eCommerce – Chapter 5

Drivers of eCommerce of the Internet

1. **Vulnerable Design of the Internet**
   The internet and its network protocols were never intended for use by untrustworthy people or criminals. It was designed for a closed and trusted community and with the goal of maximum efficiency.
2. **Shift to Profit-induced Crimes**
   In the early days of eCommerce, the main motivation of hackers was to gain fame or notoriety by defacing Web sites or gaining root access to a network.
   Today they are profit-oriented (e.g. *theft of personal information*)
3. **Developing Internet Underground Economy**
   Refers to eMarkets for stolen information.
4. **Dynamic Nature of eCommerce Systems and the Role of Insiders**
   eCommerce systems are permanently changing due to innovations, and each change involves the risk of new security problems.

Unintentional Threads

1. **Human Error**
   - Occurs in the design of the hardware of information system.
   - In programming, testing, data collection, data entry, authorization and instructions.
   - Result of negligence or miss understanding.
2. **Environmental hazards**
   - Earthquakes, severe storms, floods, power failures, fires, explosions.
3. **Defects in the computer systems**
   - Poor manufacturing, defective materials and outdated poorly maintained networks.

Intentional Attacks and Crimes

- Theft of data
- Inappropriate use of data
- Theft of laptops, equipment and computer programs
- Deliberate manipulation in handling, entering, processing, transferring, programming data.
- Vandalism
- Sabotage
- Malicious damage to computer resources
- Destruction from viruses and similar attacks
- Miscellaneous computer abuses
- Internet fraud

Network-level Security

- Refers to the protection of the process by which data items are communicated from a network to an end system.
- This excludes any coverage of what happens within the end system (both client and server systems).

Application-level Security

- Refers to security safeguards that are built into a particular application and that operate independently of any network-level security measures

Network-level Security

Firewall

- Limiting the set of applications for which traffic can enter the internal network from the Internet, and limiting the internal addresses to which traffic for different applications can go.
- Packet Filters: Filters each packet based only on information contained in the packet
- Application-Level Gateways: Intercept incoming and outgoing packets, uses proxies that copy and forward information across the gateway, and functions as proxy server, preventing any direct connection between a trusted server or client and an untrusted host.
- Stateful Packet Filter Gateways: Adds more intelligence to the filter decision-making process. Remember past packets that passed the firewall. Aware of the difference between a new and an established connection.

Demilitarized Zones

- Physical or logical subnetwork that contains and exposes an organization’s external services to a larger untrusted network, usually the internet.

Intrusion Detection Systems

- Software and/or hardware designed to detect illegal attempts to access, manipulate and/or disable system through a network.
- Types:
    - Anomaly detection
    - Signature detection

Application-level Security

Authentication

- Is a process to verify the real identity of an entity, which could be an individual, software agent, computer program or ecommerce web site.
- Verifies that the sender of the message is who the person claims to be.

Authorization

- Is the process of determining what an authenticated is allowed to access and which operations it is allowed to perform.
- Occurs after authentication.

Auditing

- The process of recording information about what was accessed, when, and by whom.

Confidentiality

- Refers to the ability to ensure that messages and data are available only to those who are authorized to view them.

Integrity

- Assurance that data are accurate and that a message has not been altered.

Non-repudiation

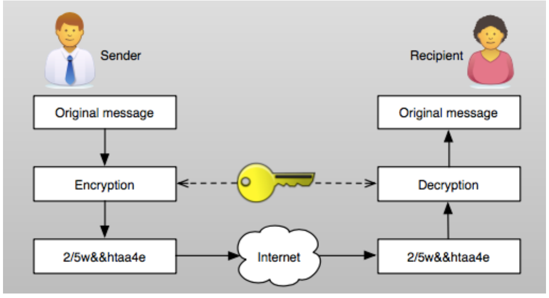
- Is a property archived through cryptographic methods to prevent an individual or entity from denying having preformed a particular action related to the data.

Availability

- Assurance that access to data, a Web site is timely available, reliable and restricted to authorized users.

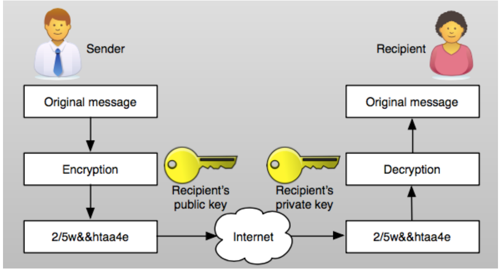
Symmetric Encryption

- Uses a single key that both sender and recipient possess.
- **Advantage**: Easy to implement.
- **Disadvantage**: Every pair of users needs its own key. If one key is lost, all other keys must be replaced as well.
- RSA Algorithm



Asymmetric Encryption

- Both sender and recipient need two keys. One of which is public and the other private. Both keys are mathematically related.
- **Public key:** Encryption. Can be passed openly between the parties.
- **Private key**: Decryption.
- Does not archive accountability, non-repudiation and authenticity.



Digital Signatures

- Can be used in conjunction with the public-key encryption scheme to provide confidentiality, integrity and non-repudiation.
- Validates the sender and time stamp of a transaction.
- Process:
  - Sender creates message
  - Hash function applied to the message creating a digital digest
  - Sender use his private key to encrypt the digital digest creating his digital signature.
  - Sender encrypt the message and digital signature using the recipients public key creating the digital envelope.
  - Sends digital envelope to receiver
  - Recipient decrypts the digital envelope using the recipient's own private key
  - Recipient decrypts the digital signature using sender's public key.
  - Using the same hash function the recipient creates a message digest from the decrypted message.
  - Compares the two digest.

Digital Certificates

- Document that uniquely identifies a party that owns the certificate, the time period for which the certificate is valid, the organization that issued the certificate and a digital signature that verifies the issuing organization's identity.
- It contains information about who owns the certificate, the public key of the subject and other relevant information.

Certification Authority

- Trusted party that generates and issues certificates on behalf users, enterprises and organizations.
- Each browser comes with a list of pre-established certification authorities and their digital signatures.