Security Threats And Safety Measures

Introduction

With the widespread use of internet, networks and computers have become increasingly susceptible to threats. These threats destroy data as well the programs computer use. The objective of these threats is to destroy the data and to steal the vital information stored in computers. This information is used by the attackers for their benefit. We occasionally hear about the data theft from the credit card companies or banks, which lead to major financial losses. Also sometimes individual users are fooled in to giving their personal and sensitive information such as passwords or bank data leading to financial loss.

VIRUSES

A computer virus is a program usually hidden within another simple program. It produces copies of itself and inserts them into other programs or files, in turn destroying the data and performing other malicious actions. Computer viruses are never naturally occurring; they are always man-made. Once created and released, however, their spread does not remain directly under our control. While developing the viruses, programmers have specific target in mind such as data theft or destruction of software, which runs the computers. The virus can be transferred hidden in files, programs or even in disks. The viruses can be of different kind but a common virus is macro virus.

Macro Viruses

A simple macro is series of programming steps that are stored in a single location. Macro allows automation of many actions with only a single keystroke. These can be embedded in the program files. Many programs, such as Word and excel allow you to record a series of keystrokes and menu selections and then save them to a file. This helps eliminate doing the same action several times increasing efficiency. Macro viruses created with the intention of fooling the user can deceive them in sharing confidential information. This information can be used by the Macro to damage the computer data or software. The virus using macro files are most popular as they are:

- Easy to write.
- Can infect more people faster as they exchange documents and data frequently
- Can easily infect any computer capable of running Office and Internet

Macro viruses can corrupt data, create new files, move text, flash colors, insert pictures, send files across the Internet, and format hard drives. Macro viruses are increasingly used as transport mechanisms to drop off even nastier bugs. Macro viruses modify registries, forward copies of it through emails, look for passwords, copy documents, and infect other programs. Macro viruses can do a lot of different damage in a lot of different ways. Example of macro Virus is Wazzo, W97M etc.

WORMS

- Worms are very similar to viruses in the manner that they are computer programs that replicate copies of themselves (usually to other computer systems via network connections). Viruses often, but not always, contain some functionality that will interfere with the normal use of a computer or a program. Unlike viruses, however, worms exist as separate entities; they do not attach themselves to other files or programs. Because of their similarity to viruses, worms are also often referred to as viruses. Some examples of the worst Worms that impacted the web are as follows:
- 1. Jerusalem is one of the earliest worms that spread in 1987. It is also one of the most commonly known viruses. It used to delete files that were executed on each Friday the 13th. It was first detected in the city of Jerusalem.
- 2. In 1991, thousands of machines running MS-DOS were hit by a new worm, Michelangelo. The virus would overwrite the hard disk or change the master boot record of infected hosts.
- 3. In 2007 Storm Worm hit the computers. Once hit, your machine becomes part of a large botnet which performs automated tasks that range from gathering data on the host machine, to sending infected emails to others. About 1.2 billion emails were sent from the infected computers propagating infection.
- Since Worms spread mostly through the email attachments, the best ways to avoid them is using caution in opening emails. If the email is from an unidentified source, it is always best to delete it. Most of the time worms attach themselves to email. Even the sender of email does not recognize what they have forwarded, as emails are sent automatically using all contact information in the user's profile.

TROJAN HORSES

- A Trojan horse is a program that claims to rid your computer of viruses but instead introduces viruses into the system. Since they look like sincere programs they are referred as Trojan like the Trojan horse of Greek mythology. The Trojan program does not attach itself to the files like a virus nor replicate itself like a worm but it does provide unauthorized access to user's computer.
- They are mostly spread through internet downloads and online gaming programs. They mostly affect the targeted computers. The trojan program prompts you to do the normal functions such as inputting your email address or profile name. You do so, not knowing that, you have provided access to the malicious software. This software is capable of taking over the functionality of your computer. An infected computer will begin to operate slowly and will exhibit pop-ups from time to time. Eventually the computer will cease to operate, or crash.
- The best way to avoid the Trojans is to adopt safe download practices. If you are not sure of the website safety, then it is probably best not to download any program from that source.
- An example of the Trojan horse was "I love you" which infected several computers in USA and Asia, completely damaging the data of millions of computers.

SPYWARE

- A Spyware as the name suggest is a program used to spy on the computer system. This program will try to get all the confidential and sensitive information such as your bank account numbers, passwords etc. Then this confidential data is misused to access user's accounts. Spyware can also change the configuration of your computer, generally without obtaining your consent first.
- There are a number of ways Spyware or other unwanted software can get on to computer. A common trick is to covertly install the software during the installation of other software that is being downloaded such as music or video or a file-sharing program.
- Once installed, the Spyware monitors user activity on the Internet and transmits that information in the background to someone else. Spyware can also gather information about e-mail addresses and even passwords and credit card numbers.
- Spyware sends information back to the spy ware's home base via the user's Internet connection, thus it eats user's internet bandwidth. Spyware applications running in the background can lead to system crashes or general system instability as they use memory and system resources of the user's computer.
- Spyware have the ability to monitor keystrokes, scan files on the hard drive, snoop other applications, such as chat programs or word processors. It also installs other Spyware programs, read cookies, change the default home page on the Web browser. While doing so, it consistently relays this information back to the Spyware author who will either sell the information to another party or use it for advertising/marketing purposes.
- Some of the common Spywares are CoolWebSearch, Internet optimizer and Zango.

MALWARE

Malware is short for "malicious software." Malware is any kind of unwanted software that is installed without your adequate consent. The intent of the malware is to damage the data or functionality of the computer or network. In fact all the threats mentioned above such as virus, Trojans etc are examples of Malware.

SPAMS

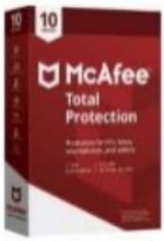
- The term "spam" refers to unsolicited commercial email (UCE) or unsolicited bulk email (UBE). It is flooding the Internet with many copies of the same message, in an attempt to force the message on people who would not otherwise choose to receive it. It is also referred as junk email. Unsolicited email mostly contains advertisements for services or products. However most of the spams are from marketers or user who are trying to deceive the users. The most commonly seen spam includes the following:
- ❖ Phishing scams, a very popular and dangerous form of email fraud ❖ Foreign bank scams or advance fee fraud schemes ❖ Other "Get Rich Quick" or "Make Money Fast" (MMF) schemes ❖ Quack health products and remedies Spam emails is not only unwanted, it clogs your email accounts and uses unnecessary server space. This creates burden on servers in the businesses. Since Internet is a public platform, it is never possible to completely stop the Spam email. However precaution can be taken while looking at an unknown email addresses. Most of the email hosts can identify such users and help filter them. Spam costs the sender very little to send -- most of the costs are paid for by the recipient or the carriers rather than by the sender. It is because of these additional costs that most of the hosts are very keen that users use spam filters as well as report spams so they can be stopped.

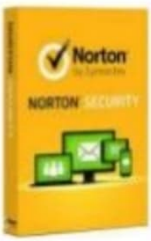
HACKERS AND CRACKERS

Hackers and crackers are the software programmers who use dubious ways to get control over your computer and systems. The intent of both hackers and crackers is to gain control over your computer so that they can get the sensitive confidential information. They then use this information against you by stealing money, personal data, pictures, bank details and government military information, so on and so forth. This information can either be sold for money or hackers access account themselves to rob you directly. Originally hackers were the gifted programmers who gain access to the systems or network to show case the security loopholes to the administrators. Later the term cracker was coined for such activist who had intentions of doing malicious activities. Crackers have an end goal of destroying data and network for personal monetary gains.

ANTIVIRUS TOOLS

Anti Virus tools are the software programs that help us detect the virus in emails or files and hence protect our computers. These tools can detect virus, worms, Trojans as well as spyware and adware. They block us from visiting unsafe websites, and also downloading unsafe programs from such websites. They protect us from identity thefts and threats from phishing websites. There are several commercial antivirus softwares available such as Norton, Mcafee, K7, Quickheal etc.





DATA BACKUP AND SECURITY

As we discussed earlier, there are threats to the computers that are sometimes hard to avoid. Unknowingly we may open an email that may have virus attachments and can destroy all the program and data on our computer. That is why to protect ourselves from such unknown threat; we need to assure backing up the data. The basic principal on data back up is very simple, just make another copy of the data and keep it elsewhere than on the same computer. This guarantees that once the data on your computer gets corrupted due to a threat, you can reload the data again on your computer once it has been rectified. These days you have external hard drives which can back up data. Also most of the smart devices are also used to back up the data. Before we discuss in detail how to use the security tools, here are some of the guiding principles to use the computers securely.

1. Using Security software such as Norton antivirus, Symantec etc.
2. Never share passwords
3. Beware of email attachments form unknown sources
4. Do not randomly download material from websites which has not been checked for security
5. Never propagate hoax or chain emails
6. Always logout your laptop or computer
7. Restrict remote access
8. Frequently back up important data and files
9. Use encryption or sites that use encrypted data

There are several security tools available which help us protect against all sorts of threats mentioned above. In brief, the tools are available for antispam, antivirus, firewalls, encryption tools, password managers and cleanup tools.

CYBER CRIMES

FIRST RECORDED COMPUTER CRIME

In 1820, Joseph-Marie Jacquard, a textile manufacturer in France, produced the loom. This device allowed the repetition of a series of steps in the weaving of special fabrics. This resulted in a fear amongst Jacquard's employees that their traditional employment and livelihood were being threatened. They committed acts of sabotage to discourage Jacquard from further use of the new technology. This is the first recorded cyber crime!

CURRENT THREATS

Top 10 E-commerce Security Threats

1. Financial frauds

Ever since the first online businesses entered the world of the internet, financial fraudsters have been giving businesses a headache. There are various kinds of Financial frauds prevalent in the e-commerce industry, but we are going to discuss the two most common of them.

a. Credit Card Fraud

It happens when a cybercriminal uses stolen credit card data to buy products on your e-commerce store. Usually, in such cases, the shipping and billing addresses vary. You can detect and curb such activities on your store by installing an AVS – Address Verification System.

Another form of credit card fraud is when the fraudster steals your personal details and identity to enable them to get a credit card.

b. Fake Return & Refund Fraud

The bad players perform unauthorized transactions and clear the trail, causing businesses great losses. Some hackers also engage in refund frauds, where they file fake requests for returns.

2. Phishing

Several e-commerce shops have received reports of their customers receiving messages or emails from hackers masquerading to be the legitimate store owners. Such fraudsters present fake copies of your website pages or another reputable website to trick the users into believing them. For example, see this image below. A seemingly harmless and authentic email from PayPal asking to provide details.

3. Spamming

Some bad players can send infected links via email or social media inboxes. They can also leave these links in their comments or messages on blog posts and contact forms. Once you click on such links, they will direct you to their spam websites, where you may end up a victim.

4. DOS & DDoS Attacks

Many e-commerce websites have incurred losses due to disruptions in their website and overall sales because of DDoS (Distributed Denial of Service) attacks. What happens is that your servers receive a deluge of requests from many untraceable IP addresses causing it to crash.

5. Malware

Hackers may design a malicious software and install on your IT and computer systems without your knowledge. These malicious programs include spyware, viruses, Trojan horses, and ransomware.

The systems of your customers, admins, and other users might have Trojan Horses downloaded on them. These programs can easily swipe any sensitive data that might be present on the infected systems and may also infect your website.

6. Exploitation of Known Vulnerabilities

Attackers are on the lookout for certain vulnerabilities that might be existing in an e-commerce store. Often an e-commerce store is vulnerable to SQL injection and Cross-site Scripting (XSS). Let's take a quick look at these vulnerabilities:

a. SQL Injection

It is a malicious technique where a hacker attacks your query submission forms to access your database. They corrupt your database with an infectious code, collect data, and later wipe the trail.

7. Bots

Some attackers develop special bots that can scrape your website to get information about inventory and prices. Such hackers, usually your competitors, can then use the data to lower the prices in their websites in an attempt to lower your sales and revenue.

8. Brute force

The online environment also has players who can use brute force to attack your admin panel and crack your password. These fraudulent programs connect to your website and try out thousands of combinations in an attempt to obtain the password. Always ensure to use strong, complex passwords that are hard to guess. Additionally, always change your passwords frequently.

9. Man in The Middle

A hacker may listen in on the communication taking place between your e-commerce store and a user. Walgreens Pharmacy Store experienced such an incident. If the user is connected to a vulnerable Wi-Fi or network, such attackers can take advantage of that.

8. Brute force

The online environment also has players who can use brute force to attack your admin panel and crack your password. These fraudulent programs connect to your website and try out thousands of combinations in an attempt to obtain the password. Always ensure to use strong, complex passwords that are hard to guess. Additionally, always change your passwords frequently.

9. Man in The Middle

A hacker may listen in on the communication taking place between your e-commerce store and a user. Walgreens Pharmacy Store experienced such an incident. If the user is connected to a vulnerable Wi-Fi or network, such attackers can take advantage of that.

10. e-Skimming

E-skimming involves infecting a website's checkout pages with malicious software. The intention is to steal the clients' personal and payment details.

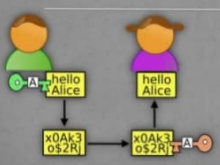
Are you an e-commerce business person? Don't downplay the seriousness of these e-commerce security threats.

Cryptography

Definition:

1. Cryptography is associated with the process of converting ordinary plain text into unintelligible text and vice-versa.
2. It is a method of storing and transmitting data in a particular form so that only those for whom it is intended can read and process it.
3. Cryptography not only protects data from theft or alteration, but can also be used for user authentication.

CRYPTOGRAPHY



CONTENTS

- SECURITY
- SECURITY THREATS
- SECURITY GOALS
- WHAT IS CRYPTOGRAPHY
- BASIC TERMS
- ENCRYPTION & DECRYPTION
- CATEGORIES OF CYRPTOGRAPHY
- COMPARISON
- CONCLUSION

WHAT DOES SECURE MEAN?

SECURITY???

THREATS

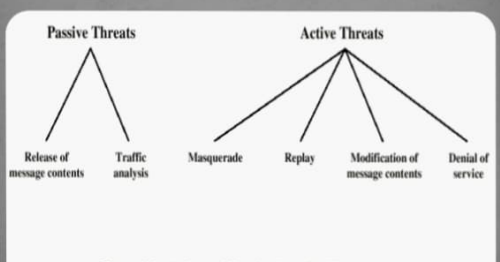
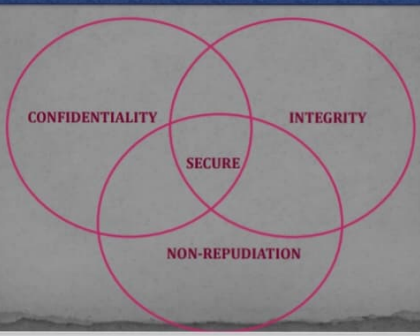


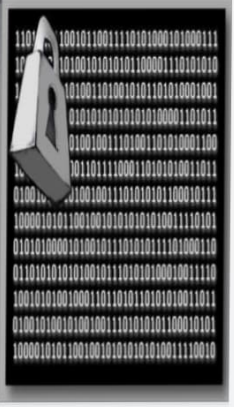
Figure 1.2 Active and Passive Security Threats

SECURITY GOALS



CRYPTOGRAPHY

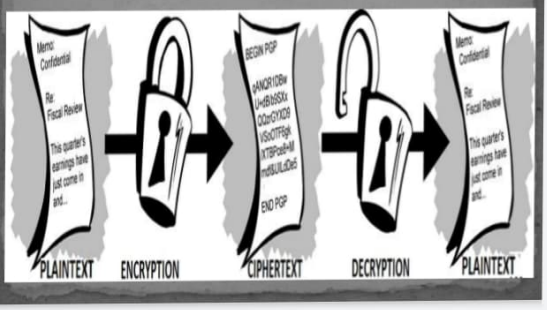
- Cryptography is the science and art of transforming messages to make them secure and immune to attack.



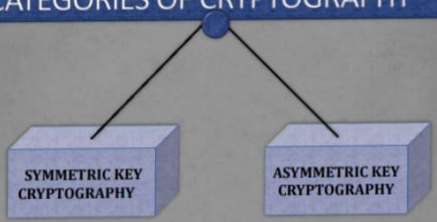
BASIC TERMS

- PLAIN TEXT
- CIPHER TEXT
- CIPHER
- ENCRYPTION & DECRYPTION
- KEYS

ENCRYPATION & DECRYPTION



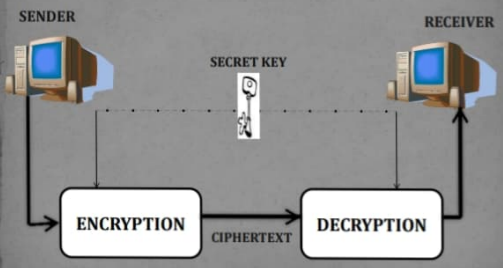
CATEGORIES OF CRYPTOGRAPHY

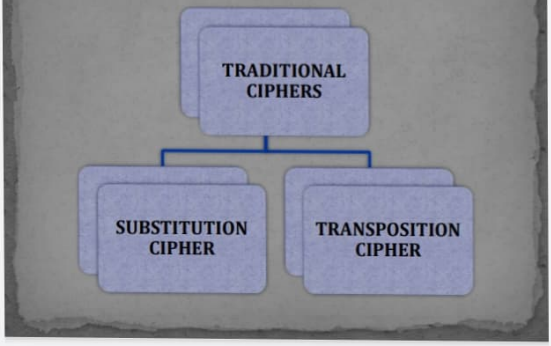


SYMMETRIC KEY CRYPTOGRAPHY

- Also known as secret key. Sender & receiver uses same key & an encryption/decryption algorithm to encrypt/decrypt data. i.e. the key is shared.

SYMMETRIC KEY CRYPTOGRAPHY





SUBSTITUTION CIPHERS

- A substitution technique is one in which the letters/number/symbols of plaintext are replaced by other letters/numbers/symbols.

e.g. A ⟶ D, T ⟶ Z
2 ⟶ 5, 3 ⟶ 6

TRANSPOSITION CIPHER

- In the transposition technique the positions of letters/numbers/symbols in plaintext is changed with one another.

1	2	3	4	5	6
M	E	E	T	M	E
A	F	T	E	R	P
A	R	T	Y		

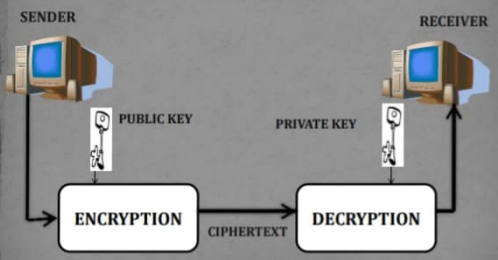
4	2	1	6	3	5
T	E	M	E	E	M
E	F	A	P	T	R
Y	R	A		T	

- Plain text: MEET ME AFTER PARTY
- Cipher text: TEMEEMEFAPTRYRAT
- KEY USED: 421635

ASYMMETRIC KEY CRYPTOGRAPHY

- Also known as public key cryptography. Sender & receiver uses different keys for encryption & decryption namely PUBLIC & PRIVATE respectively.

ASYMMETRIC KEY CRYPTOGRAPHY



KEYS USED IN CRYPTOGRAPHY

SYMMETRIC KEY CRYPTOGRAPHY

ASYMMETRIC KEY CRYPTOGRAPHY

COMPARISON

SYMMETRIC KEY CRYPTOGRAPHY	ASYMMETRIC KEY CRYPTOGRAPHY
1) The same algorithm with the same key is used for encryption and decryption.	1) One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption.
2) The key must be kept secret.	2) One of the two keys must be kept secret.
3) It may be impossible or at least impractical to decipher a message if no other information is available.	3) It may be impossible or at least impractical to decipher a message if no other information is available.

APPLICATIONS

- Defense services
- Secure data manipulation
- E –commerce
- Business transactions
- Internet payment systems
- User identification systems
- Access control
- Data security

CONCLUSION

- By using of encryption techniques a fair unit of confidentiality, authentication, integrity, access control and availability of data is maintained.

Overview

- Cryptography
- History of cryptography
- Classical cryptography
- Modern cryptography
- Types
  - Symmetric cryptography
  - Asymmetric cryptography
- Pigpen cipher
- Application
- Conclusion

Cryptography

- **Cryptography** Greek: *kryptós* "hidden, secret" ; and *graphein*, "to write".
- It is the practice and study of techniques for secure communication in the presence of third parties called adversaries.
- Constructing and analyzing protocols that prevent third parties or the public from reading private messages; various aspects in information security such as data confidentiality, data integrity, authentication, and non-repudiation are central to modern cryptography.

History of cryptography

- There are three eras in the history of cryptography:
  - Manual era
  - Mechanical era
  - Modern era
- Manual era refers to Pen and paper Cryptography and dates back to 2000 B.C. eg: Scytale, Atbash, Caesar and Vigenere.
- Mechanical era refers to the invention of cipher machines. Eg: Japanese Red and purple machines, German Enigma.modern era of cryptography refers to computers.
- There are infinity permutations of cryptography available using computers. Eg: Lucifer, Rijndael, RSA, ElGamal

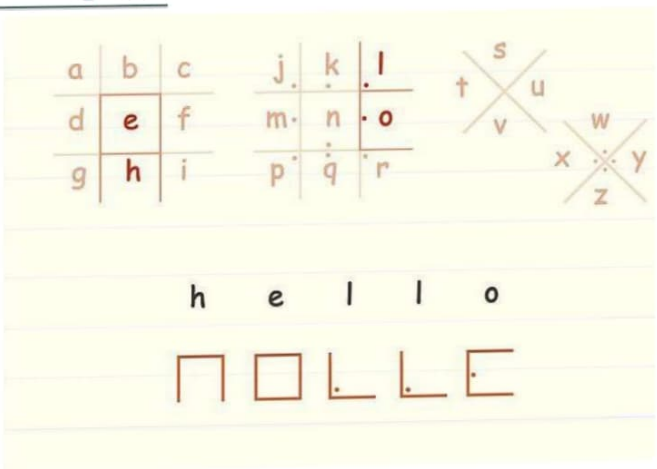
Classic cryptography

- The main classical cipher types are transposition ciphers, which rearrange the order of letters in a message and substitution ciphers, which symmetrically replace letters with other letters.

- Example: 'hello world' becomes 'ehlol owrld' in a trivially simple rearrangement scheme.

A **cipher** (or **cypher**) is an algorithm for performing encryption or decryption- a series of well-defined steps that can be followed as a procedure.

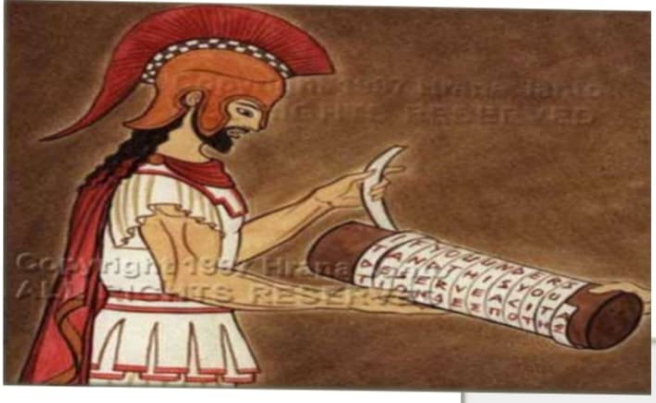
Pigpen cipher



- An early substitution cipher was the Caesar cipher, in which each letter in the plain text was reported by a letter some fixed number of positions further down the alphabet.

- Suetonius reported that Julius Caesar used it with a shift of three to communicate with his generals.

Reconstructed ancient Greek scytale
an early cipher device



Modern cryptography or computer era

- The development of digital computer and electronics after world war II made possible much more complex ciphers.
- Futhermore, computers allowed for the encryption of any kind of data represent able in any binary format, unlike classical ciphers which only encrypted written language text: this was new and significant.

German Lorenz cipher machine,
used in world war II to encrypt very-high-level general staff messages

- Todays fine example of cryptography is

Credit card with smart-card capabilities.3-5mm chip embedded in the card.

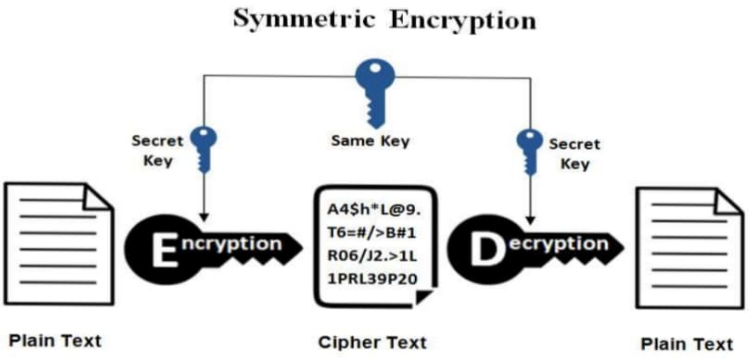
The basic elements of cryptography are:

1. Encryption
2. Decryption
3. Key

The modern field of cryptography can be divided into several areas of study:

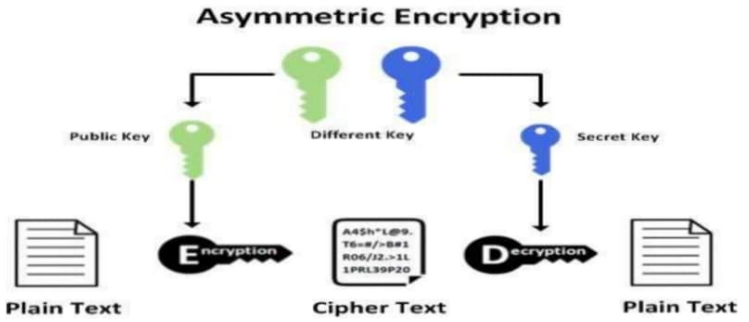
Symmetric key cryptography:

It refers to encryption methods in which both the sender and receiver share the same key.



Asymmetric or Public key cryptography:

It refers to encryption methods in which both the sender and receiver share the different keys.



Application of Cryptography

- Defense services
- Secure data manipulation
- E-commerce
- Internet payment systems
- Data security
- ATM
- E-mail
- Secure remote access
- ISDN
- PEM
- PGD
- Smart Cards

Public Key Infrastructure

A Public Key Infrastructure (PKI) is used to manage and distribute keys and digital certificates in publicly accessible networks to ensure secure digital communications. The exchange of data, information and messages via the Internet takes place in a PKI through a key pair consisting of a public key and a private key. The keys are linked by a mathematical function so that data which is encrypted with the public key can only be decrypted with the private key (one-way.) If a sender and a recipient want to exchange sensitive data, various parts of the PKI handle the verification checks of the transmitted data (integrity) and authentication of the communication participants using the key pair (authentication).

The public-key infrastructure issues certificates, passes them on to the communication participants and checks the certificates for authenticity. With this multi-stage check, sender and recipient are authenticated and the data to be transmitted is subjected to an integrity test. Public Key Infrastructures are a combination of symmetric and asymmetric encryption methods that work with two different keys to solve the key exchange problem in cryptography, using an information technology infrastructure and a certification authority that digitally signs data and keys in an automated process. The standard protocol on the Internet is called PKIX (Public Key Infrastructure Exchange). Other similar approaches exist, such as Let's encrypt or

Contents

[hide]

General information

The secure transmission of messages between senders and receivers was an important issue with the development of the Internet, which also attracted the attention of the tech-savvy public. The importance of data protection and privacy has grown rapidly with the technological development, especially in e-commerce, B2B commerce, and later also in online banking. The focus was not only on the encryption of data, but also on the threat of communication participants who were able to interfere with the transmission of data using computer-assisted methods, for example, to crack passwords, copy customer data or paralyze whole systems.

While transmitted data has been encrypted with symmetrical methods since the 1950s, the need for a review of the communication participants has become evident. A one-to-one communication between government agencies can be relatively easily protected if the key is kept secret, but one-to-many communication on the World Wide Web requires key distribution and management, because of the quantity of participants. To test the actual identities of transmitters and receivers, new asymmetric as well as hybrid methods were invented and tested. One of the best-known methods still used today is the RSA cryptosystem, which was released in 1977.[1]

The concepts of public-key infrastructure and public key encryption encompass various approaches which have developed partly in parallel over the past fifty years and built on one another. Some examples of PKIs or similar infrastructures and security protocols:

- SSL/TLS
- HTTPS
- IPsec
- PGP/OpenPGP
- S/MIME

How a public key infrastructure works

Public key infrastructures are characterized in particular by a trusted third party which is responsible for the confidentiality of transmitted messages. This party is called certification authority (CA) in a PKI. It is the hub for managing certificates and can itself be certified, for example, by Internet users (Web of Trust), ISPs, or an Internet Engineering Task Force (IETF).

The most important components of a public key infrastructure:

- Certification authority (CA): The CA is held by the key pair, including the secret key. Both keys have a mathematical relationship to one another, for example via a cryptographic hash function. The CA records each digital certificate using the secret key before verifying or issuing it to persons or companies. The persons or companies do not know the secret key, only the public key is known to them.
- Registration authority (RA): The RA is responsible for the registration of persons and companies. It allows the use of digital certificates for specific applications and also checks the certificates before they are issued by the CA.
- Directory and time stamp service: All certificates and their public keys are stored here. Anyone

- Directory and time stamp service: All certificates and their public keys are stored here. Anyone can search this service for certificates to check if the certificates of certain people or companies are genuine, similar to a whitelist. In real-time, the certificates can also be checked for their validity in time in order to exclude expired certificates.
- Certificate Revocation List (CRL): The CRL generates lists of invalid and rejected certificates whose keys are no longer secure. If the identity of the sender or recipient is not clear, certificates can be rejected. In such cases, the certificate is initially blocked and checked before it is permanently revoked. The CRL is a blacklist for certificates and associated digital signatures.
- X.509 certificates: The digital certificates in the PKI system are called X.509 certificates and are standardized. The authentication of a key is always bound to a sender or recipient, such as an email address or a domain name (DNS). Confidentiality is supposed to be guaranteed through the hierarchical structure of the certification. X.509 certificates contain various data concerning the cryptological hash function, which concerns the encryption of the public key and the validity of the digital signatures. In the latest version, X.509v3, extensions can also be implemented for specific applications.

If a message is to be encrypted and sent, the sender uses the recipient's public key. The sender signs this message and uses his private key for the digital signature. The receiver decrypts the message again with his private key. The supplied signature is also decrypted. The public key of the sender can be used for this purpose. Thanks to the separate transmission of the digital signature, the recipient can authenticate the sender and, thanks to the private key of the receiver, he can only read the message in the plaintext. The provision of the

Relevance for programming

PKI systems are, in principle, one of the safest methods of digital data transmission. However, the current state of these types of encryption methods and procedures for verifying integrity and authenticity is unclear. Depending on the application, different systems are in use and the variety of providers makes public key encryption sometimes unworkable for the end user. This is because the sender and the recipient have to define a procedure which can be problematic in large, distributed networks such as the World Wide Web.

The result is that there are currently different types of trust models in digital communication, none of which have yet been implemented. The following approaches should be mentioned:

- Strict hierarchy: A higher-level instance is responsible for the root certificates. X.509v3 works with this model.
- Loose hierarchy: Multiple instances are responsible for distributing certificates. The chain of certificates can be arranged differently, but it must not be too complex.
- Hub and spoke: If individual certification bodies want to authenticate each other, a bridge authority is used, which regulates the exchange between certificate users and issues with equal authorization.
- Web of Trust: Trust in the form of certificates or digital signatures is the task of end users in the Web of Trust. OpenPGP is based on this principle.

Authentication vs. Authorization

While often used interchangeably, authentication and authorization represent fundamentally different functions. In this article, we compare and contrast the two to show how they protect applications in complementary ways.

What are authentication and authorization?

In simple terms, authentication is the process of verifying who a user is, while authorization is the process of verifying what they have access to.

Comparing these processes to a real-world example, when you go through security in an airport, you show your ID to authenticate your identity. Then, when you arrive at the gate, you present your boarding pass to the flight attendant, so they can authorize you to board your flight and allow access to the plane.

Authentication vs. Authorization

Here's a quick overview of the differences between authentication and authorization:

Authentication	Authorization
Determines whether users are who they claim to be	Determines what users can and cannot access
Challenges the user to validate credentials (for example, through passwords, answers to security questions, or facial recognition)	Verifies whether access is allowed through policies and rules
Usually done before authorization	Usually done after successful authentication
Generally, transmits info through an ID Token	Generally, transmits info through an Access Token
Generally governed by the OpenID Connect (OIDC) protocol	Generally governed by the OAuth 2.0 framework
Example: Employees in a company are required to authenticate through the network before accessing their company email	Example: After an employee successfully authenticates, the system determines what information the employees are allowed to access

Mobile Code Security

Improve the Security of Your Mobile Applications

Increasing smartphone adoption rates coupled with the resultant rapid growth in smartphone applications have created a scenario wherein private and sensitive information is being pushed to the new device perimeter at an alarming rate. Given the rapid pace of development in the industry, the security of the application software used is becoming more and more important.

There are three main categories of mobile code security risks: malicious applications, vulnerabilities in legitimate applications, and social engineering.

Malicious Applications

Malicious applications are those that are created with the specific intent of violating the confidentiality, integrity, or ability of a user's device or data. Malicious applications can take various forms. The most common type is spyware, such as spy pixels in email attachments or Trojans, which consist of malicious code embedded in an otherwise legitimate vehicle. Users who install Trojans believe that they are installing a game or a utility app, but instead, they download hidden spyware, phishing UIs, or unauthorized premium dialing.

The following are common attack patterns performed by mobile applications:

1. Activity monitoring and data retrieval
2. Unauthorized dialing, SMS, and payments
3. Unauthorized network connectivity (exfiltration or command and control)
4. UI impersonation
5. System modification (rootkit, APN proxy config)
6. Logic or time bomb

Vulnerabilities in Legitimate Applications

The category of mobile security vulnerabilities consists of design or implementation flaws that allow for the infiltration and execution of malicious code (exploits) in otherwise legitimate applications, often without the knowledge of the legitimate parties involved.

Common vulnerability categories include:

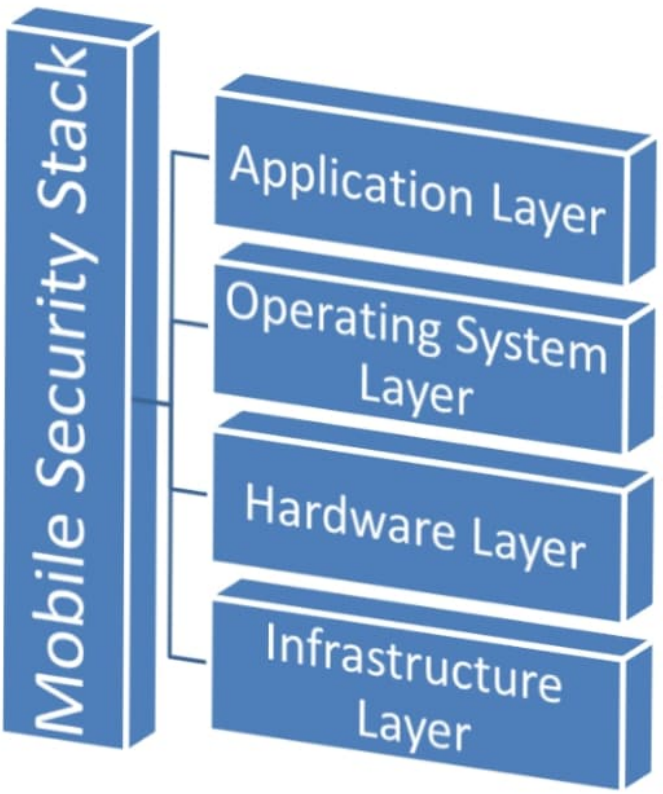
1. Sensitive data leakage (inadvertent or side channel)
2. Unsafe sensitive data storage
3. Unsafe sensitive data transmission
4. Hardcoded password/keys
5. Outdated hashing algorithms
6. Cookie theft
7. Exposure to buffer overflows
8. Storage of sensitive information in version control systems such as GitHub

Social Engineering

Even in those applications that adhere to industry standards and best practices in all matters of security, there is always a risk that the user will be tricked into willingly revealing sensitive information to an attacker, especially in mobile applications that handle highly sensitive or valuable data such as banking or health care.

Common social engineering techniques include:

1. Phishing or spear-phishing
2. Impersonation



How to Test for Mobile Code Security

When analyzing an individual device for security implications, take into account each of the layers of the mobile code security stack to determine the effectiveness of the security mechanisms that are in place. For each layer, determine what, if any, security mechanisms and mitigations the manufacturer has implemented and whether those mechanisms are sufficient for the type of data you plan to store and access on the device. The threat analysis must be repeated under different threat models (i.e., what parts of the system are compromised by the attacker).

Vulnerabilities may occur at various points in the application's lifecycle. Vulnerabilities that occur during the development stage may be addressed by unit testing and code linting. For vulnerabilities that occur during the end of the development sprint, you must conduct a pull test review. For vulnerabilities occurring during the application lifecycle, a code review/audit is in order. Finally, after application development, you may deal with vulnerabilities that occur via penetration testing.

2. MOBILE AGENT-BASED E-COMMERCE

2.1 Mobile Agent Introduction

The Object Management Group defines a software agent as "a computer program that acts autonomously on behalf of a person or organization" [1]. The following properties characterize agents:

- pro-active (support of the user's work)
- adaptive (learning the user's preferences or the ability to work on different platforms)
- autonomous (limited communication with its creator)
- intelligent (making 'intelligent' decisions)
- mobile (can actively migrate in networks to different systems and move directly to the local resources, like databases or application servers)

Mobile agents are programs that can migrate from host to host in a network, at times and to places of their own choosing. The state of the running program is saved, transported to the new host, and restored, allowing the program to continue where it left off. Lange and Oshima [2] give reasons why to use agents: e.g. improvements in latency and bandwidth of client-server applications and reducing vulnerability to network disconnection.

2.2 Mobile Agents in E-Commerce

Mobile agents are well suited for electronic commerce. A commercial transaction may require real-time access to remote resources such as stock quotes and perhaps even agent-to-agent negotiation. Different agents will have different goals, and will implement and exercise different strategies to accomplish these goals. We envision agents that embody the intentions of their

creators, and act and negotiate on their behalf. Mobile agent technology is a very appealing solution to this kind of problem.

An electronic commerce transaction may be viewed in terms of four different phases [3]: product brokering, merchant brokering, negotiation, payment and delivery.

Product brokering consists in the gathering of information about the product that is going to be bought.

Merchant brokering involves the evaluation of a set of alternatives in order to make the purchase. Making the decision implies considering all the tradeoffs that the various products offer: price, warranties, delivery time, and others.

During the negotiation phase the agent settles the final terms of the commercial transaction. The characteristics of the market directly influence the outline of this phase. In markets where prices and characteristics are fixed, negotiation may not even exist.

Finally, in the purchase and delivery phase of the transaction, the agent actually makes the acquisition and delivers the money (or its electronic equivalent) against the goods.

2.2.1 Secure Mobile Agent System

A number of advantages of using mobile code and mobile agent computing paradigms have been proposed [4, 5, 6]. One of the main obstacles to the widespread adoption of mobile agents is the legitimate security concern of system developers, network administrators, and information officers. It has been argued that once the security issues have been resolved and a collection of security mechanisms have been developed to counter the associated risks, then the users of mobile agent technology will be free to develop useful and innovative solutions to existing problems and find a wide array of application areas that will benefit from this technology. Using this collection of security mechanisms to mitigate agent-to-agent, agent-to-platform, and platform-to-agent security risks may, however, introduce performance constraints that could dictate design decisions or negate the benefit of using mobile agents for certain applications. Considering the special security requirements in e-commerce, a secure mobile agent system (SMAS) framework is presented in this paper.

SMAS consists of mobile agents and agent server (e.g. agent facilitator). Mobile agent has six modules: security shell, environment interaction module, state denotation module, task execution module, routing policy module and log file. The architecture of mobile agent is shown in figure 1.

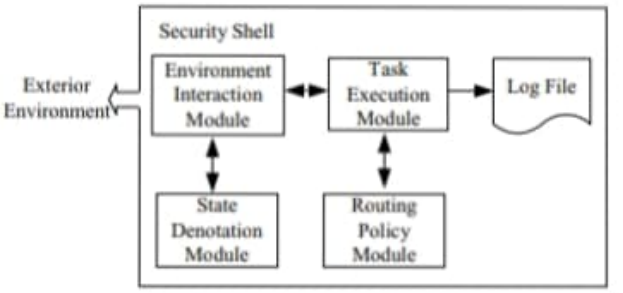


Figure 1 Mobile Agent Architecture Model

Security shell is responsible for protecting the agent from attacks of malicious hosts and other agents. The main functions include encrypting and decrypting the whole agent, authorizing the visit host, deploying the different security policy according to the different trusted level of host.

Environment interaction module is responsible for the maintenance of communication between agent and exterior environment that includes sensor (apperceive outside environment), message processor (process inter-messages, data communication between agent and environment based on KQML) and reactor (i.e. effector, output the result to outside environment).

Task execution module is the execution module of agent, which consists of action execution module and result integration module. According to the security strategy to different methods and data deployed by security shell, task execution module executes corresponding method, and makes integrated analysis of results for its goal.

State denotation module is responsible for recording the state of agent, which includes attribute value of agent and the sequence of agent's running environment. This makes agent to run successfully when it is hold up or resumed. Agent's state can also be recorded in fixed interval for its resuming in abnormal circumstance.

Routing policy module plans agent's migration route. There are two feasible routing policies, one is fixed routing, and the other is dynamic routing based on formula and catalog services.

Log file records every sensitive instruction and manipulation on agent executed by agent platform, it's used for audit afterwards. Log file must be encrypted so that it couldn't be juggled.

Mobile agent server (mobile agent service facilitator) is based on agent transfer protocol (ATP), it provides essential EE(execution environment) for agent's migration, execution, and other functions and services such as dispatch, reception, recovery, security management and service transfer. Mobile agent server includes security management, agent executing environment, agent API, agent service environment, communicating API, as shown in figure 2.

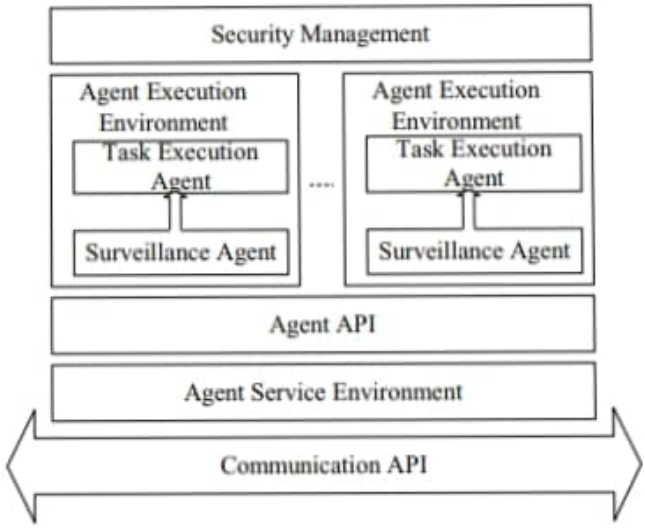


Figure 2 Mobile Agent Server Structure

Security management is responsible for the security of agent server and the agent executing on it, it takes authentication, encryption, visit controlling and other measures to protect system security.

Every agent server can process several agent EEs. Agent EE is the resource distributed for every agent by the agent server. It runs agent under the control of security management module. Every EE has two kinds of agents: task execution agent and surveillance agent. Task execution agent runs the program on behalf of agent user. Surveillance agent keeps an eye on the execution situation of the task agent. It can terminate the task agent once there is any unauthorized or illegal operation.

Agent API is the unique interface between agent and agent server. It provides many characteristic operations of mobile agent that can be utilized to finish the distributed task for the agent. For instance, agent calls Jump procedure explicitly before migrating to another host. Jump procedure captures the whole state image of the mobile agent and transfers the agent to the destination host. On the destination host, agent server loads the agent to the relevant agent EE and recoveries the agent from the hold point. The primary agent will be terminated on the local host after the agent's state image being captured, transferred and recovered successfully on the destination host.

Agent service environment manages lifecycle, event and persistence for agent. Lifecycle management realizes creation, dispatch, migration, reception, storage and termination for mobile agent, event service provides agent communication mechanism for collaboration with other agents or application system, which supplies essential condition for agent collaboration. Persistence service ensures agent execution's persistence through corresponding mechanism, it helps agent to restart accurately when there is system or network disaster before agent reach its destination.

Communication API is responsible for transmitting mobile agents, data and messages, including network protocol API and email API.

2.2.2 Mobile Agent-based E-Commerce

Based on above construction of mobile agent system, this paper brings forth the mobile agent-based e-commerce system framework. Its model is shown in figure 3.

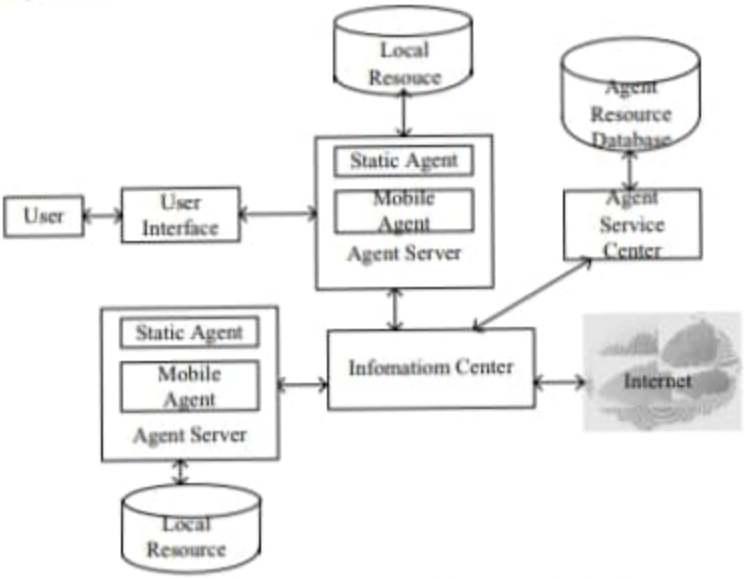


Figure 3 Mobile Agent-Based E-Commerce System Framework

In this system, agent service center provides catalog service, registers mobile agent's basic information, maintains agent's lifecycle, cancels illegal agent in time and provides agent query service. In order to enforce system security, especially for mobile agent protection, agent service center also maintains a table which records the history of host visitation, it gets task accomplish information of agent in visitation from its log files, calculates the host's credit degree, puts the result in the history table and re-calculates it so that mobile agent could optimizes routing strategy. Service center need to provide host service query function in order to help agent affirm the servers on which its task could be accomplished, and choose the best route.

Information center is responsible for security control of the whole E-Commerce system, it generates certain inbreak inspection agents, sends them to each sub-system, monitors real time condition of system execution, collects relative information of inbreak event, analyzes inbreak event, traces inbreak route and confirms its beginning. Control center takes corresponding measure when it received inbreak report and analyzed it. Control center is also responsible for downloading patches of application and operation system, upgrading virus-preventing software, after this it dispatches mobile agent to install them on every node in the system.

3.4.4. SECURE ELECTRONIC TRANSACTION OR SET:

Secure Electronic Transaction or SET is a system which ensures security and integrity of electronic transactions done using credit cards in a scenario. SET is not some system that enables payment but it is a security protocol applied on those payments. It uses different encryption and hashing techniques to secure payments over internet done through credit cards. SET protocol was supported in development by major organizations like Visa, Mastercard, Microsoft which provided its Secure Transaction Technology (STT) and NetScape which provided technology of Secure Socket Layer (SSL).

3.4.5. SET PROTOCOL FOR CREDIT CARD PAYMENT:

Requirements in SET :

SET protocol has some requirements to meet, some of the important requirements are :

- It has to provide mutual authentication i.e., customer (or cardholder) authentication by confirming if the customer is intended user or not and merchant authentication.
- It has to keep the PI (Payment Information) and OI (Order Information) confidential by appropriate encryptions.
- It has to be resistive against message modifications i.e., no changes should be allowed in the content being transmitted.

- SET also needs to provide interoperability and make use of best security mechanisms.

Participants in SET :

In the general scenario of online transaction, SET includes similar participants:

1. **Cardholder** – customer
2. **Issuer** – customer financial institution
3. **Merchant**
4. **Acquirer** – Merchant financial
5. **Certificate authority** – Authority which follows certain standards and issues certificates (like X.509V3) to all other participants.

SET functionalities:

1. **Provide Authentication**
   - **Merchant Authentication** – To prevent theft, SET allows customers to check previous relationships between merchant and financial institution. Standard X.509V3 certificates are used for this verification.
   - **Customer / Cardholder Authentication** – SET checks if use of credit card is done by an authorized user or not using X.509V3 certificates.
2. **Provide Message Confidentiality**: Confidentiality refers to preventing unintended people from reading the message being transferred. SET implements confidentiality by using encryption techniques. Traditionally DES is used for encryption purpose.
3. **Provide Message Integrity**: SET doesn't allow message modification with the help of signatures. Messages are protected against unauthorized modification using RSA digital signatures with SHA-1 and some using HMAC with SHA-1,
4. **Dual Signature:**

   The dual signature is a concept introduced with SET, which aims at connecting two information pieces meant for two different receivers:

Order Information (OI) for merchant Payment Information (PI) for bank

4.4.4 INTELLECTUAL PROPERTY IN E – COMMERCE

Intellectual Property (IP) is a legal term that has been associated with industrial **property** with copyrights and other rights in the similar field.

The **Intellectual Property** Law safeguards the business interests and entities of a company or an individual against unfair competition. **E-Commerce** based businesses consider **it** as their most valuable asset and often own Patent portfolios and trademarks to enhance the value of their online businesses.

Types of Intellectual Property :-

1. Copyright

In this digital era, copyrights play a significant role in safeguarding the creative content and information available on the websites. With rapid digitalization, the copyright owners seek the protection to prevent any unauthorized copying or distribution of work presented online.

Example:- Encryption and Watermarking can be effectively used to safeguard the IP rights of online businesses.

2. Trademarks

In the online world and E-Commerce, Trademarks have considerable importance to build a brand image by growing or selling the businesses A registered trademarks also makes it easier to take legal action and proceedings against brands that infringe on your business assets online.

3. Patents

Patents offer a considerable amount of incentives to the researchers and innovators in the arena of E-Commerce and online businesses. Patents help in licensing, contracting to outsource, and building strategic relationships involved in E-Commerce.

4.4.5 ELEMENTS OF E COMMERCE PROTECTED UNDER INTELLECTUAL PROPERTY ACT

1. E-Commerce systems, search engines or other technical Internet tools
2. Software includes the text-based HTML code
3. Website design is protected under copyright.
4. Content in the form of written material, photographs, graphics,
5. Databases can be protected by copyright or by sui generis database laws.
6. Business Names, Logos, Product names, domain names and other signs
7. Graphic Symbols, displays, graphic user interfaces

Case Studies

1. The Coca-Cola Company v. Bisleri International Pvt. Ltd. and Ors

This case is better known as the ***MAAZA War*** case . Coca Cola is the largest brand of soft drinks operating in 200 countries whereas Defendant (BIsleri)No1 earlier known as Acqua Minerals Pvt. Ltd. used to be a part of the Parle Group of Industries. The owners of Bisleri had sold the trademarks, formulation rights, know-how, intellectual property rights, and goodwill etc. of their product MAAZA amongst others to the coca cola by a master agreement.

In March 2008, when the Coca cola filed for registration of MAAZA trademark in Turkey, the defendant sent a legal notice repudiating the Licensing Agreement thereby ceasing the Coca cola from manufacturing MAAZA and using its trademarks etc. directly or indirectly. In consequence, the Coca cola claimed permanent injunction and damages for infringement of trademark and passing off. The coca cola also alleged that the defendant had unauthorisedly permitted the manufacture of certain ingredients of the beverage bases of MAAZA to be manufactured by a third party in India.

The court held that it is a well-settled position of law that exporting products from a country is to be considered as a sale within the country wherefrom the goods are exported and it amounts to infringement of the trademark.

The Court granted an interim injunction against the defendant from using the mark in India as well as in the export market to prevent the

plaintiff from irreparable loss and injury and quashed the appeal by the defendant.

2. Yahoo! Inc. v/s Akash Arora

The Yahoo s a global internet media who is the owner of the trademark **'Yahoo!'** and the domain name **'Yahoo.Com'**, which are very well-known and rendering services under its domain name. While the application of the plaintiff for registration of the trademark was pending in India, the defendant Akash Arora started providing similar services under the name **'Yahoo India'**.

The present case is brought out by Yahoo for passing off the services and goods of the defendants as that of the Yahoo's by using a name which is identical to or deceptively similar to the plaintiff's trademark **'Yahoo!'** and prayed for a permanent injunction to prevent the defendant from continuing to use the name.

The Court addressed the issue and came to the conclusion that Yahoo Inc had a good reputation in the market and that the name adopted by the defendant were deceptive and misleading causing damage to the reputation of the plaintiff and undue gain for the defendants. In consequence, the court granted an injunction in favour of Yahoo.

Difference Between Symmetric and Asymmetric Key Encryption

[redacted]

Symmetric Key Encryption: Encryption is a process to change the form of any message in order to protect it from reading by anyone. In Symmetric-key encryption the message is encrypted by using a key and the same key is used to decrypt the message which makes it easy to use but less secure. It also requires a safe method to transfer the key from one party to another.

Asymmetric Key Encryption: Asymmetric Key Encryption is based on public and private key encryption techniques. It uses two different key to encrypt and decrypt the message. It is more secure than the symmetric key encryption technique but is much slower.

Symmetric Key Encryption	Asymmetric Key Encryption
It only requires a single key for both encryption and decryption.	It requires two keys, a public key and a private key, one to encrypt and the other one to decrypt.
The size of cipher text is the same or smaller than the original plain text.	The size of cipher text is the same or larger than the original plain text.
The encryption process is very fast.	The encryption process is slow.
It is used when a large amount of data is required to transfer.	It is used to transfer small amounts of data.
It only provides confidentiality.	It provides confidentiality, authenticity, and non-repudiation.
The length of key used is 128 or 256 bits	The length of key used is 2048 or higher
In symmetric key encryption, resource utilization is low as compared to asymmetric key encryption.	In asymmetric key encryption, resource utilization is high.
It is efficient as it is used for handling large amount of data.	It is comparatively less efficient as it can handle a small amount of data.
Security is less as only one key is used for both encryption and decryption purpose.	It is more secure as two keys are used here- one for encryption and the other for decryption.
The Mathematical Representation is as follows- P = D (K, E(P)) where K -> encryption and decryption key P -> plain text D -> Decryption E(P) -> Encryption of plain text	The Mathematical Representation is as follows- P = D(Kd, E (Ke,P)) where Ke -> encryption key Kd -> decryption key D -> Decryption E(Ke, P) -> Encryption of plain text using encryption key Ke . P -> plain text

4.5.5 ELECTRONIC SIGNATURE

An E-Signature or electronic signature is a legal way to get consent or approval on electronic documents or forms. It can replace a handwritten signature in virtually any process.

Example - A scanned image of the person's ink signature, a mouse squiggle on a screen or a hand-signature created on a tablet using your finger or stylus, a signature at the bottom of your email, a typed name, a biometric hand-signature signed on a specialized signing hardware device.

Electronic Signature v/s Digital Signature

Electronic Signature	Digital Signature
1. This is not authorized and does not require certification authorities	1. This is authorized and regulated by certification authorities.
2. Does not uses any coding	2.Have secure coding
3. Verify document	3. Secure Document
4.Easy to use but less authentic	4.Prefeeered more due to high level of authenticity
5. Can Not be verified	5. Can be verified
6. Used for securing document	6. Shows intent consent

4.5.6 BENEFITS OF ELECTRONIC SIGNATURE-

1. **Enhanced security.** You can be confident that your documents will make it to the right people with security controls including automatic independent verification. Also known as Knowledge Based Authentication

(KBA), this independent verification step is required for certain IRS forms such as the 8878 and 8879 and keeps your clients' documents secure.

2. **Easy to use across industries and countries.** No matter who your clients are, or where they are located, users are accustomed to the eSignature experience, and prefer the convenience of signing a document right from their phone or tablet.

3. **Workflow tracking.** Easily track who has opened, signed, or approved a document, and who is holding you up. You'll have a complete paper trail of who viewed the document and when, without the actual paper!

4. **Convenience for you.** Collect signatures and approvals on multiple documents at one time without printing a single page of paper.

5. **Way better experience for your clients.** Clients can sign quickly from anywhere, on any device! In a time where clients want real-time access to documents, connecting your eSignature solution to your client portal software is a must.

6. **Get paid faster.** Ask for signature and payment details on the same document to securely collect all the information you need to get your clients up and running—including the payment to you!

7. **Centralized document storage**. When you pair eSignature with Smart Vault, you'll benefit from having a central document repository. Gone are the days of searching file cabinets, piles on your desk, or even different systems on your computer to find a document.

8. **Paperless workflow.** When you integrate your eSignature solution with other tools you already use, like Smart Vault, there's no need for printing, scanning, or meeting in person. The signed document is initiated and returned to the same location in Smart Vault – and you get notified when all parties sign.

9. **Increase collaboration.** Collect approvals and signatures from multiple parties in whatever order you choose to increase collaboration and keep projects moving.

10. **Save money!** All of these benefits add up to big cost savings for your business, from reducing paper and printing costs, to reducing the amount of time it takes to sign and collect payment from new clients.

Digital Signature

What is Digital Signature?

- Digital Signature is a type of electronic signature that encrypts documents with digital codes that are particularly difficult to duplicate.
- A digital signature (standard electronic signature) takes the concept of traditional paper-based signing and turns it into an electronic "fingerprint." This "fingerprint," or coded message, is unique to both the document and the signer and binds them together.
- It is used to validate the authenticity and integrity of a message, software or *digital* document. Digital signatures cryptographically bind an electronic identity to an electronic document and the signature cannot be copied to another document.

3

4

What is Digital Signature?

- Digital signature technique is based on public key cryptography with a difference.
- In public key cryptography a pair of keys are used, one public key and one private key. The public key is often used for message encryption , and the private key is often used for decrypting the message.
- However in case of digital signature message is encrypted with the private key and decrypted with the public key.
- Only a specific person with the corresponding private key can encrypt the message or in other words sign the message. However any party who has the signatory's public key can encrypt the message, in other words can verify the message.

Attributes of Digital Signature

- Digital signature ensures the confidentiality via the following three attributes:

1. Authentication
2. Integrity
3. Non-repudiation

Attributes of Digital Signature

- **Authentication:** Authentication means *the act of proving who you say you are.* Authentication means that you know who created and sent the message. Digital signature is used to authenticate the source of messages. It ensures the user of the sender.
- **Integrity:** Integrity ensures that when a message is sent over a network, the data that arrives is the same as the data that was originally sent. Integrity is the assurance that the information is trustworthy and accurate. Digital signature ensures the integrity of message.
- **Non-repudiation:** this is an important criteria of digital signature. As digital signature ensures the authentication of the message, so the sender can't repudiate it later. At the same time it also ensures the identity of the receiver, so the receiver can't repudiate it later.

What is Electronic Signature?

- An electronic signature is a typed name or a scanned image of a handwritten signature.
- As a result, e-signatures are very problematic when it comes to maintaining integrity and security, as nothing prevents one individual from typing another individual's name.
- Due to this reality, an electronic signature that does not incorporate additional measures of security (the way digital signatures do) is considered an insecure way of signing documentation.

Difference Between Digital and Electronic Signature

- A digital signature, often referred to as advanced or standard version of electronic signature, that provides the highest levels of security and universal acceptance.
- Digital signatures are based on Public Key Infrastructure (PKI) technology, and guarantee signer identity and intent, data integrity, and the non-repudiation of signed documents. The digital signature cannot be copied, tampered with or altered.

Is Digital Signature Legally Enforceable?

"Yes"

- In 2006, The parliament of Bangladesh enacted "ICT Act 2006", which made signed electronic contracts and documents as legally binding as a paper-based contract.
- Today, digital signature (standard electronic signature) solutions carry recognized legal significance, enabling organizations to comply with regulations worldwide.

DSA: How Signature is Verified by the Receiver ?

- Signature verification may be performed by any party the signatory (sender), the intended receiver or any other party using the signatory's public key.
- A signatory may wish to verify that the computed signature is correct or not, before sending the signed message to the intended receiver.
- The intended receiver (or any other party) verifies the signature to determine its authenticity upon on receiving the message.

Module 2 : EDI SECURITY
Electronic Data Interchange

E D I

a new business paradigm

1

Definitions

- **Electronic Data Interchange (EDI)**

  a subset or part of Electronic Commerce (EC) is the computer-to-computer exchange of business data in a standard, machine-processable format. The information is generally patterned after a conventional paper document, such as a purchase order or invoice. It is a "paperless trading"

4

Strategic Importance Initial

- **Time**

  Through the use of EDI, companies able to improve their response time and decrease their time to market by accelerating the Purchase Order-to-Invoice-to-Payment process from weeks or days to hours, or even minutes. Not only were they shorter, but they were also more accurate and reliable.

11

Strategic Importance Initial

- **Costs benefits**

  Through the use of EDI, innovative business programs such as Just-In-Time inventory management were possible. EDI and JIT allowed companies to have more control over their inventory levels and reduce their costs by increasing inventory turns and decreasing safety stocks.

13

Benefits of EDI

Direct transmission

EDI includes the direct transmission of data between organizations VAN. EDI is not facsimile transmission (fax) of information nor is it electronic mail (e-mail). Both of these transmission types are in "free format" (not standard format) and, therefore, generally require rekeying of data into the receiver's computer system.

15

Benefits of EDI

Cut down the possibility of human error

EDI would also cut down on the tendency for "human error". EDI eliminates this possibility because the receiving end is a computer that simply translates the message that has already been keyed into the system.

16

Benefits of EDI

The benefits of EDI include:

Time savings and associated financial savings accrued,

Improved accuracy,

Improved trading partner relationships and client interactions,

Improved reconciliation of transactions exchanged.

18

Technical Aspects of EDI

EDI messages

EDI messages are passed through a Value Added Network or "VAN." In principle a VAN is an electronic mail station for holding and passing messages.

19

Technical Aspects of EDI

EDI Hardware

EDI transactions can be passed from many types of computers (i.e. PC, Mac, UNIX, and mainframe). Trading partners do not need to use the same type of equipment. EDI messages are hardware independent, due in part to the X12 standard. The transactions are sent via dedicated links, ISDN or phone lines.

21

Summary

Eventually more and more business transactions will migrate to the World Wide Web due to the ease of access to this medium. Deciding which transactions are best suited for EDI over the Internet will be a function of accessibility, data security/privacy, and the means of communication. These three areas should be studied carefully when proceeding with large-scale EDI or E-Commerce initiatives.

31

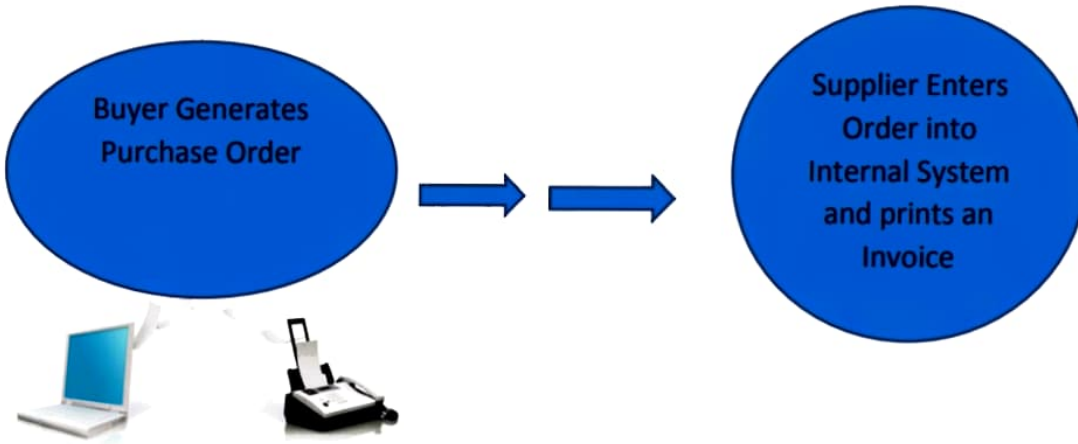
2.2 CONCEPT OF ELECTRONIC DATA INTERCHANGE (EDI)

Electronic Data Interchange (EDI) is the computer-to-computer exchange of business documents in a standard electronic format between business partners.

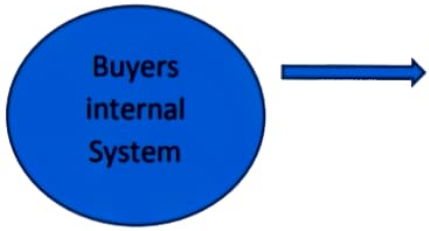
By moving from a paper-based exchange of business document to one that is electronic, businesses enjoy major benefits such as reduced cost, increased processing speed, reduced errors and improved relationship with business partners.

Computer-to-Computer: -

Computer-to-computer EDI replaces postal mail, fax and email. While email is also an electronic approach, the documents exchanged via email must still be handled by people rather than computers. Having people involved slows down the processing of the documents also introduce errors. Instead, EDI documents can flow straight through to the appropriate application on the receiver's computer and processing can begin immediately. A typical manual process looks like this, with lots of paper and people involvement:



The EDI process looks like this – no paper, no people involved:



Business Documents: -

These are any of the documents that are typically exchanged between businesses. The most common documents exchanged via EDI are purchase orders, invoices and advance ship notices. But there are many, many others such as bill of lading, customs documents, inventory documents, shipping status documents and payment documents.

Standard Format: -

Because EDI documents must be processed by computers rather than humans, a standard format must be used so that the computer will be able to read and understand the documents. A standard format describes what each piece of information is and in what format. Without a standard format, each company would send documents using its company-specific format and, much as an English-speaking person probably doesn't understand Japanese, the receiver's computer system doesn't understand the company-specific format of the sender's format.

There are several EDI standards in use Today,

- Including ANSI, EDIFACT, TRADACOMS and ebXML .and for each standard there are many different versions. E.g. ANSI 5010 or EDIFACT version D12, Release A. When two businesses decide to exchange EDI documents, they must agree on the specific EDI standard and version.

- Businesses typically use an EDI translator-either as in-house software or via an EDI service provider to translate the EDI format so the data can be used by their internal applications and thus enable straight through processing documents.

Business Partners: -

The exchange of EDI document is typically between two different Companies, referred to as business partners or trading partners. For example, Company A may buy goods from Company B. Company A sends orders to Company Company A and Company B are business partners

2.2.1 PROS AND CONS OF EDI (ADVANTAGES AND DISADVANTAGE OF EDI)

It is quite easy to see how the technology we use today has vastly improved the processes of many industries. For one, Technology improves the workforce by introducing something known as Electronic Data Interchange, or EDI. According to the national Institute of Standards and Technology, EDI is "the computer-to-computer interchange of strictly formatted messages that represent documents other than monetary instruments."

The NIST states that EDI could also refer to "a sequence of messages between two parties, either of whom may serve as originator or recipient. The formatted data representing the documents may be transmitted from originator to recipient via telecommunications or physically transported on electronic storage media."

This **Fence core** process, then, involves using machines to perform what would have traditionally been a human task.

EDI ADVANTAGES

It should not come as much of a surprise that there are many advantages to using EDI in your business.

- Cost effective: - Cutting paper waste and all paper processing quickly reduce paper costs.
- Efficiency: - cloud-computing and machine learning eliminates computational repetition, redundancies, and errors that would be more common among humans.

- Speed: - The electronic transfer of data ensures more consistency and accuracy without sacrificing pace.
- Accuracy: - By using cloud computing technology, you are able to transfer documents faster than would have otherwise been possible.
- Service: - Faster processing means better customer service, over all, in turn, helping you to expand your customer base.

EDI DISADVANTAGES: -

As with all things, wherever there are advantages there might also be disadvantages. So, with that, here are some ways that EDI might not serve your business; which means you should consider a different way to network and incorporate information technology.

- EDI uses multiple standards which can often limit have too many rigorous standards bodies with too many document formats which can malfunction in the face of cross-compatibility issues, which you will definitely encounter as you continue to apply more standards.
- EDI has a higher price point, which can be a little pricey for new business owners.
- Large Companies might actually find that EDI can limit the types of partnership you can develop with.