CHAPTER 17

Web Security

Web Security Consideration

The world wide web is fundamentally a client/server application running over the Internet and TCP/IP intranets.

1. Unlike traditional publishing environments, the web is vulnerable to attacks on the web servers over the Internet.

2. Corporate reputations can be damaged and money can be lost if the web servers are subverted.

3. The underlying software may hide many potential security flaws.

4. Once the web server is subverted, an attacker may be able to gain access to data and systems not part of the web itself but connected to the server at the local site,

5. Common and untrained users are not necessarily aware of the security risks that exist and do not have the tools or knowledge to take effective countermeasures.

Comparison of Threats on the Web

	Threats	Consequences	Countermeasures
Integrity	• Modification of user data. • Trojan horse browser. • Modification of memory. • Modification of message traffic in transit.	• Loss of information. • Compromise of machine • Vulnerability to all other threats.	Cryptographic checksums.
Confidentiality	• Eavesdropping on the net. • Theft of info from server. • Theft of data from client. • Info about network configuration. • Info about which client talks to server.	• Loss of information. • Loss of privacy.	Encryption, Web proxies.
Denial of Service	• Killing of user threads. • Flooding machine with bogus threats. • Filling up disk or memory. • Isolating machine by DNS attacks.	• Disruptive. • Annoying. • Prevent user from getting work done.	Difficult to prevent.
Authentication	• Impersonation of legitimate users. • Data forgery.	• Misrepresentation of user. • Belief that false information is valid.	Cryptographic techniques.

Web Security Threats

- Table on the previous slide shown summary of the types of security threats faced in using the web.
- These can be grouped as passive and active attacks.
- Passive attacks include eavesdropping on network traffic between browser and server and gaining access to information on a web site that is supposed to be restricted.
- Active attacks include impersonating another user, altering messages in transit between client and server, and altering information on a web site.
- Another way to classify web security threats is in terms of the location of the threat: Web server, Web browser, and network traffic between browser and server.
- Issues of server and browser security is fall into the category of computer system security.
- Issues of traffic security fall into the category of network security.

Web Traffic Security Approaches

A number of approaches to providing web security are possible.

1. One way is to use IP security (figure a).
   a. The advantage is that It is transparent to end users and applications.
   b. Further, IPSec includes a filtering capability so that only selected traffic need to incur the overhead of IPSec processing.
2. Another is to implement security just above TCP (figure b).
   a. The foremost example of this approach is the Secure Socket Layer (SSL) and the follow-on Internet standard known as Transport Layer Security (TLS).
   b. SSL (or TLS) could be provided as part of the underlying protocol suite and therefore be transparent to applications.
   c. Alternatively SSL could be embedded in specific packages.
   d. For example, Netscape and Microsoft explorer browsers come equipped with SSL, and most web servers have implemented the protocol.

Web Traffic Security Continue…

3. Application specific security services are embedded within the particular application (figure c).
   a. The advantage is that the service can be tailored to the specific needs of a given application.

   b. In the context of web security, an important example of this approach is Secure Electronic Transaction (SET).

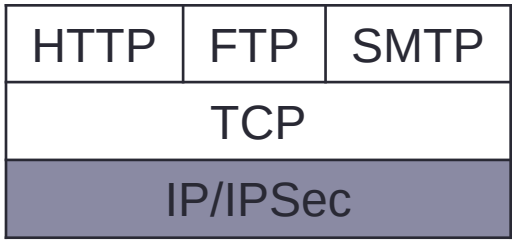

Figure a: Network level

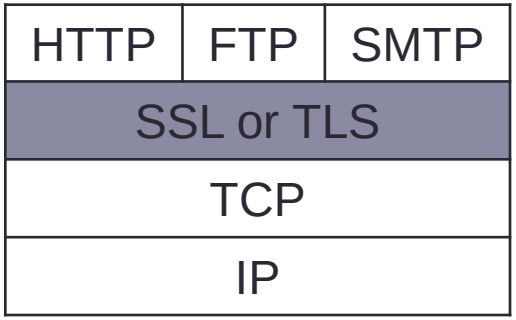

Figure b: Transport layer

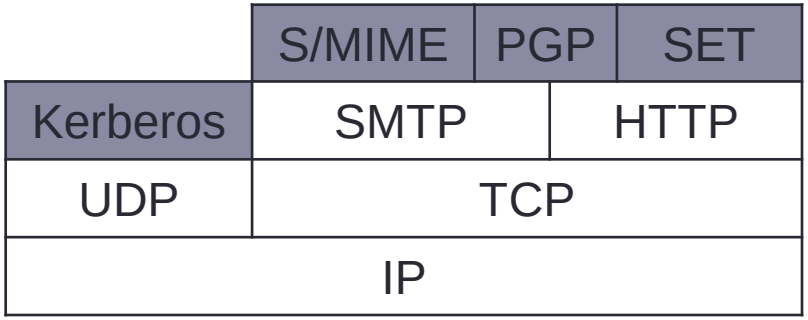

Figure c: Application level