E-Commerce - Security Systems

Security is an essential part of any transaction that takes place over the internet. Customers will lose his/her faith in e-business if its security is compromised. Following are the essential requirements for safe e-payments/transactions −

- **Confidentiality** − Information should not be accessible to an unauthorized person. It should not be intercepted during the transmission.
- **Integrity** − Information should not be altered during its transmission over the network.
- **Availability** − Information should be available wherever and whenever required within a time limit specified.
- **Authenticity** − There should be a mechanism to authenticate a user before giving him/her an access to the required information.
- **Non-Repudiability** − It is the protection against the denial of order or denial of payment. Once a sender sends a message, the sender should not be able to deny sending the message. Similarly, the recipient of message should not be able to deny the receipt.
- **Encryption** − Information should be encrypted and decrypted only by an authorized user.
- **Auditability** − Data should be recorded in such a way that it can be audited for integrity requirements.

Measures to ensure Security

Major security measures are following −

- **Encryption** − It is a very effective and practical way to safeguard the data being transmitted over the network. Sender of the information encrypts the data using a secret code and only the specified receiver can decrypt the data using the same or a different secret code.
- **Digital Signature** − Digital signature ensures the authenticity of the information. A digital signature is an e-signature authenticated through encryption and password.
- **Security Certificates** − Security certificate is a unique digital id used to verify the identity of an individual website or user.

Security Protocols in Internet

We will discuss here some of the popular protocols used over the internet to ensure secured online transactions.

Secure Socket Layer (SSL)

It is the most commonly used protocol and is widely used across the industry. It meets following security requirements −

- Authentication
- Encryption
- Integrity
- Non-reputability

"https://" is to be used for HTTP urls with SSL, where as "http:/" is to be used for HTTP urls without SSL.

Secure Hypertext Transfer Protocol (SHTTP)

SHTTP extends the HTTP internet protocol with public key encryption, authentication, and digital signature over the internet. Secure HTTP supports multiple security mechanism, providing security to the end-users. SHTTP works by negotiating encryption scheme types used between the client and the server.

Secure Electronic Transaction

It is a secure protocol developed by MasterCard and Visa in collaboration. Theoretically, it is the best security protocol. It has the following components −

- **Card Holder's Digital Wallet Software** − Digital Wallet allows the card holder to make secure purchases online via point and click interface.
- **Merchant Software** − This software helps merchants to communicate with potential customers and financial institutions in a secure manner.
- **Payment Gateway Server Software** − Payment gateway provides automatic and standard payment process. It supports the process for merchant's certificate request.
- **Certificate Authority Software** − This software is used by financial institutions to issue digital certificates to card holders and merchants, and to enable them to register their account agreements for secure electronic commerce.

Threat to E-Commerce

E-Commerce 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.

Electronic payments system:

With the rapid development of the computer, mobile, and network technology, e-commerce has become a routine part of human life. In e-commerce, the customer can order products at home and save time for doing other things. There is no need of visiting a store or a shop. The customer can select different stores on the Internet in a very short time and compare the products with different characteristics such as price, colour, and quality.

The electronic payment systems have a very important role in e-commerce. E-commerce organizations use electronic payment systems that refer to paperless monetary transactions. It revolutionized the business processing by reducing paperwork, transaction costs, and labour cost. E-commerce processing is user-friendly and less time consuming than manual processing. Electronic commerce helps a business organization expand its market reach expansion. There is a certain risk with the electronic payments system.

Some of them are:

The Risk of Fraud

An electronic payment system has a huge risk of fraud. The computing devices use an identity of the person for authorizing a payment such as passwords and security questions. These authentications are not full proof in determining the identity of a person. If the password and the answers to the security questions are matched, the system doesn't care who is on the other side. If someone has access to our password or the answers to our security question, he will gain access to our money and can steal it from us.

The Risk of Tax Evasion

The Internal Revenue Service law requires that every business declare their financial transactions and provide paper records so that tax compliance can be verified. The problem with electronic systems is that they don't provide cleanly into this paradigm. It makes the process of tax collection very frustrating for the Internal Revenue Service. It is at the business's choice to disclose payments received or made via electronic payment systems.

The IRS has no way to know that it is telling the truth or not that makes it easy to evade taxation.

The Risk of Payment Conflicts

In electronic payment systems, the payments are handled by an automated electronic system, not by humans. The system is prone to errors when it handles large amounts of payments on a frequent basis with more than one recipients involved. It is essential to continually check our pay slip after every pay period ends in order to ensure everything makes sense. If it is a failure to do this, may result in conflicts of payment caused by technical glitches and anomalies.

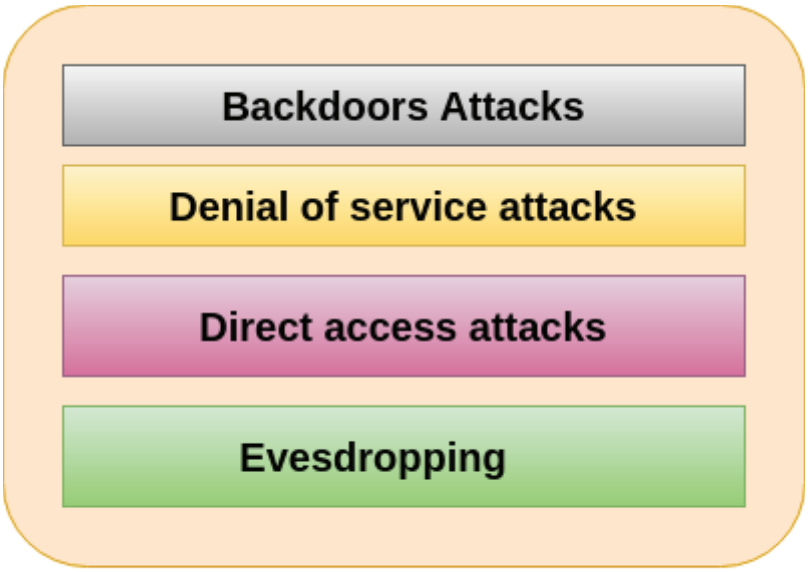
E-cash

E-cash is a paperless cash system which facilitates the transfer of funds anonymously. E-cash is free to the user while the sellers have paid a fee for this. The e-cash fund can be either stored on a card itself or in an account which is associated with the card. The most common examples of e-cash system are transit card, PayPal, GooglePay, Paytm, etc.

E-cash has four major components-

1. **Issuers** - They can be banks or a non-bank institution.
2. **Customers** - They are the users who spend the e-cash.
3. **Merchants or Traders** - They are the vendors who receive e-cash.
4. **Regulators** - They are related to authorities or state tax agencies.

In e-cash, we stored financial information on the computer, electronic device or on the internet which is vulnerable to the hackers. Some of the major threats related to e-cash system are-



E-cash Threats

Backdoors Attacks

It is a type of attacks which gives an attacker to unauthorized access to a system by bypasses the normal authentication mechanisms. It works in the background and hides itself from the user that makes it difficult to detect and remove.

Denial of service attacks

A denial-of-service attack (DoS attack) is a security attack in which the attacker takes action that prevents the legitimate (correct) users from accessing the electronic devices. It makes a network resource unavailable to its intended users by temporarily disrupting services of a host connected to the Internet.

Direct Access Attacks

Direct access attack is an attack in which an intruder gains physical access to the computer to perform an unauthorized activity and installing various types of software to compromise security. These types of software loaded with worms and download a huge amount of sensitive data from the target victims.

Eavesdropping

This is an unauthorized way of listening to private communication over the network. It does not interfere with the normal operations of the targeting system so that the sender and the recipient of the messages are not aware that their conversation is tracking.

Credit/Debit card fraud

A credit card allows us to borrow money from a recipient bank to make purchases. The issuer of the credit card has the condition that the cardholder will pay back the borrowed money with an additional agreed-upon charge.

A debit card is of a plastic card which issued by the financial organization to account holder who has a savings deposit account that can be used instead of cash to make purchases. The debit card can be used only when the fund is available in the account.

Some of the important threats associated with the debit/credit card are-

ATM (Automated Teller Machine)-

It is the favourite place of the fraudster from there they can steal our card details. Some of the important techniques which the criminals opt for getting hold of our card information is:

Skimming-

It is the process of attaching a data-skimming device in the card reader of the ATM. When the customer swipes their card in the ATM card reader, the information is copied from the magnetic strip to the device. By doing this, the criminals get to know the details of the Card number, name, CVV number, expiry date of the card and other details.

Unwanted Presence-

It is a rule that not more than one user should use the ATM at a time. If we find more than one people lurking around together, the intention behind this is to overlook our card details while we were making our transaction.

Vishing/Phishing

Phishing is an activity in which an intruder obtained the sensitive information of a user such as password, usernames, and credit card details, often for malicious reasons, etc.

Vishing is an activity in which an intruder obtained the sensitive information of a user via sending SMS on mobiles. These SMS and Call appears to be from a reliable source, but in real they are fake. The main objective of vishing and phishing is to get the customer's PIN, account details, and passwords.

Online Transaction

Online transaction can be made by the customer to do shopping and pay their bills over the internet. It is as easy as for the customer, also easy for the customer to hack into our system and steal our sensitive information. Some important ways to steal our confidential information during an online transaction are-

- By downloading software which scans our keystroke and steals our password and card details.
- By redirecting a customer to a fake website which looks like original and steals our sensitive information.

- By using public Wi-Fi

POS Theft

It is commonly done at merchant stores at the time of POS transaction. In this, the salesperson takes the customer card for processing payment and illegally copies the card details for later use.

Security Policies

Security policies are a formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidelines related to the security of information. It is a written document in the organization which is responsible for how to protect the organizations from threats and how to handles them when they will occur. A security policy also considered to be a "living document" which means that the document is never finished, but it is continuously updated as requirements of the technology and employee changes.

Need of Security policies-

1) It increases efficiency.

The best thing about having a policy is being able to increase the level of consistency which saves time, money and resources. The policy should inform the employees about their individual duties, and telling them what they can do and what they cannot do with the organization sensitive information.

2) It upholds discipline and accountability

When any human mistake will occur, and system security is compromised, then the security policy of the organization will back up any disciplinary action and also supporting a case in a court of law. The organization policies act as a contract which proves that an organization has taken steps to protect its intellectual property, as well as its customers and clients.

3) It can make or break a business deal

It is not necessary for companies to provide a copy of their information security policy to other vendors during a business deal that involves the transference of their sensitive information. It is true in a case of bigger businesses which ensures their own security interests are protected when dealing with smaller businesses which have less high-end security systems in place.

4) It helps to educate employees on security literacy

A well-written security policy can also be seen as an educational document which informs the readers about their importance of responsibility in protecting the organization sensitive data. It involves on choosing the right passwords, to providing guidelines for file transfers and data storage which increases employee's overall awareness of security and how it can be strengthened.

We use security policies to manage our network security. Most types of security policies are automatically created during the installation. We can also customize policies to suit our specific environment. There are some important cybersecurity policies recommendations describe below-

1. Virus and Spyware Protection policy

This policy provides the following protection:

- It helps to detect, removes, and repairs the side effects of viruses and security risks by using signatures.
- It helps to detect the threats in the files which the users try to download by using reputation data from Download Insight.
- It helps to detect the applications that exhibit suspicious behaviour by using SONAR heuristics and reputation data.

2. Firewall Policy

This policy provides the following protection:

- It blocks the unauthorized users from accessing the systems and networks that connect to the Internet.
- It detects the attacks by cybercriminals.
- It removes the unwanted sources of network traffic.

3. Intrusion Prevention policy

This policy automatically detects and blocks the network attacks and browser attacks. It also protects applications from vulnerabilities. It checks the contents of one or more data packages and detects malware which is coming through legal ways.

4. LiveUpdate policy

This policy can be categorized into two types one is LiveUpdate Content policy, and another is LiveUpdate Setting Policy. The LiveUpdate policy contains the setting which determines when and how client computers download the content updates from LiveUpdate. We can define the computer that clients contact to check for updates and schedule when and how often clients computer check for updates.

5. Application and Device Control

This policy protects a system's resources from applications and manages the peripheral devices that can attach to a system. The device control policy applies to both Windows and Mac computers whereas application control policy can be applied only to Windows clients.

6. Exceptions policy

This policy provides the ability to exclude applications and processes from detection by the virus and spyware scans.

7. Host Integrity policy

This policy provides the ability to define, enforce, and restore the security of client computers to keep enterprise networks and data secure. We use this policy to ensure that the client's computers who access our network are protected and compliant with companies? securities policies. This policy requires that the client system must have installed antivirus.