



STRATEGIC WEBSITE TECHNOLOGIES – SECURITY

M. Turan Söylemez
Yeditepe University
MBA Program

1



E-Commerce Security

An e-commerce security system has four fronts:

- Web Client Security
- Data Transport Security
- Web Server Security
- Operating System Security

A safe e-commerce system must handle all these fronts appropriately.

THE SECURITY OF A SYSTEM IS ONLY AS STRONG AS ITS WEAKEST LINK

2



The Client-Side Vulnerabilities

Active form content (such as plug-in software, Active-X controls, Java applets, even Images) can contain malicious code.

Such code may consume resources (such as CPU), reveal secure data (passwords etc) or format the hard-drives.

It is not possible to completely trust any third-party software including the browsers.

Client-side vulnerability becomes a bigger concern for a company who does business on the web, if the staff is allowed to surf the internet freely.

A good solution might be not allowing any web surfing on the server machine.

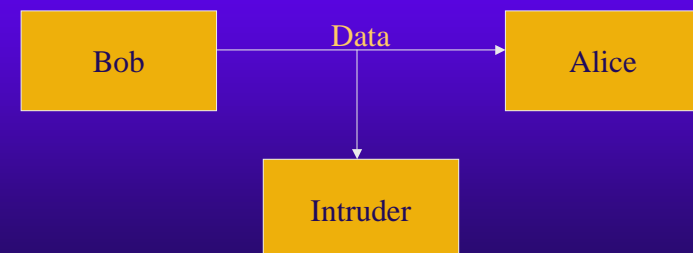
3



Securing the Data Transaction

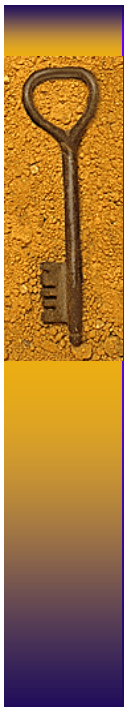
This is one of the greatest concerns in an e-commerce application, as the network itself cannot be trusted as a safe way of communicating.

Any information that is send from a machine to another machine over a network can be captured by intruders.




In order to understand this concept, we need to have a closer look in networks

4



How can two computers communicate with each other?

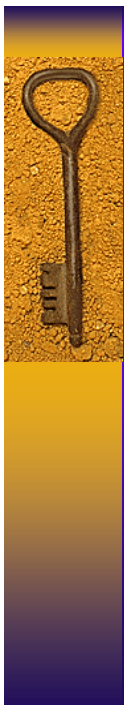
5



By using the same language!

That is they use a set of predefined **protocols** to communicate with each other.

6



The Philosophy Behind Networking


A network can be organized into the following major network elements:

- Physical Connections
- Protocols
- Applications

To determine the hierarchy between the network elements a **conceptual** framework called OSI (Open Systems Interconnect) Model was suggested by ISO in late 70s.

This framework has formed the key element of networking.

7



The OSI Model

The OSI Model is a recommended conceptual (abstract) mechanism that allows several applications to communicate with each other over the same network smoothly.

According to the OSI model a network can be thought as consisting of 7 layers. The lowest level is the physical layer which consists of actual wiring and electrical signals, and the highest level consists of applications such as www browsers and servers.

The system works analogous to the mail delivery system.

8



7 Layers of the OSI Model

1. Physical
2. Data Link
3. Network
4. Transport
5. Session
6. Presentation
7. Application



Physical Layer

(Postman)

This is the actual hardware part of the network consisting of wires, satellite communications equipment, electrical signals that carry bits of information.

The physical layer has no knowledge of the structure of the data transmitted. The responsibility of the physical layer is to transmit the data bits over the physical media using an appropriate signalling technique.



Data Link Layer

(The envelope)

Data link layer provides the secure transmission of data over the physical layer. The data is covered by some additional information such as addresses of communicating machines and error control information.



Network Layer

(Mail dispatch centers)

The network layer decides how to route the data *packets* and ensure that the transmission is established through the best possible route (routing), which can dynamically change.

This layer also allows two different networks (such as Token Ring and Ethernet) to be interconnected by using routers and a uniform network addressing mechanism (IP – IP Addresses).

(An IP address = NetID + HostID)



Transport Layer

(recorded mail)

This layer helps ensure reliable data delivery and end-to-end **data integrity**.

It may also be responsible for creating several logical connections over the same network connection (*multiplexing*).

Some well known protocols at this layer are:

TCP: Transmission Control Protocol

UDP: User Datagram Protocol

13



Session Layer

(secretary)

Session layer provides one or two way communications between applications. Among the enhancements provided by session layer are

- Dialog control
- Token management (only one side holds the token)
- Activity management

Session synchronisation is maintained using checkpoints.

The layers below this one are usually implemented as part of the hardware or the operating system. From this layer upwards, things are implemented by the networking software.

14



Presentation Layer

(translators)

This layer manages the way data is presented (ASCII, EBCDIC). Makes sure that a common language is used by different platforms.

ASN.1 (Abstract Syntax Representation, Rev 1) used by SNMP (Simple Network Management Protocol).

XDR (External Data Representation) used by NFS (Network File System).

(Many applications do not use this layer)

15



Application Layer

(the boss)

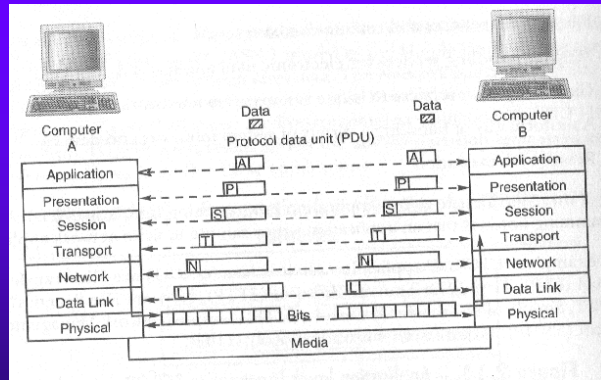
The application layer contains the protocols and functions needed by user applications to perform communication tasks, including:

- Protocols for providing remote file services (NFS, HTTP).
- File transfer services and remote database access (ftp).
- Message handling services (SMTP - e-mail)
- Remote job execution (telnet)
- Managing the network (SNMP)

Many of these services are called Application Programming Interfaces (APIs). APIs are programming libraries that an application writer can use to write network applications.

16

Data Traversal in the OSI Model



(peer-to-peer data communication)

How to send secure information through internet:

The layers below Session layer are considered as insecure and any information send through these layers can be intercepted.

Therefore the only way of securing the data transaction through internet is ciphering the information above Transport layer.

There are two main technologies in this direction:

- 1) SSL (Secure Sockets Layer)
- 2) S-HTTP (Secure HTTP)

SSL

SSL (provided by Netscape) works as a separate layer just on top of the transport layer (TCP layer).

Applications that use SSL will have the secure connection provided by it, the reliable delivery of packets provided by TCP, and the routing of packets provided by IP.

In order to use SSL, our web server should be SSL enabled.

Then all we need to do is use **https://** instead of **http://** in front of any web page addresses we want the content to be sent securely.

In theory, it is possible to have other network applications (such as telnet, ftp etc) that use SSL.

S-HTTP

S-HTTP is a secure extension of the HTTP.

Commercialised by Terisa Systems (www.terisa.com)

The security properties of a connection is negotiated between client and server during the initialisation of the connection.

The client or server may specify that a specific secure property is Required, Optional or Refused

Secure properties can include

- Message digests (such as sum checks)
- Nonrepudiation (Confirmation of the identity and information) (E.g. digital signatures can be required in some transactions)
- Type of technologies to be used (symmetric encryption, authentication etc)

How does it work?

Symmetric Encryption:

When a piece of confidential information has to be sent through an insecure media, the easiest and probably the best way is encrypting the data by using a shared secret.

```

    graph LR
      Bob[Bob "Hello"  
Shared secret: 12] -- "lgmnp" --> Alice["Hello" Alice  
Shared secret: 12]
      Intruder[Intruder]
      Bob -- "lgmnp" --> Intruder
  
```

Intruder cannot interpret the message intelligently.

21

Asymmetric (Public Key) Encryption

Unfortunately, in many cases two parties have never met before to share a secret.

Public Key Encryption can be used for these cases. Pretty Good Privacy (PGP) was one of the first applications that used this technology.

Here, using an algorithm and a secret password each party produce a pair of keys called *public key* and *private key*.

A message encrypted by one's public key can be decrypted only by that person's private key.

Therefore, parties first send their public keys to each other and then send messages using each other's public keys.

Even if the messages are intercepted, they cannot be decrypted by intruders.

22

```

    graph LR
      Bob["Hello" Bob] -- "lgmnp" --> Alice["Hello" Alice]
      Alice -- Alice's Public key --> Bob
      Alice -- Alice's private key --> Alice
      Intruder[Intruder]
      Bob -- "lgmnp" --> Intruder
  
```

The intruder cannot decrypt the message without the Alice's private key.

Using the same technology it is possible to digitally sign electronic documents:

```

    graph LR
      Bob["Hello" Bob] -- "lgmnp" --> Alice["Hello" Alice]
      Bob -- Bob's Private key --> Bob
      Bob -- Bob's public key --> Alice
      Intruder[Intruder]
      Bob -- "lgmnp" --> Intruder
  
```

Alice confirms that the message is sent by Bob. (Nonrepudiation)
The intruder cannot imitate Bob's messages without his private key.

23

In public key encryption method, there is the problem of sending the public key safely.

A really sophisticated intruder can intercept the public key exchanging and replace fake public keys:

```

    graph LR
      Bob["Hello" Bob] -- "lgmnp" --> Alice["Hello" Alice]
      Alice -- Alice's Private key --> Alice
      Alice -- Alice's Public key --> Alice
      Intruder["Hello" Intruder]
      Bob -- "lgmnp" --> Intruder
      Intruder -- "lgmnp" --> Alice
  
```

Bob thinks that Intruder's public key is actually Alice's public key.

24



In order to prevent this occurring, parties should find other ways of confirming the public keys (eg phoning etc).

In e-commerce applications usually digital certificate authorities are used to ensure that a message has been sent by a certain person or company.

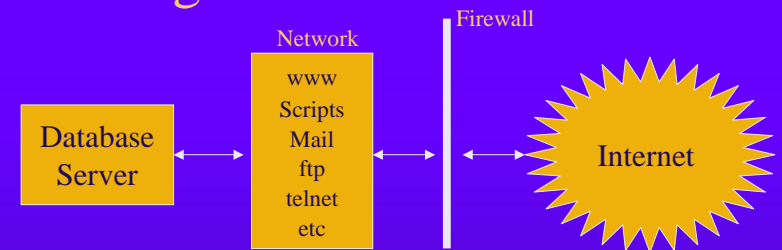
Digital certificate authorities are trusted authorities that can help authentication of servers. (Verisign etc.)

The certificate is not an approval of the content, but simply an endorsement of the identity of the website.

Note that disguises are still possible with digital certificates. (Any person could have certified his side as Microsoft before the real company has got the certificate).

History is full of disguise stories (including the famous ATM case).

Securing the Server



The best defence against web-based attacks is to know where you are vulnerable.

Often simple errors in configuring the server lead to the security holes. So the first thing to do is to check how your web server is configured.

Testing is the best way to detect errors and vulnerabilities.



File Access Permissions

File access permissions specify who can read, write or execute a file from the operating system's perspective.

It is important to set these right to have a secure system.

All the configuration files, the log files, CGI program sources and executables, and administrative files and programs should have correct file access permissions.

User's outside the Web server's group should not have read or write permissions to any files in the server root.

A secure approach is to restrict everything to a minimum and give permissions as necessary.

Ports

The connections to a computer is done via ports.

There are 65536 ports available.

Ports numbered from 0 to 1023 are reserved for privileged network services.

When installing the web server you can select which port is to be used by the web server. Usually port 80 is used by the http connections and port 443 is used for SSL connections.

Using a non-standard port could be safe but users must know it. For example, if the server uses port 8080 we would use `http://www.server.com:8080` in order to reach it.

It is possible to disallow any unused ports by the help of firewalls. This will be a good precaution against **Trojan horses**.



Accessing Sensitive Documents

Some documents on the server are required to be accessed only by authorised people. Three mechanisms can be used for this purpose:



Server Side Scripts

Server-side scripts play an important role in securing the e-commerce server.

It is easy to write powerful programs using scripting languages. This, however, means it is easy to write destructive programs with these.

The risks that server-side scripts pose:

- Read, replace, modify, remove files.
- Mail files back over the internet.
- Execute programs on the server.
- Launch a denial of service attack by overloading the CPU.



Escalating Client Privilege

Probably the most egregious error in configuring the Web server is to set the execution privilege of the Web server processes, which handle Web requests, to the super user privilege level.

Privilege escalation occurs when an unauthorised user is able to obtain higher privilege in accessing files on the server file system than that would normally be permitted.



Accessing Sensitive Documents

1. *Client hostname and IP address restrictions.* (A good idea is to check domain name against IP address through a reverse DNS look-up). **It is possible to spoof an IP address.**
2. User and password authentication. (Storing usernames and encrypted passwords in a database). Some servers provide Access Control Lists (ACL) to determine the permissions given for each user. **Some users may pick easy to guess passwords.** (use SSL for authentication).
3. Using Digital Certificates. SSL can be configured to authenticate both the Web server and the client. The problem here is that each client is required to have a digital certificate.