Web Security

- Chapter 6

Learning Objectives

- Understand SSL/TLS protocols and their implementation on the Internet
- Understand HTTPS protocol as it relates to SSL
- Explore common uses of instant messaging applications and identify vulnerabilities associated with those applications

continued…

Learning Objectives

- Understand the vulnerabilities of JavaScript, buffer overflow, ActiveX, cookies, CGI, applets, SMTP relay, and how they are commonly exploited

Secure Sockets Layer (SSL) and Transport Layer Security (TLS)

- Commonly used protocols for managing the security of a message transmission across the “insecure” Internet

Secure Sockets Layer (SSL)

- Developed by Netscape for transmitting private documents via the Internet
- Uses a public key to encrypt data that is transferred over the SSL connection
- URLs that require an SSL connection start with “https:” instead of “http:”

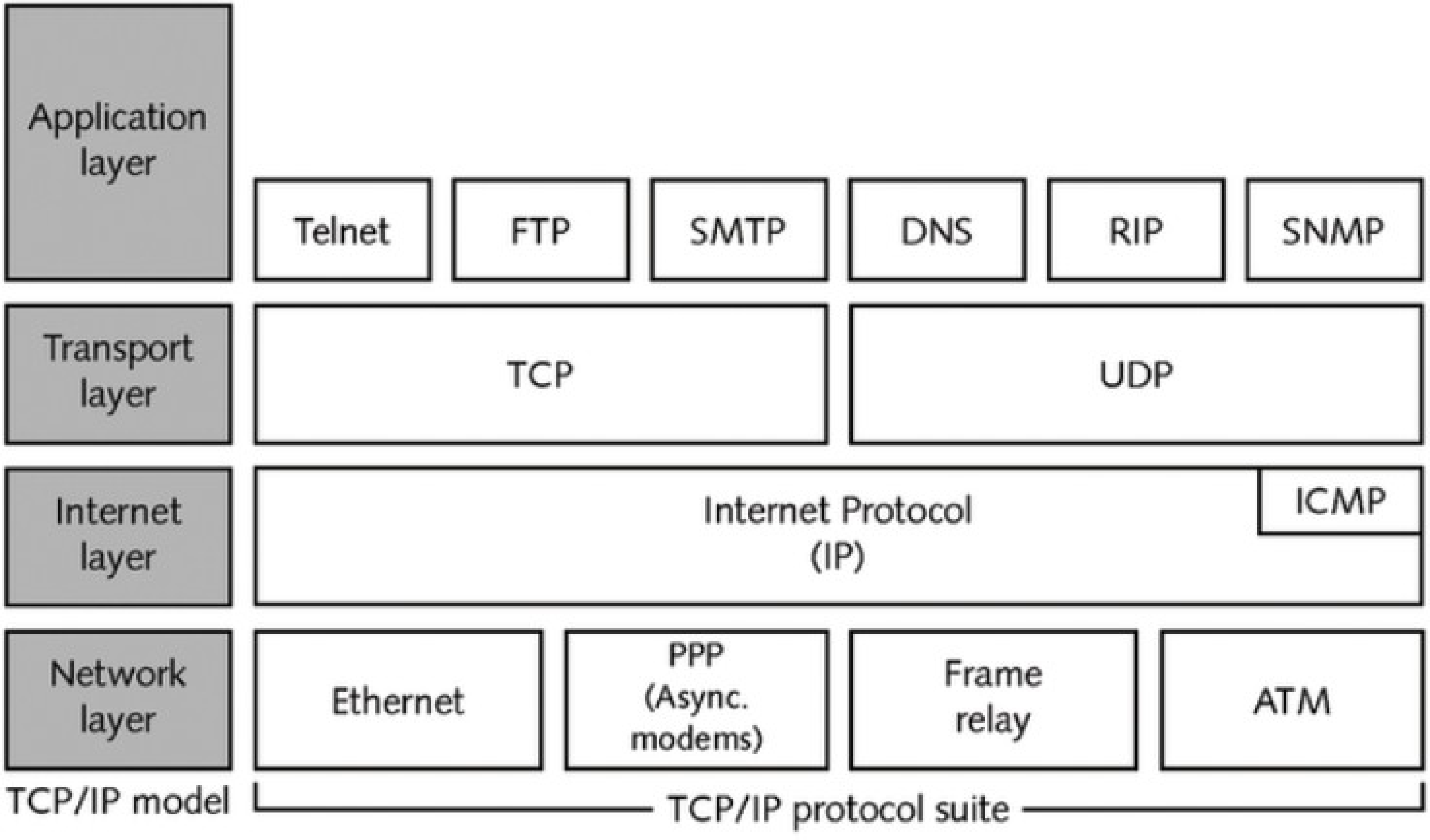
Transport Layer Security (TLS)

- Latest version of SSL
- Not as widely available in browsers

SSL/TLS Protocol

- Runs on top of the TCP and below higher-level protocols
- Uses TCP/IP on behalf of higher-level protocols
- Allows SSL-enabled server to authenticate itself to SSL-enabled client
- Allows client to authenticate itself to server
- Allows both machines to establish an encrypted connection

Secure Sockets Layer Protocol



Application layer	Telnet	FTP	SMTP	DNS	RIP	SNMP
Transport layer	TCP			UDP		
Internet layer	Internet Protocol (IP)					ICMP
Network layer	Ethernet	PPP (Async. modems)	Frame relay	ATM		
TCP/IP model	TCP/IP protocol suite					

Figure 6-1 Secure Sockets Layer protocol

SSL/TLS Protocol

- Uses ciphers to enable encryption of data between two parties
- Uses digital certificates to enable authentication of the parties involved in a secure transaction

Cipher Types Used by SSL/TLS

- Asymmetric encryption (public key encryption)
- Symmetric encryption (secret key encryption)

Digital Certificates

- Components
  - Certificate user’s name
  - Entity for whom certificate is being issued
  - Public key of the subject
  - Time stamp
- Typically issued by a CA that acts as a trusted third party
  - Public certificate authorities
  - Private certificate authorities

Secure Hypertext Transfer Protocol (HTTPS)

- Communications protocol designed to transfer encrypted information between computers over the World Wide Web
- An implementation of HTTP
- Often used to enable online purchasing or exchange of private information over insecure networks
- Combines with SSL to enable secure communication between a client and a server

Instant Messaging (IM)

- Communications service that enables creation of a private chat room with another individual
- Based on client/server architecture
- Typically alerts you whenever someone on your private list is online
- Categorized as enterprise IM or consumer IM systems
- Examples: AOL Instant Messenger, ICQ, NetMessenger, Yahoo! Messenger

IM Security Issues

- Cannot prevent transportation of files that contain viruses and Trojan horses
- Misconfigured file sharing can provide access to sensitive or confidential data
- Lack of encryption
- Could be utilized for transportation of copyrighted material; potential for substantial legal consequences
- Transferring files reveals network addresses of hosts; could be used for Denial-of-Service attack

IM Applications

- Do not use well-known TCP ports for communication and file transfers; use registered ports
- Ports can be filtered to restrict certain functionalities or prevent usage altogether

Vulnerabilities of Web Tools

- Security of Web applications and online services is as important as intended functionality
  - JavaScript
  - ActiveX
  - Buffers
  - Cookies
  - Signed applets
  - Common Gateway Interface (CGI)
  - Simple Mail Transfer Protocol (SMTP) relay

JavaScript

- Scripting language developed by Netscape to enable Web authors to design interactive sites
- Code is typically embedded into an HTML document and placed between the <head> and </head> tags
- Programs can perform tasks outside user’s control

JavaScript Security Loopholes

- Monitoring Web browsing
- Reading password and other system files
- Reading browser’s preferences

ActiveX

- Loosely defined set of technologies developed by Microsoft
  - Outgrowth of OLE (Object Linking and Embedding) and COM (Component Object Model)
- Provides tools for linking desktop applications to WWW content
- Utilizes embedded Visual Basic code that can compromise integrity, availability,and confidentiality of a target system

Buffer

- Temporary storage area, usually in RAM
- Acts as a holding area, enabling the CPU to manipulate data before transferring it to a device

Buffer Overflow Attacks

- Triggered by sending large amounts of data that exceeds capacity of receiving application within a given field
- Take advantage of poor application programming that does not check size of input field
- Not easy to coordinate; prerequisites:
  - Place necessary code into program’s address space
  - Direct application to read and execute embedded code through effective manipulation of registers and memory of system

Cookies

- Messages given to Web browsers by Web servers
  - Browser stores message in a text file
  - Message is sent back to server each time browser requests a page from server
- Verify a user’s session
- Designed to enhance browsing experience

Vulnerabilities of Cookies

- Contain tools that are easily exploited to provide information about users without consent
  - Attacker convinces user to follow malicious hyperlink to targeted server to obtain the cookie through error handling process on the server
  - User must be logged on during time of attack
- To guard against EHE attacks
  - Do not return unescaped data back to user
  - Do not echo 404 file requests back to user

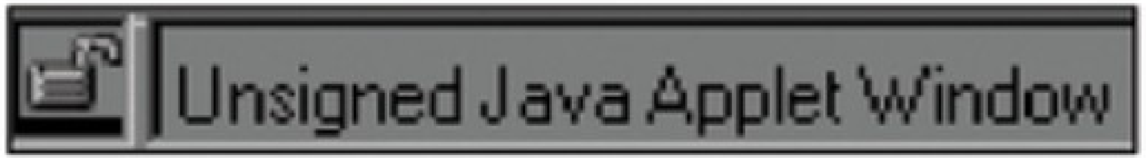
Java Applets

- Internet applications (written in Java programming language) that can operate on most client hardware and software platforms
- Stored on Web servers from where they can be downloaded onto clients when first accessed
- With subsequent server access, the applet is already cached on the client and can be executed with no download delay

Signed Applets

- Technique of adding a digital signature to an applet to prove that it came unaltered from a particular trusted source
- Can be given more privileges than ordinary applets
- Unsigned applets are subject to sandbox restrictions

Unsigned Applets



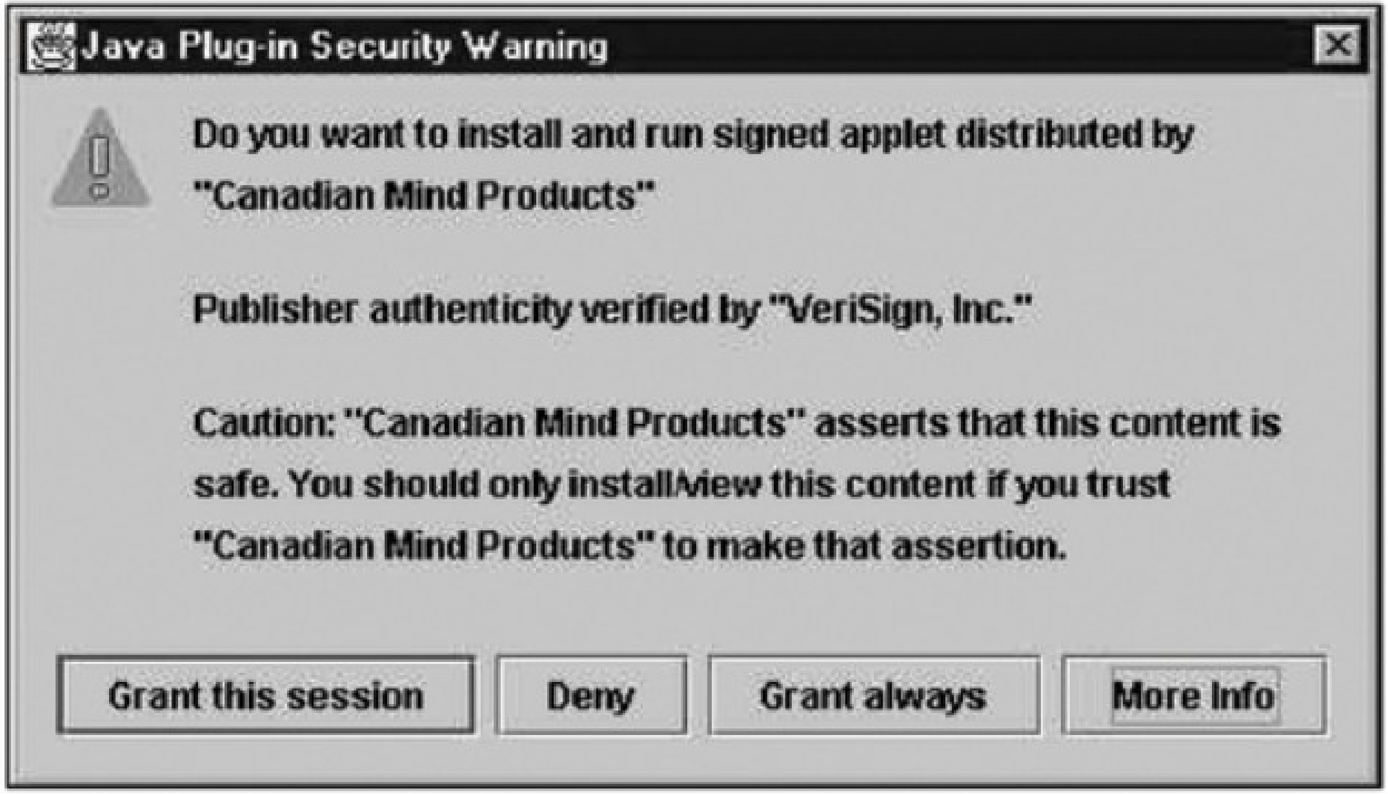
Unsigned Java Applet Window

Figure 6-3 Unsigned applet warning message

Sandbox Model

- Prevent the applet from:
  - Performing required operations on local system resources
  - Connecting to any Web site except the site from which the applet was loaded
  - Accessing client’s local printer
  - Accessing client’s system clipboard and properties

Signed Applets



Java Plug-in Security Warning

Do you want to install and run signed applet distributed by "Canadian Mind Products"

Publisher authenticity verified by "VeriSign, Inc."

Caution: "Canadian Mind Products" asserts that this content is safe. You should only install/view this content if you trust "Canadian Mind Products" to make that assertion.

Figure 6-4 Security message confirming consent

Reasons for Using Code Signing Features

- To release the application from sandbox restrictions imposed on unsigned code
- To provide confirmation regarding source of the applications code

Common Gateway Interface (CGI)

- Interface specification that allows communication between client programs and Web servers that understand HTTP
- Uses TCP/IP
- Can be written in any programming language
- Parts of a CGI script
  - Executable program on the server (the script itself)
  - HTML page that feeds input to the executable

Typical Form Submission

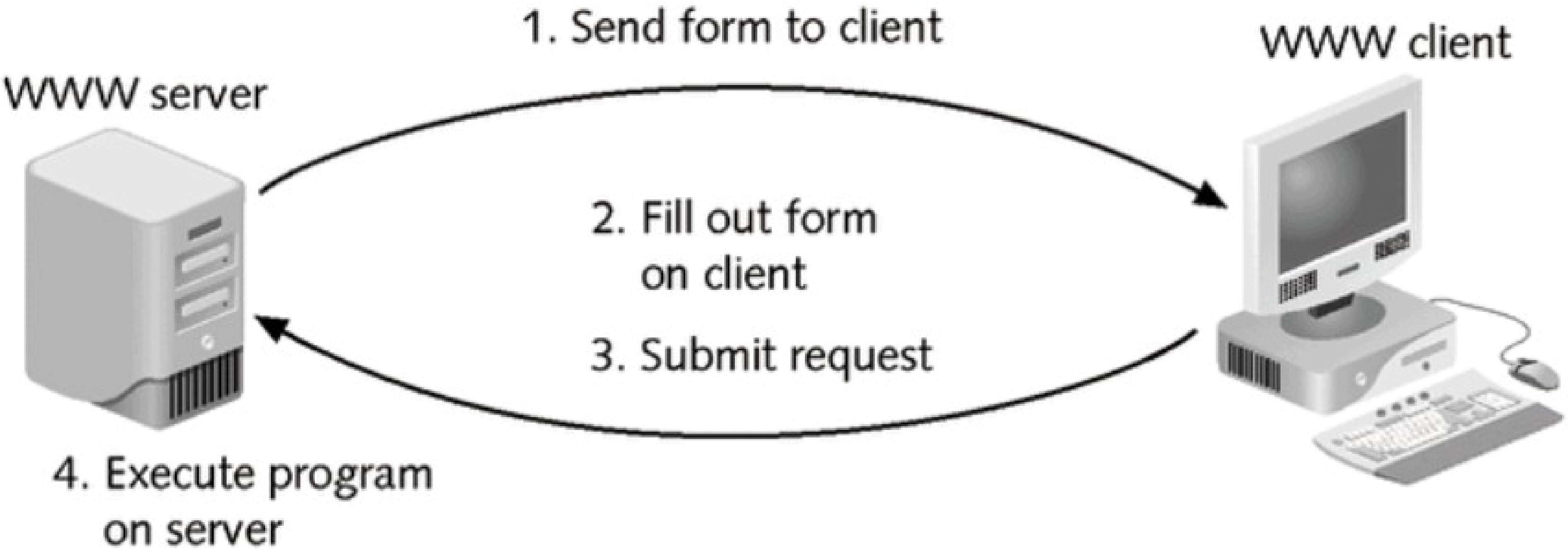


Figure 6-5 CGI

CGI

- Interactive nature leads to security loopholes
  - Allowing input from other systems to a program that runs on a local server exposes the system to potential security hazards

Precautions to Take When Running Scripts on a Server

- Deploy IDS, access list filtering, and screening on the border of the network
- Design and code applications to check size and content of input received from clients
- Create different user groups with different permissions; restrict access to hierarchical file system based on those groups
- Validate security of a prewritten script before deploying it in your production environment

Simple Mail Transfer Protocol (SMTP)

- Standard Internet protocol for global e-mail communications
- Transaction takes place between two SMTP servers
- Designed as a simple protocol
  - Easy to understand and troubleshoot
  - Easily exploited by malicious users

Vulnerabilities of SMTP Relay

- Spam via SMTP relay can lead to:
  - Loss of bandwidth
  - Hijacked mail servers that may no longer be able to serve their legitimate purpose
- Mail servers of innocent organizations can be subject to blacklisting

Chapter Summary

- Protocols commonly implemented for secure message transmissions
  - Secure Socket Layer
  - Transport Layer Security
- Data encryption across the Internet through Secure Hyper Text Transfer Protocol in relation to SSL/TSL

continued…

Chapter Summary

- Instant Messaging
  - Common uses
  - Vulnerabilities
- Well-known vulnerabilities associated with web development tools