Security Strategies in Web Applications and Social Networking

Lesson 7

Introducing the Web Application Security Consortium (WASC)

Learning Objective and Key Concepts

Learning Objective

- Analyze common Web site attacks, weaknesses, and security best practices.

Key Concepts

- Sources of Web site attacks and weaknesses
- Attack techniques using available tools and sources
- Web site security best practices

Identify Attacks and Weaknesses

- Web Application Security Consortium (WASC)
  - Lists 34 types of Web attacks and 15 classes of weaknesses
  - Maintains database of Web site hacking incidents

Threats Identified by WASC

- Abuse of Functionality
- Brute-Force Attack
- Buffer Overflow
- Content Spoofing
- Credential/ Session Prediction
- Cross-Site Scripting (XSS)
- Cross-Site Forgery
- Denial of Service (DoS)

Threats Identified by WASC (Cont.)

- Fingerprinting
- Format String
- HTTP Response Smuggling
- HTTP Response Splitting
- HTTP Request Smuggling
- HTTP Request Splitting
- Integer Overflow
- LDAP Injection
- Mail Command Injection

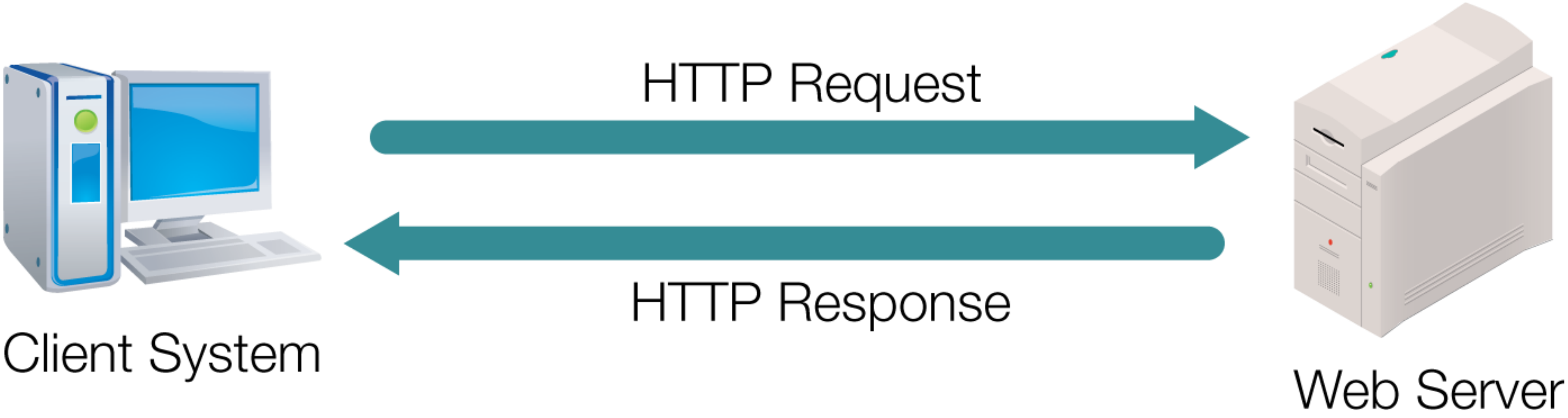
Threats Identified by WASC (con't)

- Null Byte Injection
- OS Commanding
- Path Traversal
- Predictable Resource Location
- Remote File Inclusion (RFI)
- Routing Detour
- Session Fixation
- SOAP Abuse Array
- Server-side include (SSI) Injection

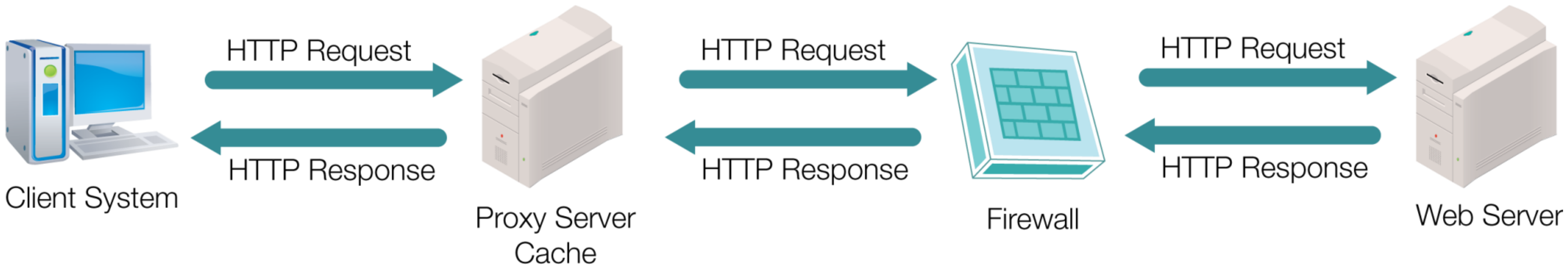
Threats Identified by WASC (con't)

- SQL Injection
- URL Redirector Abuse
- XPath Injection
- XML Attribute Blowup
- XML External Entities
- XML Entity Expansion
- XML Injection
- XQuery Injection

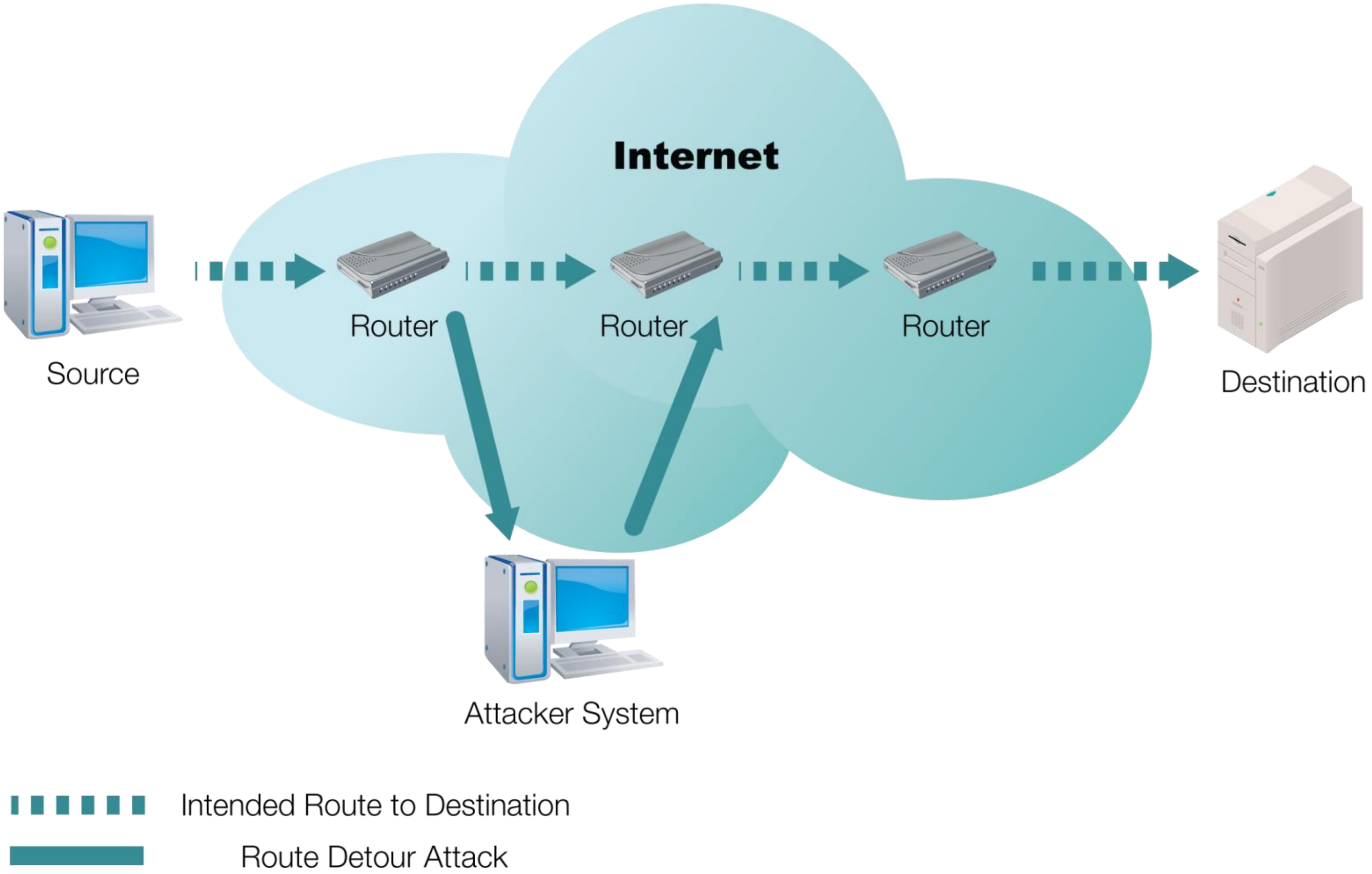
HTTP Communication Process



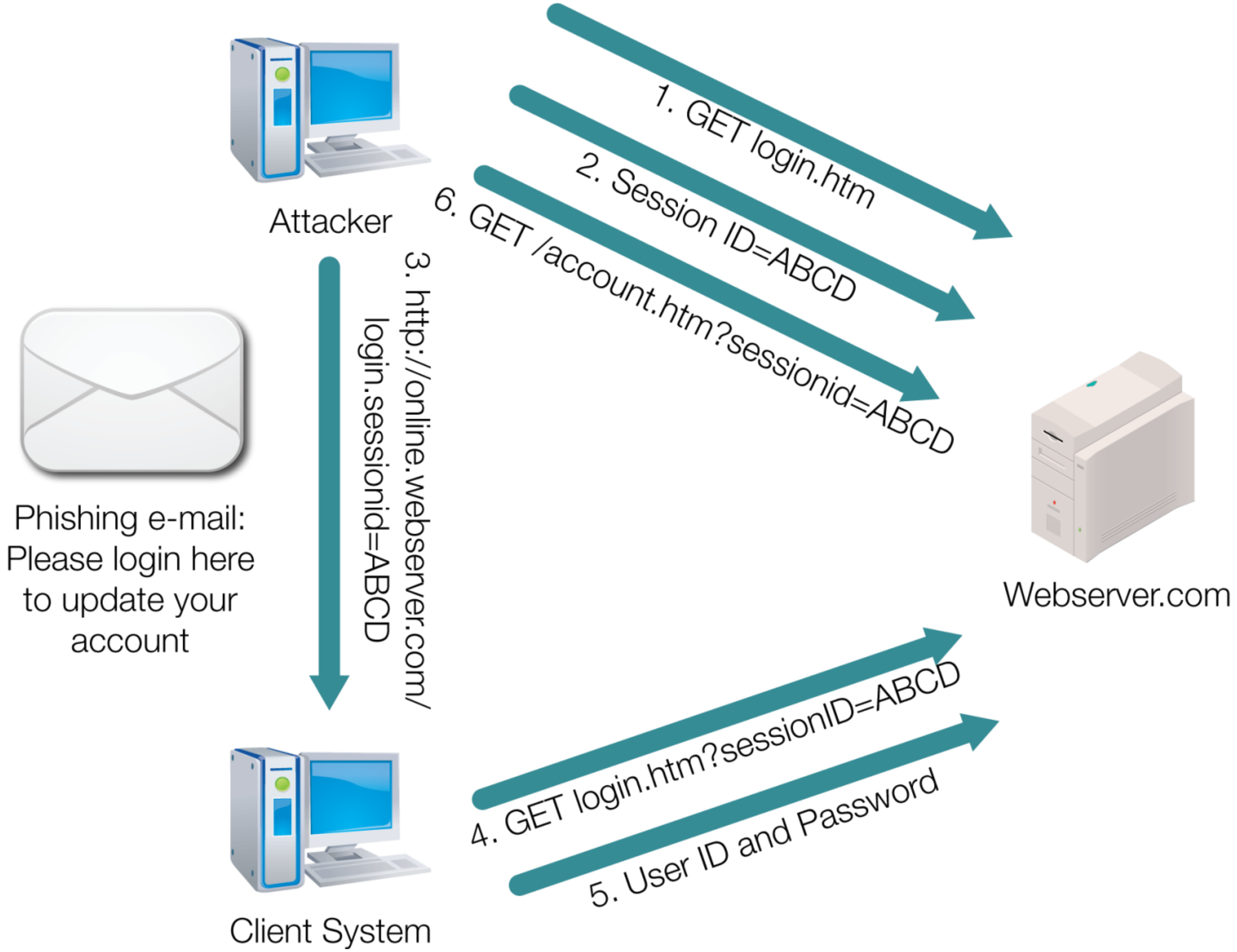
HTTP Communication Through Intermediary Points



Routing Detour Attack



Session Fixation Attack


Attacker
1. GET login.htm
2. Session ID=ABCD
6. GET /account.htm?sessionid=ABCD
3. http://online.webserver.com/ login.sessionid=ABCD
Phishing e-mail: Please login here to update your account
Webserver.com
Client System
4. GET login.htm?sessionID=ABCD
5. User ID and Password

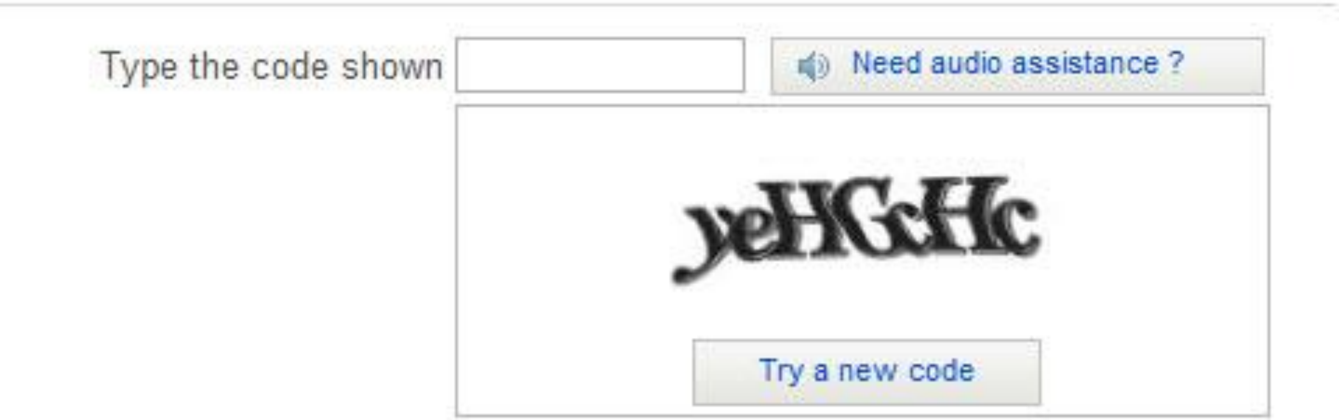
Fifteen Web Site Attacks

- Application Misconfiguration
- Directory Indexing
- Improper File System Permissions
- Improper Input Handling
- Improper Output Handling
- Information Leakage
- Insecure Indexing
- Insufficient Anti-Automation e.g. use capcha to prevent automating login forms
- Insufficient Authentication

Fifteen Web Site Attacks (Cont.)

- Insufficient Authorization
- Insufficient Password Recovery
- Insufficient Process Validation
- Insufficient Session Expiration
- Insufficient Transport Layer Protection
- Server Misconfiguration

An Example of CAPTCHA



Best Practices

Mitigating Attack Risks	Implement a best practices approach.
	Be security conscious as early as possible.
	Know your infrastructure.
	Be proactive in gaining necessary support at all levels.
Mitigating Weaknesses	Practice due diligence for mitigating weaknesses.
	Be aware of vulnerabilities.
	Be aware of WASC’s threats to Web Application security.
	Validate user input.

Summary

- Sources of the Web site attacks and weaknesses
- Attack techniques using available tools and sources
- Web site security best practices

Virtual Lab

- Applying OWASP to a Web Security Assessment