COURSE TECHNOLOGY
CENGAGE Learning™

Guide to Network Security
1st Edition

Chapter Eight
Security of Web Applications

Objectives

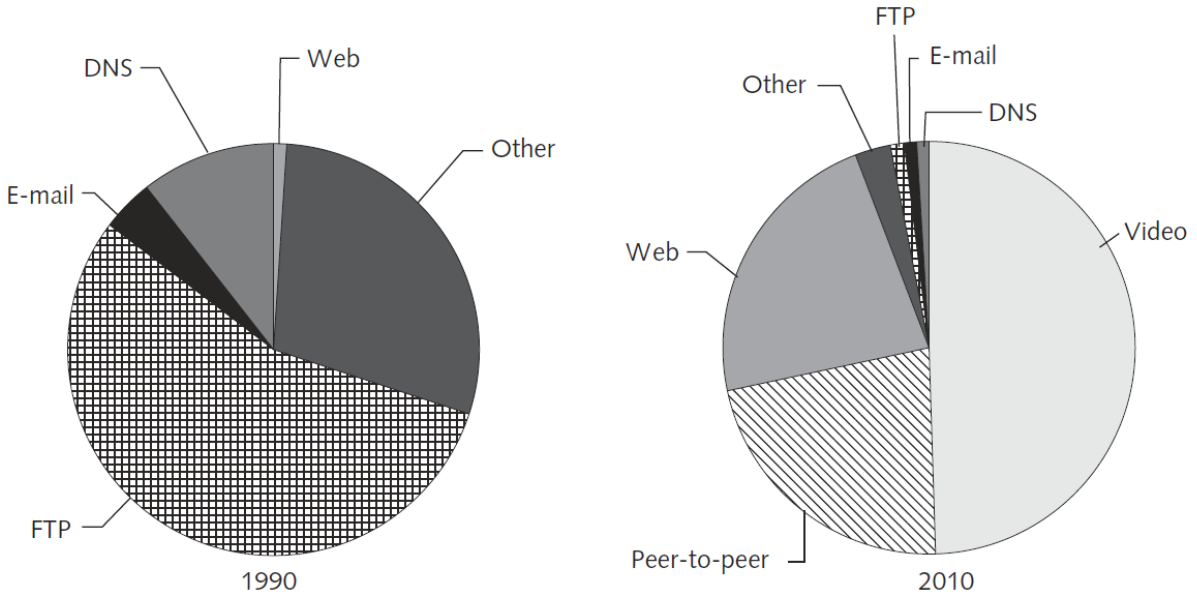
- List the various Internet services in use
- Identify threats to Internet services and basic countermeasures
- Describe the basics of Web client-server communication
- Identify the various Web languages and describe their uses
- Identify various Web threats and attacks
- Discuss the steps necessary to secure a Web server

Introduction

- Internet
  - Physical set of networks
  - Many services available
- World Wide Web
  - Set of applications running on top of the Internet
  - Documents linked via HTTP
- Majority of Internet attacks aimed at Web applications

Internet Services

- Components of Internet security
  - Securing Web sites
  - Securing various services that use the interconnected networks



Internet traffic 1990 to 2010					
	1990	1995	2000	2005	2010
Video	0%	0%	1%	8%	51%
Peer-to-peer	0%	0%	23%	42%	23%
Web	1%	40%	54%	40%	23%
Other (Telnet, newsgroups, etc.)	30%	31%	12%	11%	3%
FTP	57%	24%	9%	1%	1%
E-mail	4%	3%	2%	1%	1%
DNS	11%	1%	1%	1%	1%

Figure 8-1 Overall Internet usage by service

SMTP, POP, and IMAP

- Simple Mail Transfer Protocol (SMTP)
  - Used to send Internet mail
- Post Office Protocol 3 (POP3) and Internet Message Access Protocol (IMAP)
  - Used to receive Internet mail
- Protocols operate within Application layer of the OSI reference model

Service	Function	TCP Port	UDP Port	RFC Number
SMTP	Sending Internet mail	25	25	RFC 2821
POP3	Receiving Internet mail	110	110	RFC 1939
IMAP	Receiving Internet mail	143	143	RFC 1203
FTP	Transferring files	21 – command 20 – data	NA	RFC 959
TFTP	Transferring files	NA	69	RFC 1350
Telnet	Remote system administration	23	NA	RFC 854
DNS	Translating domain names into IP addresses	53	53	RFC 1035
SNMP	Network monitoring	161, 162	161, 162	RFC 1157
LDAP	Directory services	389	389	RFC 2251
NNTP	Newsgroup information	119	NA	RFC 977

Table 8-1 Quick reference guide for some of the most common Internet services

SMTP, POP, and IMAP (cont'd.)

- Attacks on E-mail
  - Attacker uses e-mail server to send messages:
    - From the victim organization
- SMTP initially had no way of authenticating users
- ESMTP protocol introduced SMTP-AUTH feature
- Open relay
  - Attackers look for unrestricted SMTP servers
- Mail bombing
  - E-mail based denial of service attack

SMTP, POP, and IMAP (cont'd.)

- Security solutions
  - Restrict mail relayed on the e-mail server
  - Test server configuration to be sure it is not set up as open relay
  - Use real-time blacklisting
  - Authenticate on POP before allowing mail sent through SMTP server

FTP

- File Transfer Protocol (FTP)
  - Simple method of transferring files between computer systems
  - Operates in the Application layer of the OSI reference model
  - Requires two TCP ports for communications
    - Command port and data port
  - Can operate in active or passive mode

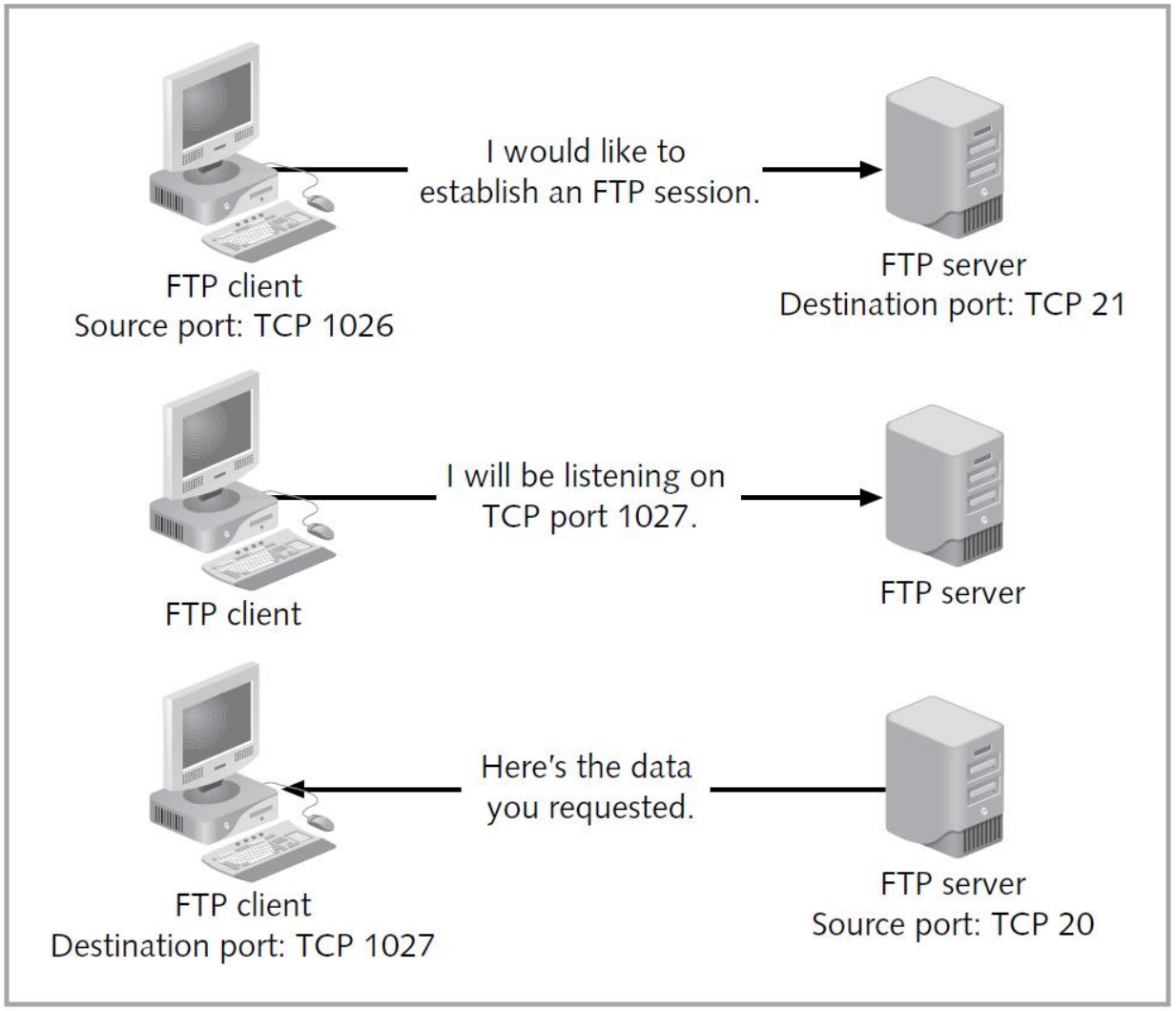


Figure 8-3 Example of FTP session established in active mode

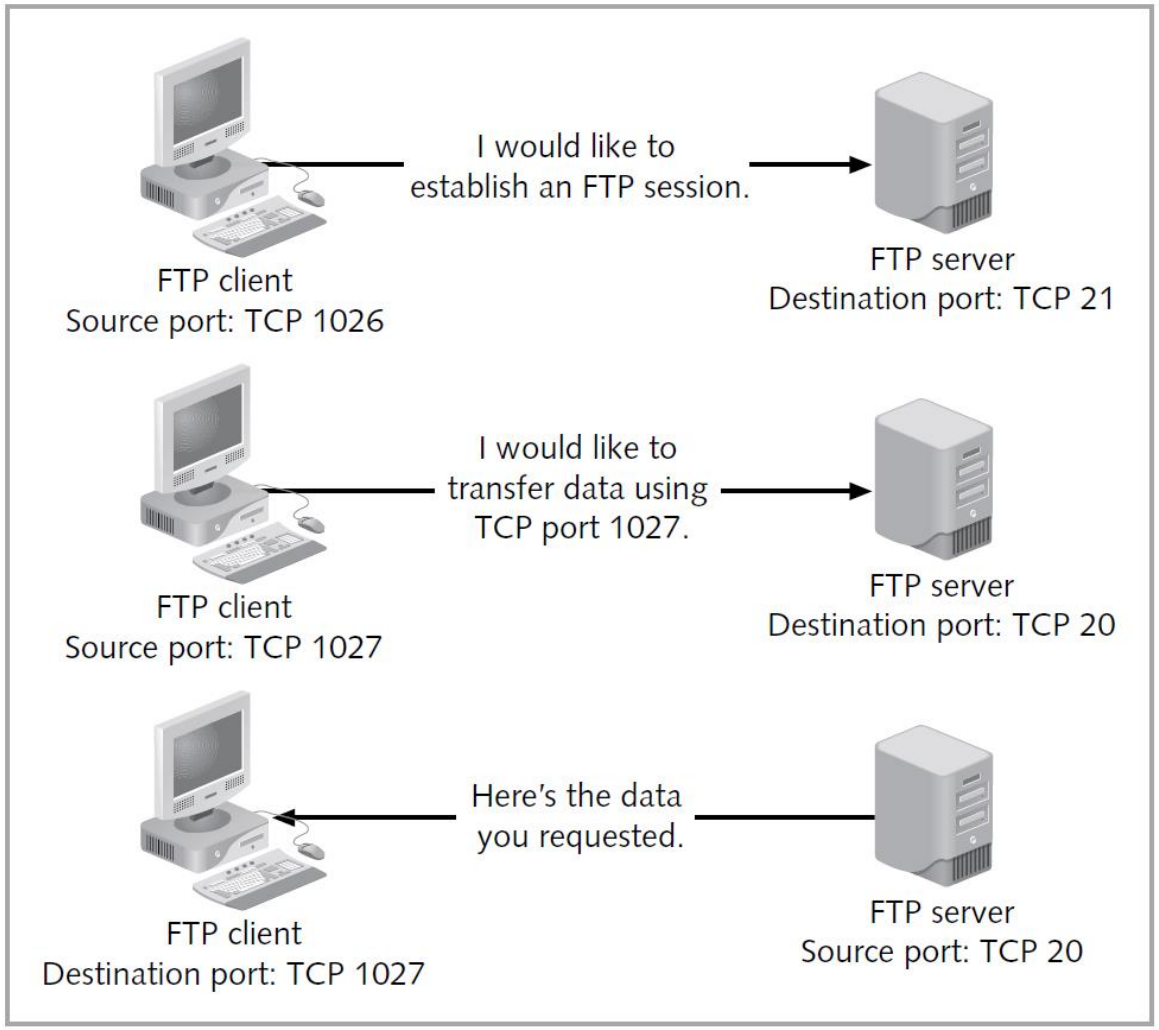


Figure 8-4 Example of FTP session established in passive mode

FTP (cont'd.)

- Trivial File Transfer Protocol (TFTP)
  - Used to transfer data files
  - Fewer features than FTP
  - Uses only one port
  - Used most often on network appliances
    - To transfer configuration files, backups, and boot files
- Attacks on FTP and TFTP
  - Server can be set up with anonymous FTP access
    - Problematic if anonymous user given too many rights
  - Weakness: TFTP does not allow authentication

FTP (cont'd.)

- Security solutions
  - Best option: not enable FTP or TFTP server
  - Use encryption and authentication
  - Avoid anonymous FTP
- Secure substitute methods of transferring files
  - FTP over SSL
  - Secure Copy (SCP)

Telnet

- Application-layer protocol for connecting to a remote computer
- Users connect a remote shell to run programs, view files, and perform other actions:
  - As if using the system locally
- Attacks on Telnet
  - Misconfigured or poorly administered servers vulnerable
  - Telnet traffic sent unencrypted over the network

Telnet (cont'd.)

- Security solutions
  - Best practice: do not use Telnet
    - Secure Shell or other tool that uses encryption a better choice
  - All users should have appropriate rights and strong passwords
  - Avoid having the server available to the Internet
  - Have external users attach using a VPN

SNMP

- Simple Network Management Protocol (SNMP)
  - Application layer management protocol
  - Used to monitor status and performance of network devices and systems
- SNMP agent installed on desired host or network device
- Management information base
  - Translates information sent from agents
- Trap
  - Status information message about monitored device

SNMP (cont'd.)

- Attacks on SNMP
  - Most weaknesses occur with SNMP version 1
    - Uses only simple authentication
    - Sends data over network in plaintext
- Security solutions
  - Upgrade SNMP to a newer version (e.g., v3)
  - Do not connect SNMP-enabled systems to the Internet

LDAP

- Lightweight Directory Access Protocol (LDAP)
  - Provides a communication framework with centralized directories
  - Example use: central database of users, user rights, and user properties
- LDAP protocol standard operations
  - Authenticating to the directory
  - Searching the directory
  - Reading attributes from the directory

LDAP (cont'd.)

- LDAP protocol standard operations (cont'd.)
  - Adding entries to the directory
  - Modifying entries in the directory
  - Removing entries from the directory
- Attacks on LDAP
  - Most common attacks similar to SQL injection attacks
- Security solutions
  - Protect servers with physical security, user ID management, and rights management

LDAP (cont'd.)

- Security solutions (cont'd.)
  - Input validation
    - Scrub incoming data to pass only valid information to LDAP server

NNTP

- Network News Transfer Protocol (NNTP)
  - Designed to facilitate newsgroup communications
  - Similar to SMTP in architecture and function
- Clients use a newsgroup client to connect via NNTP
  - Central newsgroup server used to download and post messages
- Attacks on NNTP
  - Usenet groups and forums may have links to malicious Web sites or files

NNTP (cont'd.)

- Security solutions
  - Ensure NNTP servers are patched regularly
  - Scan newsgroup content for malware
  - Implement user authentication when possible

DNS

- Domain Name System (DNS)
  - Service that translates domain name into IP address
  - Operates within the Application layer
  - Allows clients to access various DNS servers to perform the translation
  - Information store is distributed
- DNS overview
  - Operations split among three components
    - DNS servers, DNS protocol, and DNS clients (resolvers)

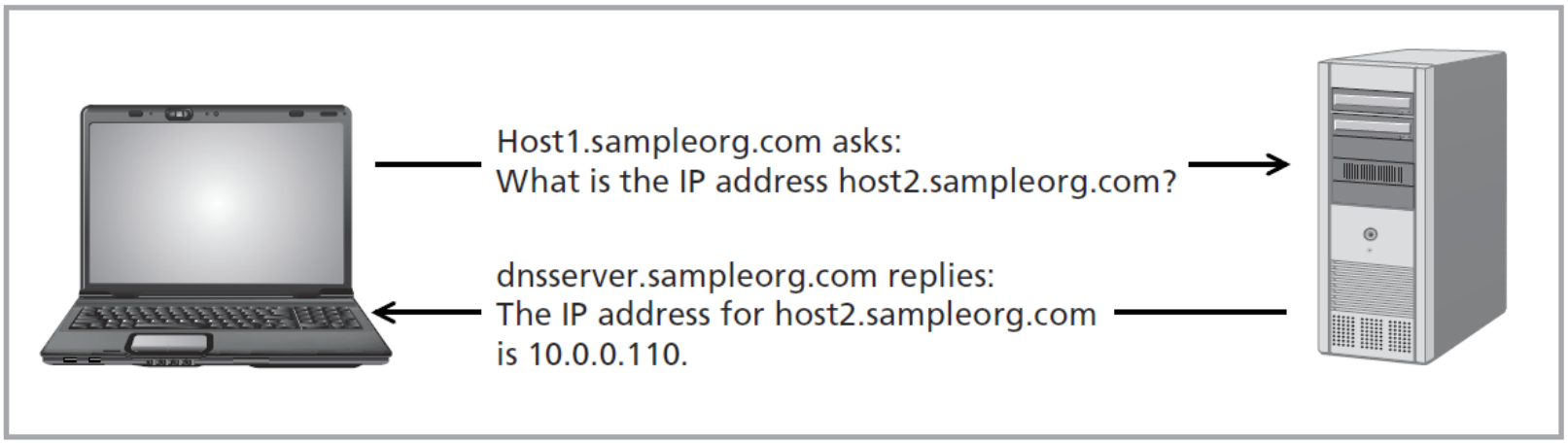


Figure 8-8 Typical DNS query confined to a local organization

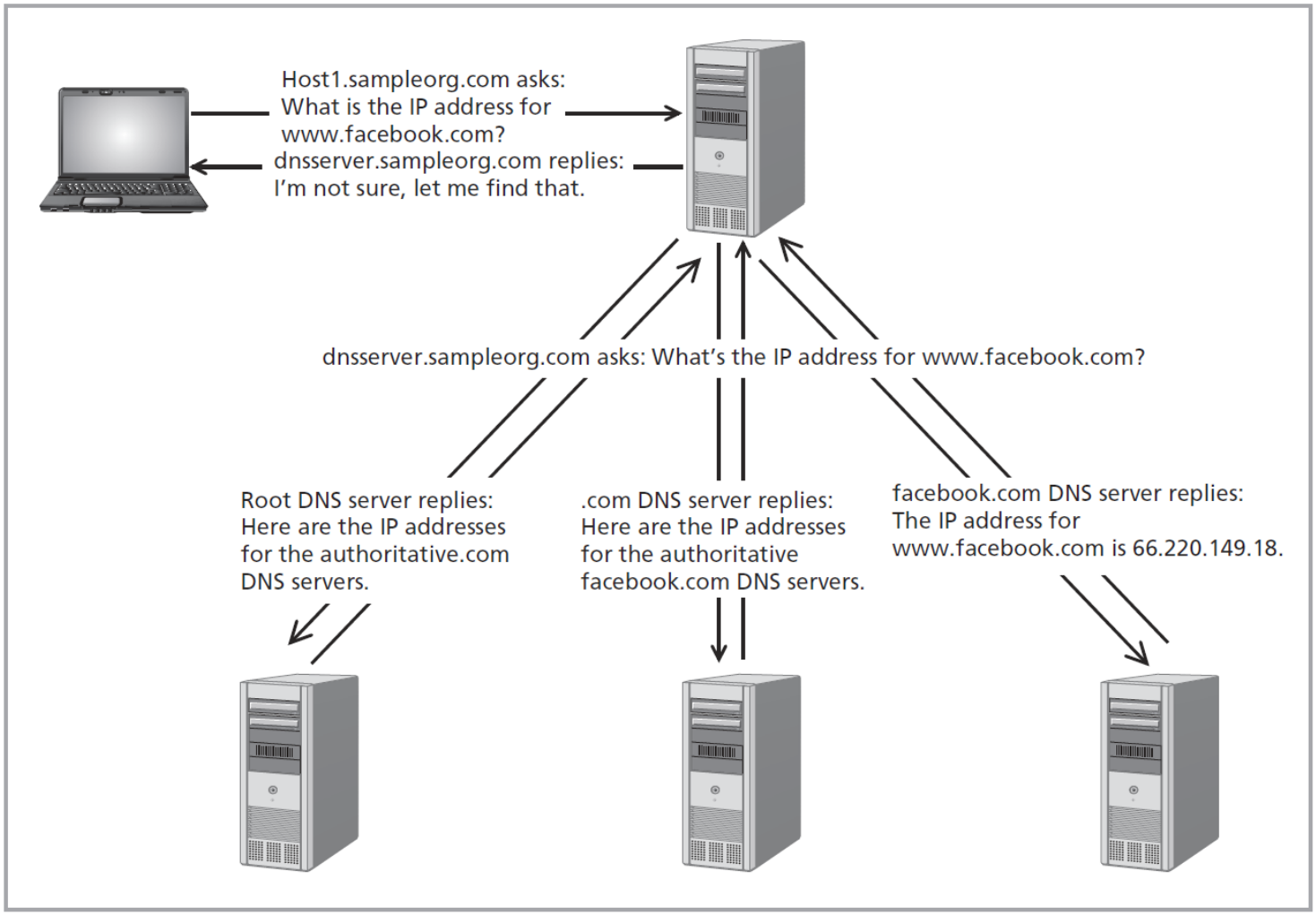


Figure 8-9 Typical DNS query for a public Internet system (iterative query)

DNS (cont'd.)

- Fully qualified domain name
  - Uniquely identifies a host
  - Represents host name, subdomain, second-level domain, and top-level domain
  - Example mailserver1.mail.sampleorg.com
- Top-level domains managed by Internet Assigned Numbers Authority (IANA)

TYPE	Value
A	Host address
NS	Authoritative name server
CNAME	Canonical name for an alias
SOA	Marks the start of a zone of authority
MX	Mail exchange

Table 8-2 DNS record types

DNS (cont'd.)

- DNS zones
  - Divide responsibility among various DNS servers
- Attacks on DNS
  - DNS open resolver
  - DNS poisoning
  - DNS denial-of-service attack

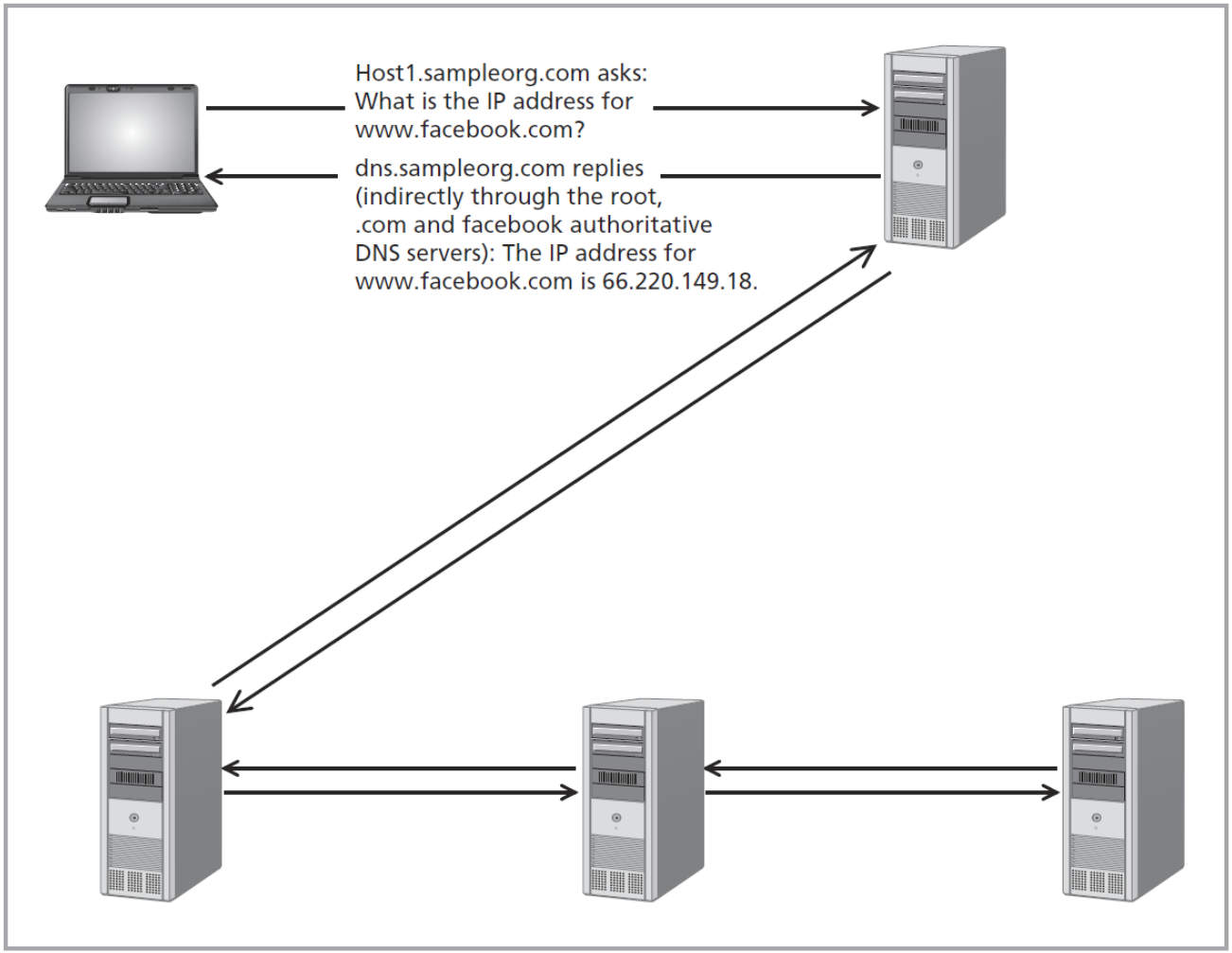


Figure 8-10 DNS query using recursive queries
© *Cengage Learning 2013*

DNS (cont'd.)

- Security solutions
  - Secure DNS servers and update software regularly
  - Block incoming DNS traffic
  - Limit zone transfers to trusted IP addresses
  - Digitally sign information using Domain Name System Security Extensions
  - Disable recursive query ability

Web Overview

- Web
  - HTTP-driven content transmitted over the Internet
- Web Client/Server Architecture
  - Server
  - Client
  - Communication protocol

Web Client/Server Architecture

- Web server requirements
  - Connect system to the Internet or internal network
  - Install Web server software
  - Have content to share
  - Allow incoming connections
- Web client
  - Web browser
  - Command-line clients

Web Client/Server Architecture (cont'd.)

- HTTP communication
  - Basis for Web communication
  - Consists of requests and responses

Request Method	Use
OPTIONS	Allows a client to identify the various communication options available
GET	Retrieves information from the resource signified by the Uniform Resource Identifier (URI)
HEAD	Retrieves meta-information only from the resource signified in the URI
POST	Used to send information to the Web server; the actual action varies, depending on the server functions offered
PUT	A request to store information at the specified URI
DELETE	Removes the resource specified in the URI
TRACE	A troubleshooting request that tells the Web server to mirror the request for viewing

Table 8-3 Common HTTP request methods
© Cengage Learning 2013

Common Codes	Response Status Code Family	Description
100 Continue	100s: Informational	The server has sent a provisional response that consists of a status and optional headers.
200 OK	200s: Success	The server successfully processed the request.
300 Multiple Choices 301 Moved Permanently 302 Found 304 Not Modified	300s: Redirection	The client must take further action to fulfill the request.
400 Bad Request 401 Unauthorized 403 Forbidden 404 Not Found 410 Gone	400s: Client Error	An error has occurred on the client side.
500 Internal Server Error 501 Not Implemented 503 Service Unavailable 504 Gateway Timeout 505 HTTP Version Not Supported	500s: Server Error	An error has occurred on the server side.

Table 8-4 Common HTTP response codes

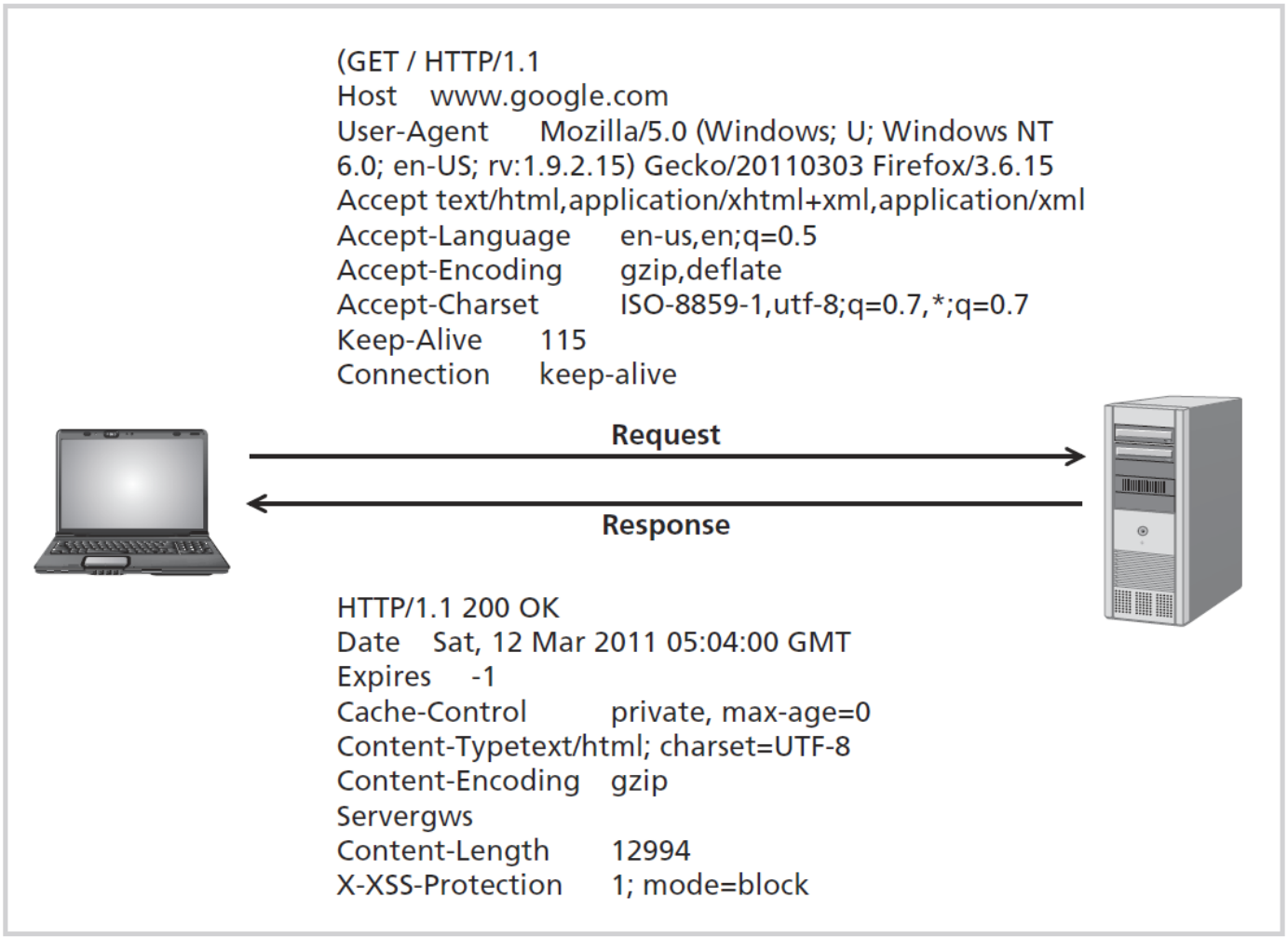


Figure 8-11 Typical HTTP request and response exchange
© Cengage Learning 2013

Web Programming Languages

- HTML
  - Works with HTTP to move content from servers to clients
  - Uses tags to tell browsers how to format content
  - Versions include HTML 1.0 to HTML 5
- CSS
  - Standardizes HTML formatting for an entire Web site
- XML
  - Allows developers to define their own tags

Web Programming Languages (cont'd.)

- CGI
  - Application programming interface
  - Allows external programs or scripts to interact with a Web server
- Perl
  - Programming language developed in 1987
  - Provides more robust scripting capability for UNIX
  - Strength: text-manipulation

Web Programming Languages (cont'd.)

- PHP
  - Allows developers to create dynamically generated HTML content
  - Interpreted on the server side prior to content being delivered to the user
- Javascript
  - Developed in 1995
  - Code interpreted on the client side
    - Instead of on the Web server

Web Programming Languages (cont'd.)

- AJAX
  - New use of existing technologies
  - Several mini-requests from client to server make content seem dynamic
  - See Figure 8-14 for example exchange
- Other languages
  - Ruby
  - Python

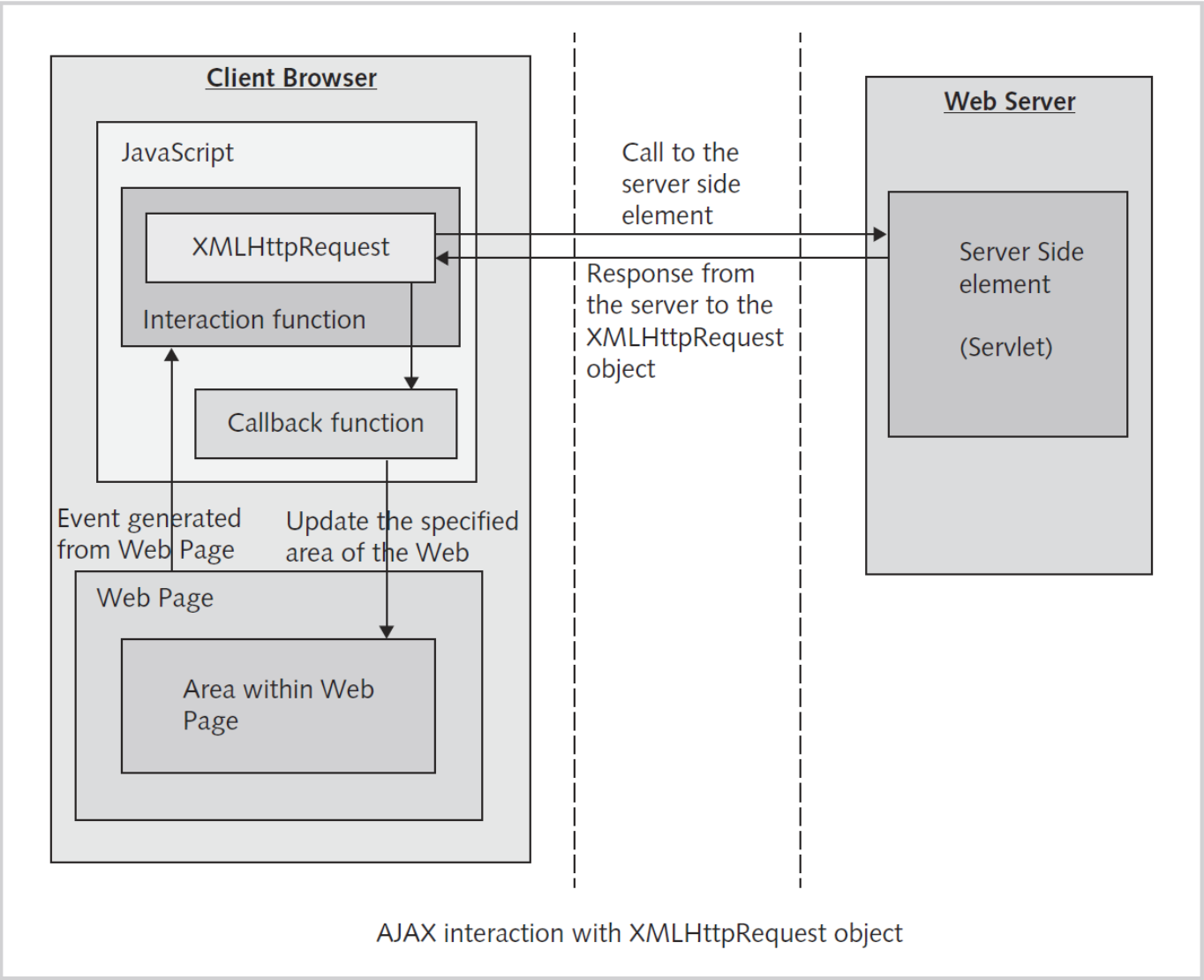


Figure 8-14 Client and server interaction using AJAX

© Cengage Learning 2013

Threats and Vulnerabilities in Web Applications

- Open Web Application Security Project (OWASP)
  - Organization dedicated to security of Web applications
  - Promotes collaboration, discussion, and education
- OWASP's top ten risks to Web applications
  - Covered on subsequent slides

Injection

- Deemed top risk in Web applications
- Attacks use various techniques to inject data into SQL command
- Can add, modify, or remove data from back-end database communicating with Web application
- Security solutions
  - Limit access to Web application within database
  - Use prebuilt statements that do not take user input
  - Invoke stored procedures instead of sending SQL queries to the database

Injection (cont'd.)

- Security solutions (cont'd.)
  - Scrub input
  - Indicate which type of data is acceptable and discard the rest

Cross-Site Scripting (XSS)

- Server sends unverified data to the client
  - Client executes code that exploits the Web browser
- Attack occurs due to vulnerabilities of legitimate Web sites
- Security solutions
  - Ensure untrusted data cannot be inserted into HTML returned to a client
    - Or into URL parameters passed to a Web application
  - Scrub all accepted input prior to return
  - Remove special URL characters from input data used to form a URL parameter

Broken Authentication and Session Management

- Vulnerabilities occur with custom systems to authenticate users
  - Example: banking Web session that does not automatically end when browser closes
- Security solutions
  - Require complex passwords
  - Use encryption to transmit password information
  - Disconnect sessions after certain time period
  - Do not give away information in error messages
  - Lock account after several invalid logon attempts
  - Session IDs should be random and encrypted

Insecure Direct Object References

- HTML form often restricts user choices
  - Drop-down list, check box, etc.
  - Does not necessarily limit data passed to Web application
  - Attacker can intercept and modify request
- Security solutions
  - Ensure server prevents directory traversal
  - Ensure user is authenticated and authorized to access requested data
  - Avoid exposing key names, variable types, or other attributes

Cross-Site Request Forgery (CSRF)

- Attack that exploits Web site's previous authentication of a user
- Security solutions
  - Generate random tokens for each HTML form used
    - Pass tokens to server for sensitive Web actions
  - Use challenge-response mechanism
  - Ensure users log off every session

Security Misconfiguration

- System administrator steps to secure Web server
  - Stay informed of updates as they are released
  - Treat Web server as a bastion host
  - Secure application and development frameworks
  - Limit user accounts to the absolutely essential
    - Ensure complex passwords are used
  - Limit error messaging to Web visitors
    - Limits information an attacker can use

Insecure Cryptographic Storage

- Data may be encrypted while resting in a database:
  - But not when sent to backup
  - Encryption key may be included on the backup
- Security solutions
  - Use strong encryption algorithms and keys
  - Encrypt backups separate from managing keys
  - Verify data can only be decrypted by authorized users

Failure to Restrict URL Access

- Attacker may guess a URL
  - If Web server does not check for authentication, attacker can access scripts meant for administrator only
- Security solutions
  - Ensure sensitive pages require authentication
  - Check user authorization for specific pages

Insufficient Transport Layer Protection

- Network sniffer can display packet text if unencrypted
- Security solutions
  - Encrypt data during transfer from client to server
    - And vice versa
  - Use the “secure” flag on all sensitive cookies
  - Ensure SSL is valid and issued by a trusted CA
  - Encrypt communications from Web server to back-end systems

Unvalidated Redirects and Forwards

- Web site may need to redirect visitors to another page
  - Redirects may be manipulated
- Security solutions
  - Do not use redirects
  - Make sure no parameters are fed to the redirects
  - Validate parameters and authorize users if they must be used

Securing a Web Server

- Best practices
  - Upgrade and patch Web server software
  - Remove or disable unnecessary applications and services
  - Limit user accounts
  - Enforce strong password policy
  - Monitor user activity
  - Limit access to sensitive OS and Web resources

Securing a Web Server (cont'd.)

- Best practices (cont'd.)
  - Configure security settings
    - Ensure application does not run with admin privileges
  - Do not use links in public Web content
  - Disallow search engine indexing on sensitive directories
  - Control access to specific pages and directories

Summary

- SMTP is used to send Internet mail
- POP3 and IMAP are used to receive Internet mail
- FTP and TFTP are simple methods of transferring files between computer systems
  - Should be used in conjunction with SSL
- Telnet allows users to connect to a computer remotely
  - Must be used over a secure network link for safety
- SNMP is used to monitor status and performance of network devices

Summary (cont'd.)

- LDAP provides a communication framework with centralized directories
- NNTP allows users to use a distributed protocol to download and post messages
- DNS performs translation of domain names to network addresses
- A variety of Web programming languages exist
- Common attacks on Web applications include injection attacks and cross-site scripting