SECURITY IN E COMMERCE

1. Ecommerce Security

   E-commerce security is the protection of e-commerce assets from unauthorized access, use, alteration, or destruction.

   Six dimensions of e commerce security:
   1. Integrity: prevention against unauthorized data modification
   2. Nonrepudiation: prevention against any one party from reneging on an agreement after the fact
   3. Authenticity: authentication of data source
   4. Confidentiality: protection against unauthorized data disclosure
   5. Privacy: provision of data control and disclosure
   6. Availability: prevention against data delays or removal

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 users 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 the figure below illustrates, an Internet connection opens itself to access from other networks comprising the public Internet.

Fig: Unprotected Internet Connection 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. 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 house key 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.

Security Threats in Client –Server Systems

Mobile Codes Emerging threat in the e-commerce world is mobile code which in many ways resembles a more traditional virus threat. It is an executable program that has the ability to move from machine to machine and also to invoke itself without external influence. it can be divided into two major categories.

- Threats to local computing environment from mobile software
- Access control and threats to servers that include impersonation, eavesdropping, denial of service, packet relay and packet modification.

Threats to Client

The Internet tends to be the major security threat for running client software as client programs interpret data downloaded from arbitrary servers on the internet. In absence of checks on imported data, the potential exists for this data to disrupt programs running on the systems.Most of the client threats arise from malicious data or code (viruses, worms, Trojan Horse, logic bombs).These codes mistakenly intrude into standalone PCs and have the ability to attack systems on network where the maintenance cost tends to be significant.

Threats to Servers

Threats to servers consist of unauthorized modification of server data, eavesdropping, modification of data packets and compromise of a server system by exploiting bugs in the server software. They are much more susceptible to attacks where legitimate users are impersonated. Hackers have potential access to a large number of systems. As a result, computers that are not properly configured and running programs with security holes are particularly vulnerable.Hackers can use popular UNIX programs like Finger, rsh or ruser to discover account names and then try to guess simple passwords using a dictionary

Hackers can spoof or configure a system to masquerade as another system thus gaining unauthorized access to resources or information on systems that trust the system being mimicked.

Hackers can eavesdrop using software that monitors packets sent over the network. Information sent over Telnet or FTP is often sent unencrypted which allows a hacker to make a complete transcript of network activity and obtain sensitive information.The two most common forms of Denial of Service (DOS) attacks are:

Service overloading: This may happen to servers for instance, if anyone writes a small loop that sends continuous requests for a particular file. The server tries to respond in good faith. It may also happen due to accidental infinite loops.

Message flooding: This occurs when someone sends a very large file to a message box every few minutes. This message box rapidly grows in size and begins to occupy all the space on the disk and increases the number of receiving processes on the recipient's machine, trying it up even more and often causing a disk crash. The best way to avoid message overloading is to provide separate areas for different programs and to make provisions for graceful failure.

Security Threats in E Commerce:

ECommerce refers to the activity of buying and selling things over the internet. Simply, it refers to the commercial transactions which are conducted online. E-commerce can be drawn on many technologies such as mobile commerce, Internet marketing, online transaction processing, electronic funds transfer, supply chain management, electronic data interchange (EDI), inventory management systems, and automated data collection systems.

E-commerce threat is occurring by using the internet for unfair means with the intention of stealing, fraud and security breach. There are various types of e-commerce threats. Some are accidental, some are purposeful, and some of them are due to human error. The most common security threats are an electronic payments system, e-cash, data misuse, credit/debit card frauds, etc.

Malicious Code:

Malicious code is the term used to describe any code in any part of a software system or script that is intended to cause undesired effects, security breaches or damage to a system. Malicious code is an application security threat that cannot be efficiently controlled by conventional antivirus software alone. Malicious code describes a broad category of system security terms that includes attack scripts, viruses, worms, Trojan horses, backdoors and malicious active content.

Malicious code may also include time bombs, hardcoded cryptographic constants and credentials, deliberate information and data leakage, rootkits and anti-debugging techniques. These targeted malicious code threats are hidden in software and mask their presence to evade detection by traditional security technologies.

Once inside your environment, malicious code can enter network drives and propagate. Malicious code can also cause network and mail server overload by sending email messages; stealing data and passwords; deleting document files, email files or passwords; and even reformatting hard drives.

Adware:

Adware, or advertising supported software, is software that displays unwanted advertisements on your computer. Adware programs will tend to serve you pop-up ads, can change your browser's homepage, add spyware and just bombard your device with advertisements. Adware is a more succinct name for potentially unwanted programs. It's not quite a virus and it may not be as obviously malicious as a lot of other problematic code floating around on the Internet. Make no mistake about it, though, that adware needs to come off of whatever machine it's on. Not only can adware be really bothersome every time you use your machine, it could also cause long-term issues for your device.

Adware uses the browser to collect your web browsing history in order to 'target' advertisements that seem tailored to your interests. At their most innocuous, adware infections are just annoying. For example, adware barrages you with pop-up ads that can make your Internet experience markedly slower and more labor intensive.

The most common reason for adware is to collect information about you for the purpose of making advertising dollars. It's called adware when it's on a computer, and madware when it's on a mobile device, such as your smartphone or tablet. No matter what the adware or malware is, it's likely going to slow down your machine and or even make it more prone to crashing.

Spyware:

Spyware is unwanted software that infiltrates your computing device, stealing your internet usage data and sensitive information. Spyware is classified as a type of malware — malicious software designed to gain access to or damage your

computer, often without your knowledge. Spyware gathers your personal information and relays it to advertisers, data firms, or external users.

Spyware is used for many purposes. Usually it aims to track and sell your internet usage data, capture your credit card or bank account information, or steal your personal identity. How? Spyware monitors your internet activity, tracking your login and password information, and spying on your sensitive information.

Some types of spyware can install additional software and change the settings on your device, so it's important to use secure passwords and keep your devices updated.

If you've ever been a victim of identity theft or credit card fraud, you're not alone. Cybercrime statistics tell the story:

- A total of 978 million people in 20 countries were affected by cybercrime in 2017, according to Norton Cyber Security Insights Report Global Results.
- Victims of cybercrime globally lost $172 billion.

Spyware contributed to those numbers.

Spyware is one of the most common threats on the internet. It can easily infect your device and it can be hard to identify. Spyware is a threat to businesses and individual users, since it can steal sensitive information and harm your network.

Check out our guide to help understand how spyware works, how to remove it, and how to help protect yourself or your business.

There are four main types of spyware. Each uses unique tactics to track you.

- **Adware.** This type of spyware tracks your browser history and downloads, with the intent of predicting what products or services you're interested in. The adware will display advertisements for the same or related products or services to entice you to click or make a purchase. Adware is used for marketing purposes and can slow down your computer.
- **Trojan**. This kind of malicious software disguises itself as legitimate software. For example, Trojans may appear to be a Java or Flash Player update upon download. Trojan malware is controlled by third parties. It can

be used to access sensitive information such as Social Security numbers and credit card information.

- **Tracking cookies**. These track the user's web activities, such as searches, history, and downloads, for marketing purposes.
- **System monitors**. This type of spyware can capture just about everything you do on your computer. System monitors can record all keystrokes, emails, chat-room dialogs, websites visited, and programs run. System monitors are often disguised as freeware.

Social Engineering

In the context of information security, social engineering is the psychological manipulation of people into performing actions or divulging confidential information. This differs from social engineering within the social sciences, which does not concern the divulging of confidential information. A type of confidence trick for the purpose of information gathering, fraud, or system access, it differs from a traditional "con" in that it is often one of many steps in a more complex fraud scheme.

It has also been defined as "any act that influences a person to take an action that may or may not be in their best interests."

An example of social engineering is the use of the "forgot password" function on most websites which require login. An improperly-secured password-recovery system can be used to grant a malicious attacker full access to a user's account, while the original user will lose access to the account.

Phishing:

Phishing is the fraudulent attempt to obtain sensitive information or data, such as usernames, passwords and credit card details or other sensitive details, by impersonating oneself as a trustworthy entity in a digital communication. Typically carried out by email spoofing, instant messaging, and text messaging, phishing

often directs users to enter personal information at a fake website which matches the look and feel of the legitimate site,

Phishing is an example of social engineering techniques used to deceive users. Users are lured by communications purporting to be from trusted parties such as social networking websites, auction sites, banks, mails/messages from friends or colleagues/executives, online payment systems or IT administrators.

Attempts to deal with phishing incidents include legislation, user training, public awareness, and technical security measures (the latter being due to phishing attacks frequently exploiting weaknesses in current web security).

Spoofing

Spoofing is a type of scam in which criminals attempt to obtain someone's personal information by pretending to be a legitimate business, a neighbor, or some other innocent party.

Types of Spoofing

Email Spoofing

Sometimes referred to as phishing, this tactic is used by both dishonest advertisers and outright thieves. The spoofer sends out emails with a falsified “From:” line to try to trick victims into believing that the message is from a friend, their bank, or some other legitimate source. Any email that asks for your password, Social Security number, or any other personal information could be a trick.

Text Message Spoofing

Sometimes referred to as smishing, this is similar to email spoofing. The text message may appear to come from a legitimate source, such as your bank. It may

request that you call a certain phone number or click on a link within the message, with the goal of getting you to divulge personal information.

Caller ID Spoofing

Here, the spoofer falsifies the phone number from which they are calling in hope of getting you to take their call. On your caller ID, it might appear that the call is coming from a legitimate business or government agency, such as the Internal Revenue Service. Note that the IRS says it doesn't call taxpayers to tell them they owe taxes without first sending them a bill in the mail.

Neighbor Spoofing

This is a type of caller ID spoofing in which the call will appear to be from someone you know or a person who lives near you. The Federal Communications Commission (FCC) says that the Truth in Caller ID Act prohibits "anyone from transmitting misleading or inaccurate caller ID information with the intent to defraud, cause harm or wrongly obtain anything of value." If they're caught (and that's a big "if"), the spoofer can face penalties of up to $10,000 for each violation.

URL Spoofing

URL spoofing happens when scammers set up a fraudulent website to obtain information from victims or to install malware on their computers. For instance, victims might be directed to a site that looks like it belongs to their bank or credit card company and be asked to log in using their user ID and password. If the person falls for it and actually logs in, the scammer could use the information the victim typed in to log into the real site and access their accounts.

GPS Spoofing

GPS spoofing has a somewhat different purpose. It attempts to trick a GPS receiver into believing it is in a different location or headed in a different direction, by

broadcasting bogus GPS signals or other means. At this point, GPS spoofing is more likely to be used in warfare or by gamers than to target individual consumers, although the technology exists to make anyone vulnerable.

Pharming

Pharming is a scamming practice in which malicious code is installed on a personal computer or server, misdirecting users to fraudulent Web sites without their knowledge or consent. Pharming has been called "phishing without a lure."

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.
- Non 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.

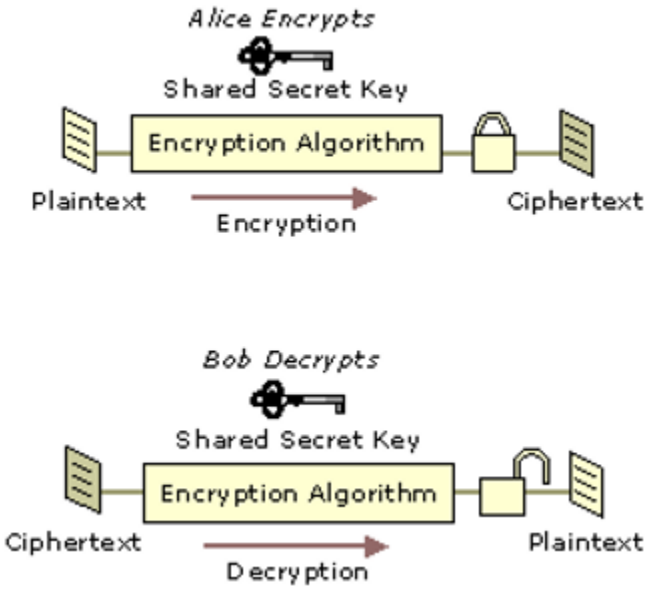

Fig: Encryption and Decryption with a Symmetric Key

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.

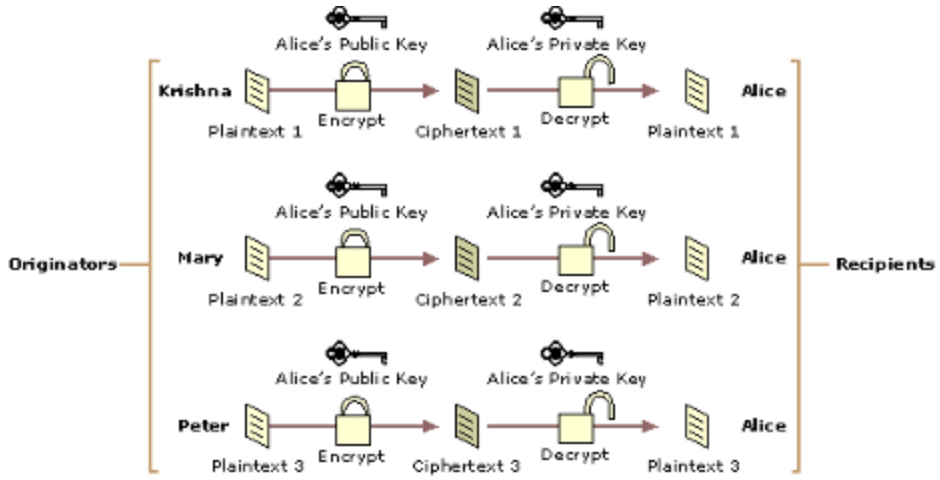

Fig: Encryption and Decryption with Asymmetric Keys

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.

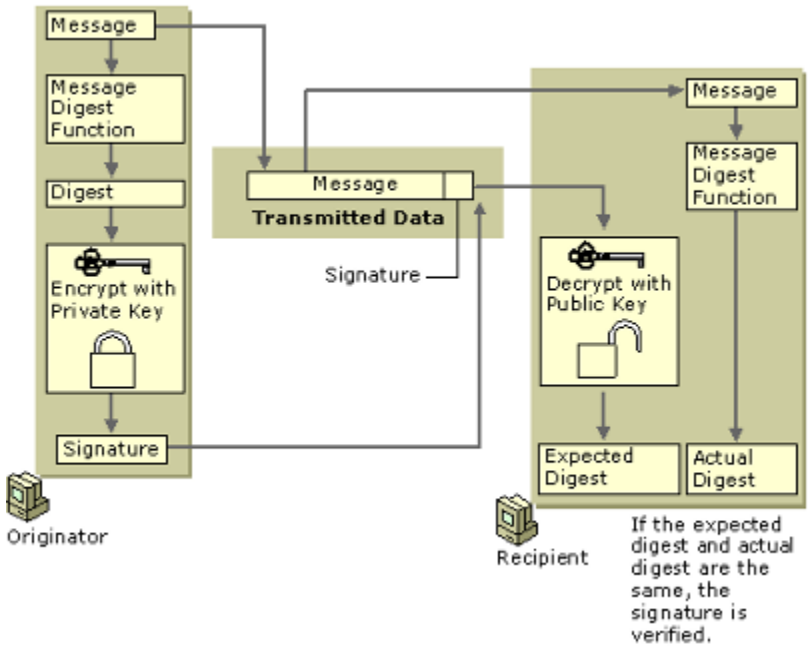

Fig: Basic RSA Data Security Digital Signature Process

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.

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.

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.