**Lecture 29: E-Commerce Security – Part 1**



**1. Elements of E-Commerce Security**

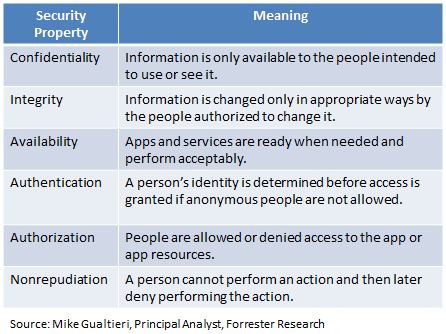
**E-commerce security** refers to the protection of online transactions, personal data, and business operations from malicious activities. It is crucial for both businesses and consumers to ensure that sensitive information like credit card details, login credentials, and personal data is protected from cybercriminals.

Key **elements** of e-commerce security include:



* 1. **Confidentiality**:
     + Ensures that sensitive data, such as credit card numbers and personal details, is only accessible to authorized parties.
     + **Example**: Encryption ensures that even if data is intercepted during a transaction, it cannot be read without the decryption key.
  2. **Integrity**:
     + Ensures that data is not altered during transmission. It guarantees that the information sent from the buyer to the seller is exactly what was intended.
     + **Example**: **Hashing** techniques are used to verify the integrity of files, ensuring that no changes have been made to the data.
  3. **Authentication**:
     + Ensures that both parties in the transaction (buyer and seller) are who they claim to be.
     + **Example**: **Two-factor authentication (2FA)** on online banking or e-commerce websites requires a second form of identification, such as a text message code or fingerprint.
  4. **Non-repudiation**:
     + Ensures that a transaction cannot be denied once it is completed. Both parties must acknowledge the transaction.
     + **Example**: **Digital signatures** are used to verify that a person has signed off on a particular transaction and cannot later deny it.
  5. **Authorization**:
     + Ensures that users can only access data or services they are allowed to use.
     + **Example**: If a user is logged in to an online store, their access to the admin panel should be restricted.

**FOR MORE CLARITY**



**Common Threats in E-Commerce**

While e-commerce has revolutionized the way businesses and consumers interact, it also exposes both parties to a variety of security threats. Some of the most common threats include:

**Phishing**:

* + - Phishing attacks involve tricking users into revealing sensitive information, such as usernames, passwords, and credit card details, by pretending to be a legitimate source (e.g., a trusted e-commerce platform or bank).
    - **Example**: A user may receive an email that appears to be from **Amazon**, asking them to verify their account by clicking on a link. The link leads to a fake website designed to steal login credentials.
  1. **SQL Injection**:
     + SQL injection is a type of attack where malicious code is inserted into the input fields of an e-commerce website to manipulate the database and access sensitive data.
     + **Example**: Attackers may exploit vulnerabilities in a search box or login page to inject harmful SQL queries into the website’s database.
  2. **Man-in-the-Middle (MITM) Attacks**:
     + In this type of attack, cybercriminals intercept the communication between the buyer and seller to steal sensitive information during the transaction.
     + **Example**: When a user makes a payment via an unsecured Wi-Fi network, a hacker could intercept the credit card information and use it for fraudulent transactions.
  3. **Cross-Site Scripting (XSS)**:
     + XSS attacks occur when attackers inject malicious scripts into a website. When users visit the website, the scripts execute and can steal data like cookies or credentials.
     + **Example**: A hacker inserts malicious JavaScript code into the review section of an e-commerce site. When users leave reviews, their data gets captured by the hacker.
  4. **Denial-of-Service (DoS) Attacks**:
     + In a DoS attack, a hacker floods an e-commerce site with traffic, making it unavailable for legitimate users.
     + **Example**: During the holiday shopping season, a hacker might flood a major retailer's website with excessive traffic, preventing customers from making purchases.

**MORE CLARITY ON CONCEPTS**

### Electronic Payments Threat

The idea of everything taking place online is now applicable for the finance and banking sector as well. The system of online wallets and e-transactions have become very common as a mode of payment. But handling money on a network is also dangerous as hackers may break into the firewall. There are many other risks like –

#### 1. Fraud

The users have pins or passwords to facilitate an online transaction. But payment authorization based on just passwords and security questions does not guarantee the identity of a person. This may lead to a fraud case if someone else gets ahold of our passwords. This way the third person can steal money easily.

#### 2. Tax Evasion

The invoice is provided by the companies as paper records to verify tax collection. But in an online scenario, things become blurry and the Internal Revenue Service faces the challenge. It becomes hard for them to process tax collection and verify if the organization is being ethical or not.

#### 3. Payment Conflicts

These transactions take place between automated electronic systems and the users. Because it’s a machine at the end of the day, errors while handling payments are possible. These glitches and anomalies lead to conflicts of payment and users end up losing their money.

#### 4. E-cash

The paperless cash system is by using online wallets like PayPal, GooglePay, Paytm, etc. Because all the financial information is in that application, a single security breach can lead to the disclosure of private information and monetary loss.

It has four components – issuers, customers, merchants, and regulators. The issuers are the financial institutions, customers are the ones using this money, merchants are the ones earning it and regulators are for monitoring its movement. Some of the threats that e-commerce website face while using e-cash are –

##### a. Direct Access Attacks

The hackers get direct access to the device and install programs in it without permission. These softwares have worms that automatically save information from the device without getting caught. It can lead to server paralysis and eventually make it offline.

It can also slow down the speed and make consumers go back with a negative experience. To solve this issue in particular, always use a web application firewall, go blacking or change server IP in the worst case scenario. You can read about more solutions in detail below.

##### b. Backdoors Attacks

The hackers use this attack to enter the user’s system by escaping normal authentication using unethical means. As the name suggests, it functions in the background making it difficult for the users to detect and remove it.

##### c. Denial of service attacks and Distributed Denial Service Attacks

The hacker breaks into the system and takes away all the accessibility from the user. They block the users from all the functions and resources and disrupt the system temporarily. This is mainly done by using an internet network and the hackers may ask for ransom/favors to activate the device again. In case of DDoS, the hackers will use your computer to sabotage the security of another computer.

##### d. Eavesdropping

This is a comparatively new way by which hackers listen to our personal conversations over the internet. It doesn’t lead to disruption in the system functioning but gives them access to private communication which they might leverage upon later. The users in this case are not aware of their conversation being tracked. Wifi eavesdropping is also a part of this type.

### Personal Information Threats

#### 1. Scraping

This is mostly done by competitive brands to get their hands on sensitive data and valuable internal metrics. The companies are very confidential about such information but hackers/bots can break into the system to get access.

#### 2. Spam

This is usually by sending out attractive baits to get personal information. The spammers can also use blog pages and contact forms to get companies to click on malicious links. This allows them to harm the website’s speed, security, and consumers as well.

#### 3. SQL Injection

It is a technique in which hackers use query submission forms to gain database access. They corrupt all the information using viruses and make it infectious. They may copy the data for personal benefit and delete it from the main system permanently.

#### 

#### 4. Bots

These are software that has web crawlers to decide website rankings of existing pages on the internet. The hackers can use these crawlers to track competitor’s policies and strategy leading to unfair market practices. This may be used against the company or in favor of the competitor.

#### 5. Brute Force Attacks

The hackers use this method to draw patterns and guesses to crack user/company passwords. They will do so by using algorithms and multiple combinations until they get the correct password to get in.

#### 6. Trojan horses

This is a malware that users download thinking of it as legitimate software. But it can collect the user pattern, financial information, personal details, and more without the owner’s permission. The commercial website becomes prone to sensitive data leaks and system infections.

#### 7. Cross-Site Scripting (XSS)

This technique uses the planting of malicious JavaScript snippets that track consumer behavior and patterns on websites. This is by accessing customers’ cookies and computers. Content Security Policy is one way to assure customers about their privacy and safety.

#### 8. Man in the middle

Similar to eavesdropping, the hackers use open networks or weaker networks to listen in on conversations between a store consultant and a customer. They can manipulate the message or the response and use the information for personal gain.

#### 9. Hacktivism

Hacking activism is a type of hacking that targets social media more than the websites. It is usually to bring out social issues by breaking into a company’s social media accounts. It can also include spamming websites with email addresses to bring the server down.

### Credit/Debit Card Threats

#### ATM

The fraudsters are very active at these machines to steal card details. Some of the common ways are –

##### a. Skimming

A device is attached to the card reader at the ATM which skims data as soon as the card enters the machine. AS the user swipes the card, the information from the magnetic strip is copied on the skimming device. The scammers by this method get access to all financial details about the person.

##### b. Unwanted Presence

This is a physical way of getting financial information which is quite common. The rule at the ATM celery says one person at a time but many people tend to lurk and overlook the card details with negative intention.

##### c. POS Theft

The salesperson at the store may have an ulterior motive and use the financial information of customers for personal benefits. It is commonly done at merchant stores at the time of POS transactions. This may be done at the billing counter when the person copies the information on the card using unfair means.

##### d. Online Transaction

Like we read above, online transactions are very risky as hackers can break at any time. They can steal passwords, card details. Personal information, identity, and much more by unethical means. The ways to do them are already mentioned above.

##### e. Vishing/Phishing

The scammers use SMS and calls to set baits for the users to make them reveal personal information. They may act as a financial institution or some other credible entity to get your card details for unfair practices.

1. **Case Studies of E-Commerce Security Breaches**

Several high-profile e-commerce security breaches have occurred over the years, resulting in financial losses and reputational damage. Here are a few examples:

1. **Target Data Breach (2013)**:
   * **What happened**: In 2013, hackers stole the credit and debit card details of **40 million** customers from Target's e-commerce platform. They gained access hrough a third-party vendor and used this access to install malware on Target's network.
   * **Impact**: The breach led to massive financial losses and harmed Target's reputation. The company spent millions of dollars on fixing the security vulnerabilities and offering compensation to affected customers.
   * **Lesson**: This breach highlighted the importance of securing vendor relationships and regularly testing third-party systems for vulnerabilities.
2. **eBay Data Breach (2014)**:
   * **What happened**: In 2014, cybercriminals accessed **145 million** eBay user accounts by exploiting a vulnerability in eBay's security systems. The breach was discovered when hackers gained access to user passwords, names, and other personal details.
   * **Impact**: The breach caused eBay to advise its users to change their passwords. The company also had to deal with a loss of trust and credibility.
   * **Lesson**: It emphasized the need for strong encryption methods for password storage and better monitoring of accounts for suspicious activity.
3. **Yahoo Data Breach (2013-2014)**:
   * **What happened**: In one of the largest data breaches in history, **Yahoo** revealed in 2016 that hackers had stolen **3 billion** accounts over a period of time between 2013 and 2014. The attackers gained access to user data, including names, email addresses, and passwords.
   * **Impact**: The breach severely damaged Yahoo's reputation, and the company had to pay fines and settle lawsuits with affected users.
   * **Lesson**: It highlighted the importance of encryption, multi-factor authentication (MFA), and continuous monitoring of user accounts for unusual activities.