Secure Electronic Transaction (SET)

Secure Electronic Transaction (SET) is a standard protocol developed by Visa and MasterCard to ensure secure payment card transactions over the Internet.

Objectives of SET:

- Ensure **confidentiality** of payment information.
- Ensure **integrity** of all transmitted data.
- Authenticate **cardholders** and **merchants**.
- Prevent unauthorized access and fraud.

Key Components:

- **Cardholder:** The buyer making the payment.
- **Merchant:** The seller receiving the payment.
- **Payment Gateway:** Processes the payment between merchant and banks.
- **Certificate Authority (CA):** Issues digital certificates to cardholders and merchants.

Working Steps:

1. Customer places an order and provides payment information encrypted with the merchant's public key.
2. Merchant forwards payment details to the payment gateway.
3. Payment gateway processes the transaction with the bank.
4. Digital certificates authenticate the merchant and customer.
5. Transaction completed securely.

Note: SET is now largely obsolete, replaced by TLS/SSL-secured communications and modern payment systems.

Intruders

Intruders are unauthorized users who try to gain access to computer systems to steal, modify, or destroy information.

Types of Intruders:

- **Masqueraders:** External users pretending to be authorized users.
- **Misfeasors:** Legitimate users who misuse their access privileges.
- **Clandestine Users:** Users who take control of a system and evade detection.

Intruder Activities:

- Password guessing and cracking.
- Installing malware.

- Stealing sensitive data.
- Disrupting services (Denial of Service attacks).

Viruses

A **virus** is a malicious software program designed to replicate and spread from one computer to another, often without user consent.

Types of Viruses:

- **File Infectors:** Attach to executable files.
- **Boot Sector Viruses:** Infect the boot sector of storage media.
- **Macro Viruses:** Infect documents like Word and Excel files.
- **Polymorphic Viruses:** Change code to avoid detection.

Effects of Viruses:

- Corrupt or delete data.
- Slow down system performance.
- Allow unauthorized access to systems.
- Cause system crashes.

Firewalls

A **firewall** is a security system that controls incoming and outgoing network traffic based on predetermined security rules.

Types of Firewalls:

- **Packet-Filtering Firewalls:** Inspect packets and allow/block based on IP addresses, ports, protocols.
- **Stateful Inspection Firewalls:** Track the state of active connections and make decisions based on connection state.
- **Application-Level Gateways (Proxy Firewalls):** Filter traffic at the application layer.
- **Next-Generation Firewalls (NGFWs):** Combine traditional firewall features with intrusion prevention, deep packet inspection, etc.

Functions of Firewalls:

- Block unauthorized access while permitting outward communication.
- Protect internal networks from external attacks.
- Log and report network activity.
- Enforce security policies.

Intrusion Detection

Intrusion Detection Systems (IDS) monitor network or system activities for malicious actions.

Types of IDS:

- **Network-based IDS (NIDS):** Monitors traffic on a network for suspicious activity.
- **Host-based IDS (HIDS):** Monitors activities on a specific host or device.

Techniques Used:

- **Signature-Based Detection:** Matches traffic patterns to known attack signatures.
- **Anomaly-Based Detection:** Looks for unusual behavior that may indicate an attack.

Benefits of IDS:

- Detect unauthorized access attempts.
- Identify policy violations.
- Alert administrators of potential threats.

Password Management

Password Management involves practices and systems designed to protect passwords and maintain authentication security.

Best Practices:

- **Strong Passwords:** Use a combination of letters, numbers, and symbols.
- **Multi-Factor Authentication (MFA):** Add an extra layer of security beyond just a password.
- **Regular Password Changes:** Update passwords periodically.
- **Password Storage:** Store passwords securely using hashing algorithms like bcrypt or PBKDF2.
- **Avoid Reuse:** Do not reuse passwords across multiple sites or systems.

Password Cracking Techniques:

- **Brute Force Attack:** Trying all possible password combinations.
- **Dictionary Attack:** Trying common words and phrases.
- **Social Engineering:** Tricking users into revealing their passwords.