish its identity. Because the corporate root authority is trusted and the corporate root CA issued the certificate of the VPN server, the client computer can proceed with the connection and the employee knows their computer is actually connected to their organization’s VPN server.

The VPN server must also be able to authenticate the VPN client before data can be exchanged over the VPN connection. Either computer-level authentication occurs with the exchange of computer certificates or user-level authentication occurs though the use of a Point-to-Point Protocol (PPP) authentication method.

The client computer certificate can serve multiple purposes, most of which are based in authentication, allowing the client to use many organizational resources without needing individual certificates for each resource. For example, the client certificate might allow clients VPN connectivity, as well as access to the company store intranet site, product servers, and the human resources database where employee data is stored.

Secure Electronic Transmission (SET)

The **Secure Electronic Transmission** protocol imitates the current structure of the credit card processing system. SET makes banks by default one of the major distributors of certificates. When a user might change organizations or lose his or her key pair, or an e-commerce site using SSL may discontinue its operations; a certificate must be revoked before it expires. In all these cases, the certificate needs to be revoked before it expires so that it cannot be used intentionally or unintentionally.

The most important property of SET is that the credit card number is not open to the seller. On the other hand, the SET protocol, despite strong support from Visa and MasterCard, has not appeared as a leading standard.

The two major reasons for lack of widespread acceptance are followings:
(1) The complexity of SET
(2) The need for the added security that SET provides.

Though, this might change in the future as encryption technology becomes more commonly utilized in the e-business world.

Advantages of SET: Some of the advantages of SET contain the following:

1. Information security: Neither anyone listening in nor a merchant can use the information passed during a transaction for fraud.
2. Credit card security: There is no chance for anybody to steal a credit card.
3. Flexibility in shopping: If a person has a phone he/she can shop.

Disadvantages of SET: Some of the disadvantages of SET include its complexity and high cost for implementation.