UNIVERSITI TEKNIKAL MALAYSIA MELAKA

Fakulti Teknologi Maklumat dan Komunikasi

Network Security Administration and Management

BITS 3353

Lecture 5: Application and Network Attacks

Objectives

- List and explain the different types of Web application attacks
- Define client-side attacks
- Explain how a buffer overflow attack works
- List different types of denial of service attacks
- Describe interception and poisoning attacks

WHAT?

any attempt to expose, alter, disable, destroy, steal or gain unauthorized access to or make unauthorized use of an asset.

APPLICATION ATTACKS (Attacks that target applications)

1. Web application attacks
2. Client-side attacks
3. Buffer overflow attacks

NETWORK ATTACKS

1. Denial of service (DoS)
2. Distributed denial of services (DDoS)

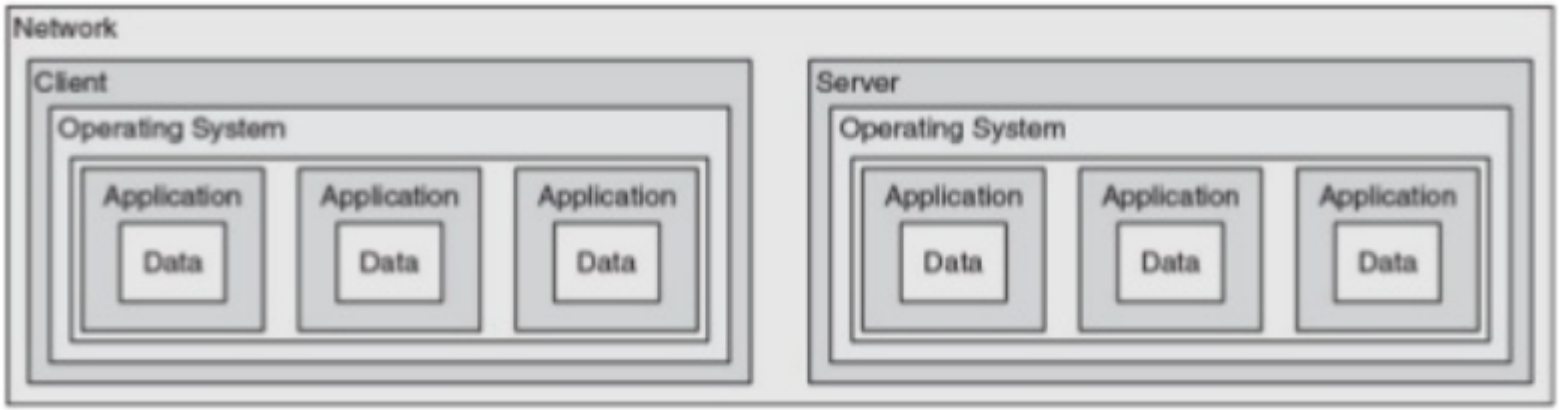
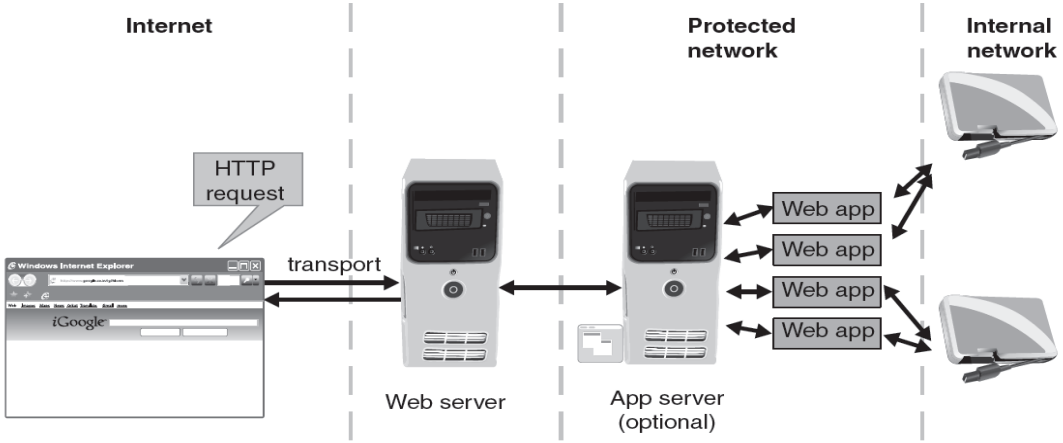


Figure 3-1 Conceptual networked computer system

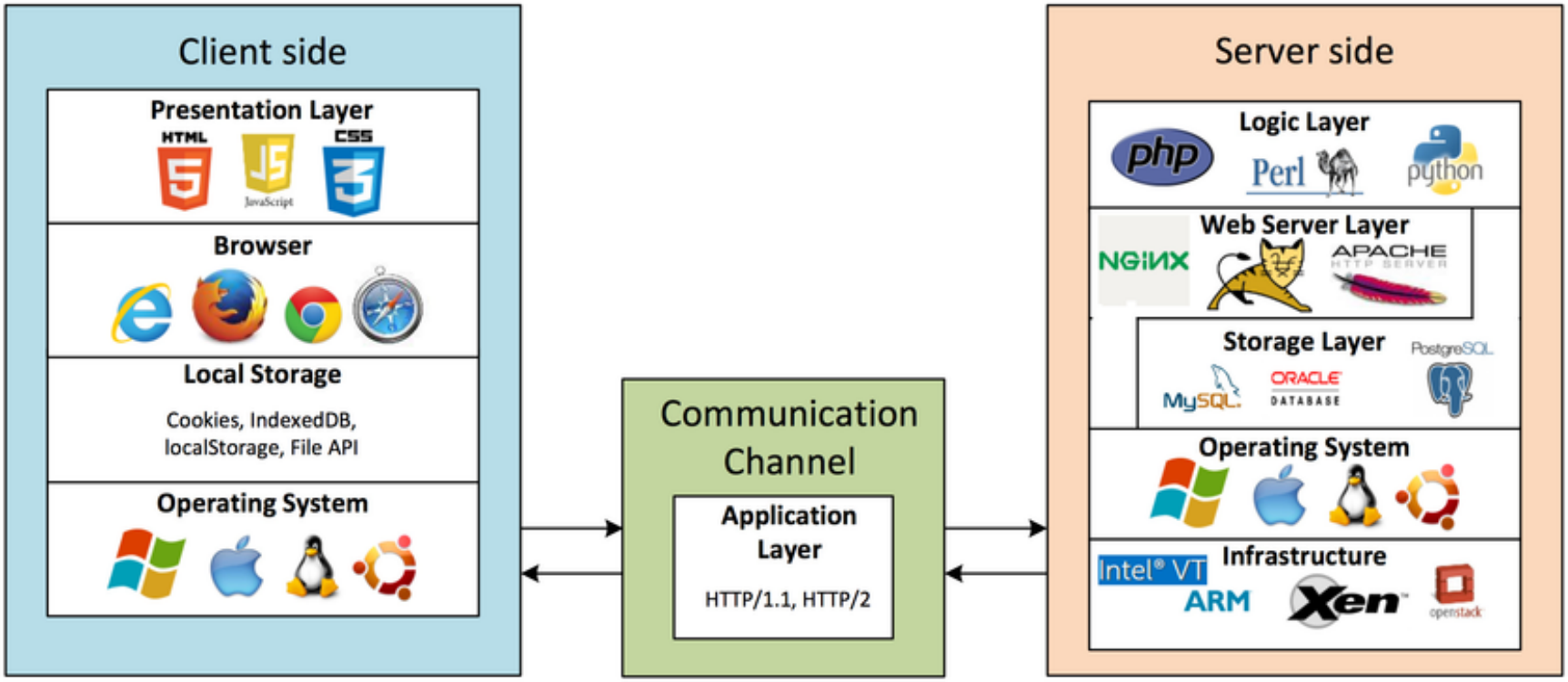
Web Application Attacks

- Web application is an application that runs on a web server and users access it using a web browser.
- Any security loop hole in browser will lead to exploiting vulnerabilities in web application.
- Approach to securing Web applications
  - –Hardening the Web server
  - –Protecting the network

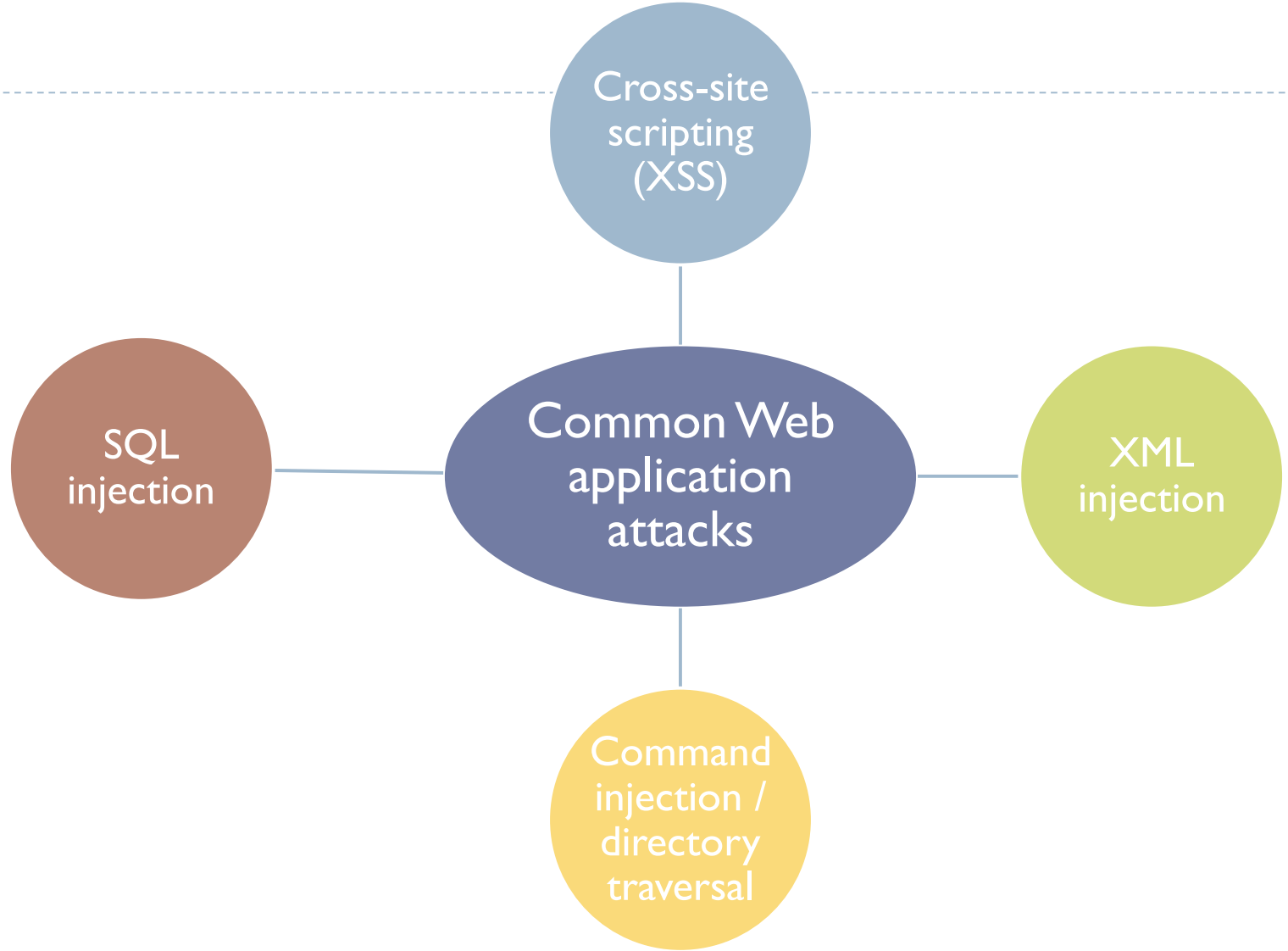


Web application infrastructure

Web Application Attacks

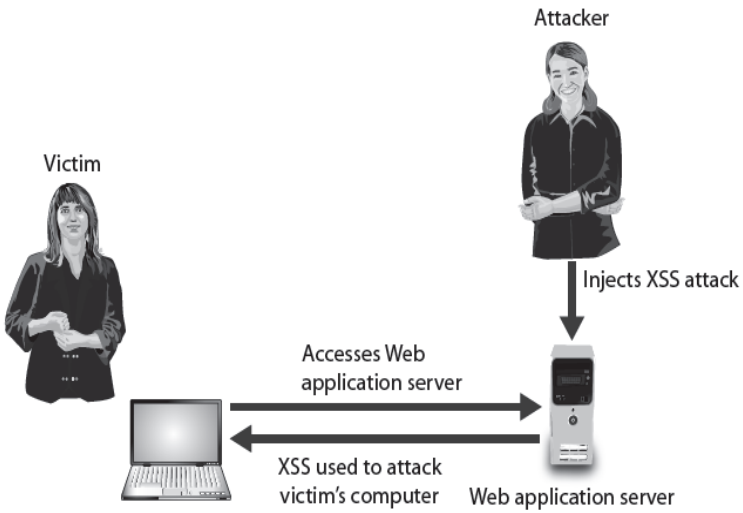


Vadlamudi, Satya Gautam, et al. (2016)


Cross-site scripting (XSS)
SQL injection
Common Web application attacks
XML injection
Command injection / directory traversal

Web application attacks:
1. Cross-Site Scripting (XSS)

- Injecting scripts into a Web application server
  - –Directs attacks at clients



XSS attacks

When victim visits injected Web site:

–Malicious instructions sent to victim's browser

Browser cannot distinguish between valid code and malicious script

Requirements of the targeted Web site
–Accepts user input without validation
–Uses input in a response without encoding it

Web application attacks:
2. SQL Injection

SQL (Structured Query Language)
–Used to manipulate data stored in relational database

Target

SQL servers

How

injecting command

Example: Forgotten password

1. Attacker enters incorrectly formatted e-mail address
2. Response lets attacker know whether input is being validated
3. Attacker enters email field in SQL statement
4. Statement processed by the database
   –Example statement:
   SELECT fieldlist FROM table WHERE field = 'whatever' or 'a'='a'
5. Result: All user email addresses will be displayed

SQL injection statement	Result
whatever' AND email IS NULL; --	Determine the names of different fields in the database
whatever' AND 1=(SELECT COUNT(*) FROM tabname); --	Discover the name of the table
whatever' OR full_name LIKE '%Mia%'	Find specific users
whatever'; DROP TABLE members; --	Erase the database table
whatever'; UPDATE members SET email = 'attacker-email@evil.net' WHERE email = 'Mia@good.com';	Mail password to attacker's e-mail account

SQL injection statements

Web application attacks:
3. XML Injection

XML (eXtensible Markup Language)

- defines a set of rules for encoding documents in a format that is both human-readable and machine-readable
  - Used to store and transport data.

How

injecting command

- Similar to SQL injection attack
- Attacker discovers Web site that does not filter user data
- Injects XML tags and data into the database

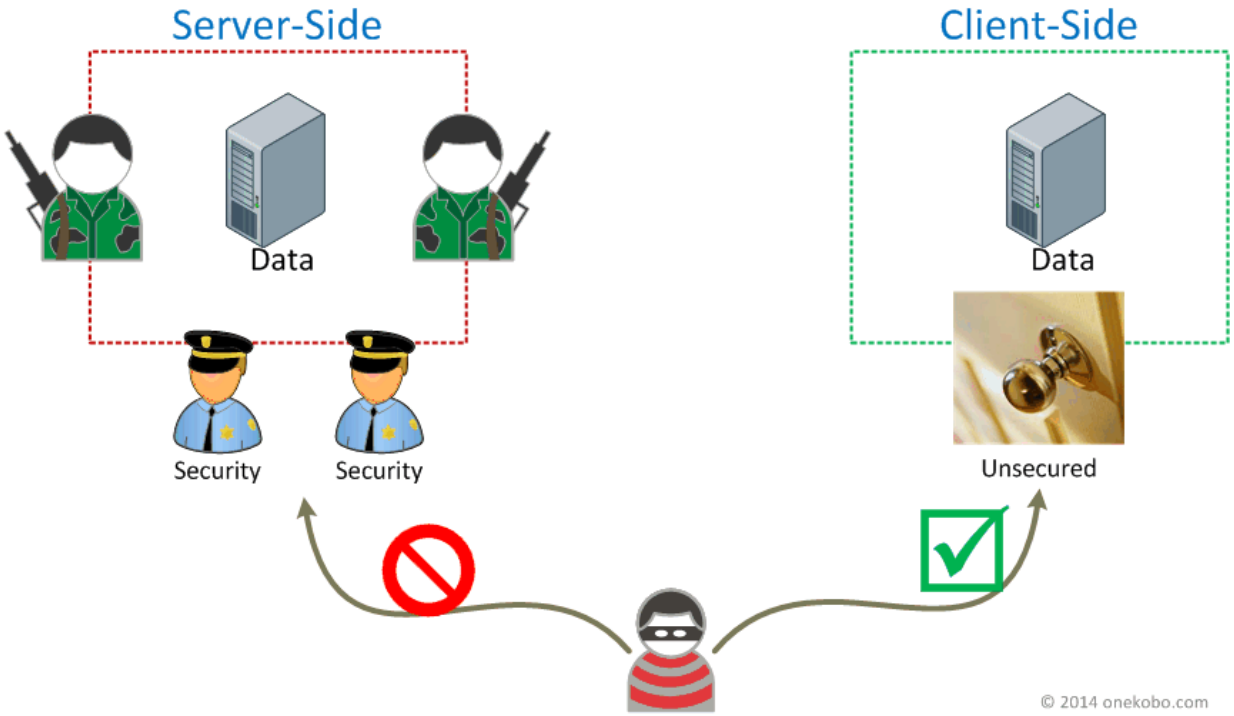
Web application attacks:
4. Command Injection / Directory Traversal

- Web server users typically restricted to root directory
- Users may be able to access subdirectories:
  –But not parallel or higher level directories
- HTTP attack which allows attackers to access restricted **directories** and execute commands outside of the web server's root **directory**.
- In this type of attack, an authenticated or unauthenticated user can request and view or execute files that they should not be able to access.

CMD.Exe – can be used to enter text-based commands
Passwd (Linux) contains user account information

Client-Side Attacks

- Web application attacks are server-side attacks
- Client-side attacks target vulnerabilities in client applications



Client-Side Attacks

- A client can be a standard web browser such as Internet Explorer or Google Chrome or it can be an embedded browser object in an application such as an email client, media players, e-book reader, etc.
- Two reasons why client applications are more inviting targets for attackers include:
    1. Clients generally undergo less rigorous security testing than server applications
    2. Clients are more difficult to patch due to the diverse range of client versions, owners and environments

How it happen?

- When a user downloads malicious content
- They require user-interaction such as clicking a malicious link or running executable payload.

Client-Side Attacks

How it happen?

- Header manipulation
  - Referer
    - –Attacker can modify this field to hide fact it came from another site
    - –Modified Web page hosted from attacker's computer
  - Accept-language
    - –Some Web applications pass contents of this field directly to database
    - –Attacker could inject SQL command by modifying this header

Client-Side Attacks

How it happen?

- Cookies and Attachments.
  - –Cookies store user-specific information on user's local computer
- Web sites use cookies to identify repeat visitors
- Examples of information stored in a cookie
  - –Travel Web sites may store user's travel itinerary
  - –Personal information provided when visiting a site

Client-Side Attacks

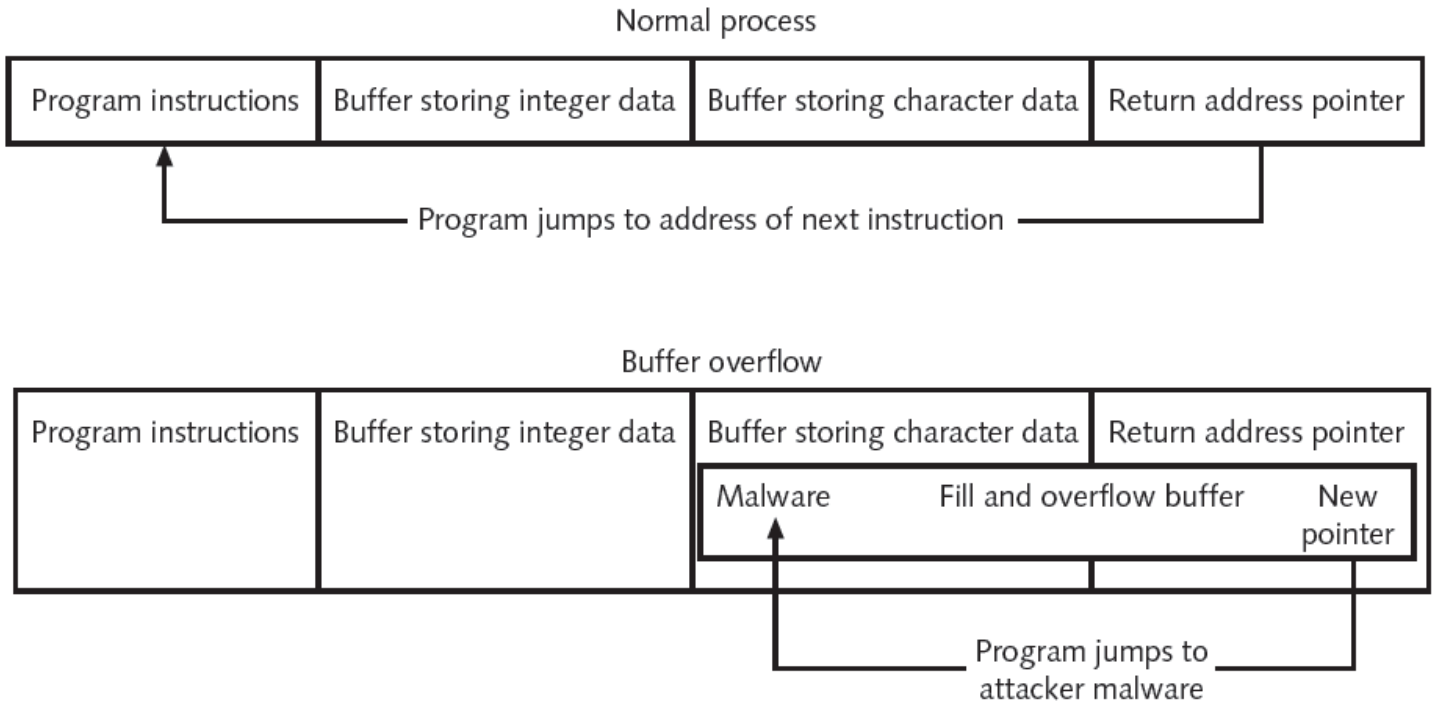
- **First-party cookie**
  - –Cookie created by Web site user is currently visiting
- **Third-party cookie**
  - –Site advertisers place a cookie to record user preferences
- **Session cookie**
  - –Stored in RAM and expires when browser is closed
- **Persistent cookie**
  - –Recorded on computer's hard drive
  - –Does not expire when browser closes
- **Flash cookie**
  - —Uses more memory than traditional cookie
  - –Cannot be deleted through browser configuration settings
- **Secure cookie**
  - —Used only when browser visits server over secure connection
  - –Always encrypted

Client-Side Attacks: Buffer Overflow Attacks

Process attempts to store data in RAM beyond boundaries of fixed-length storage buffer

Data overflows into adjacent memory locations

May cause computer to stop functioning

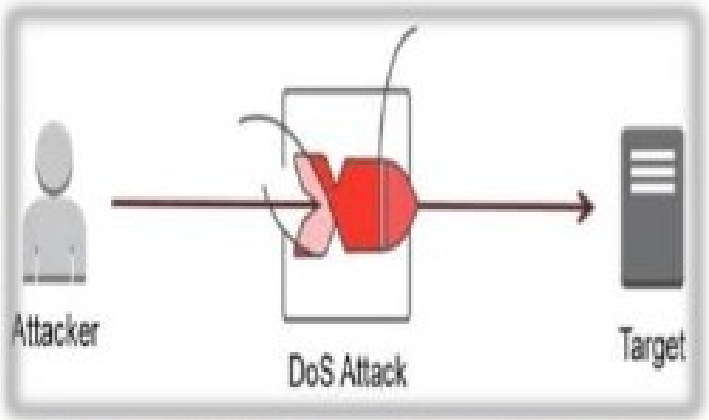


Buffer overflow attack

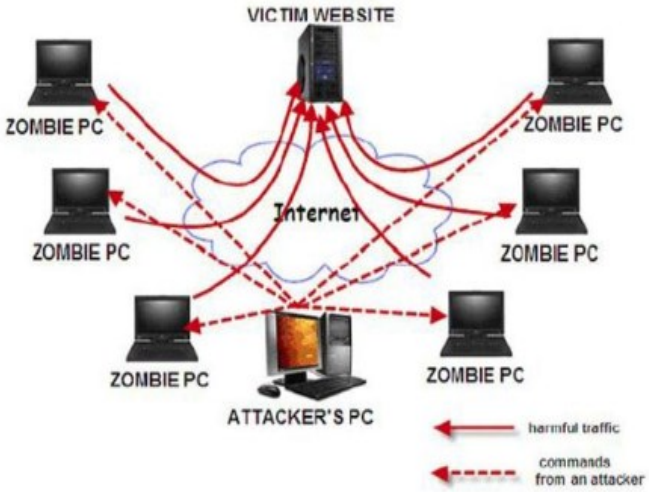
Network Attacks

- Attempts to prevent system from performing normal functions

- In a denial-of-service (DoS) attack, an attacker attempts to prevent legitimate users from accessing information or services.



- In a distributed denial-of-service (DDoS) attack, an attacker may use your computer to attack another computer.



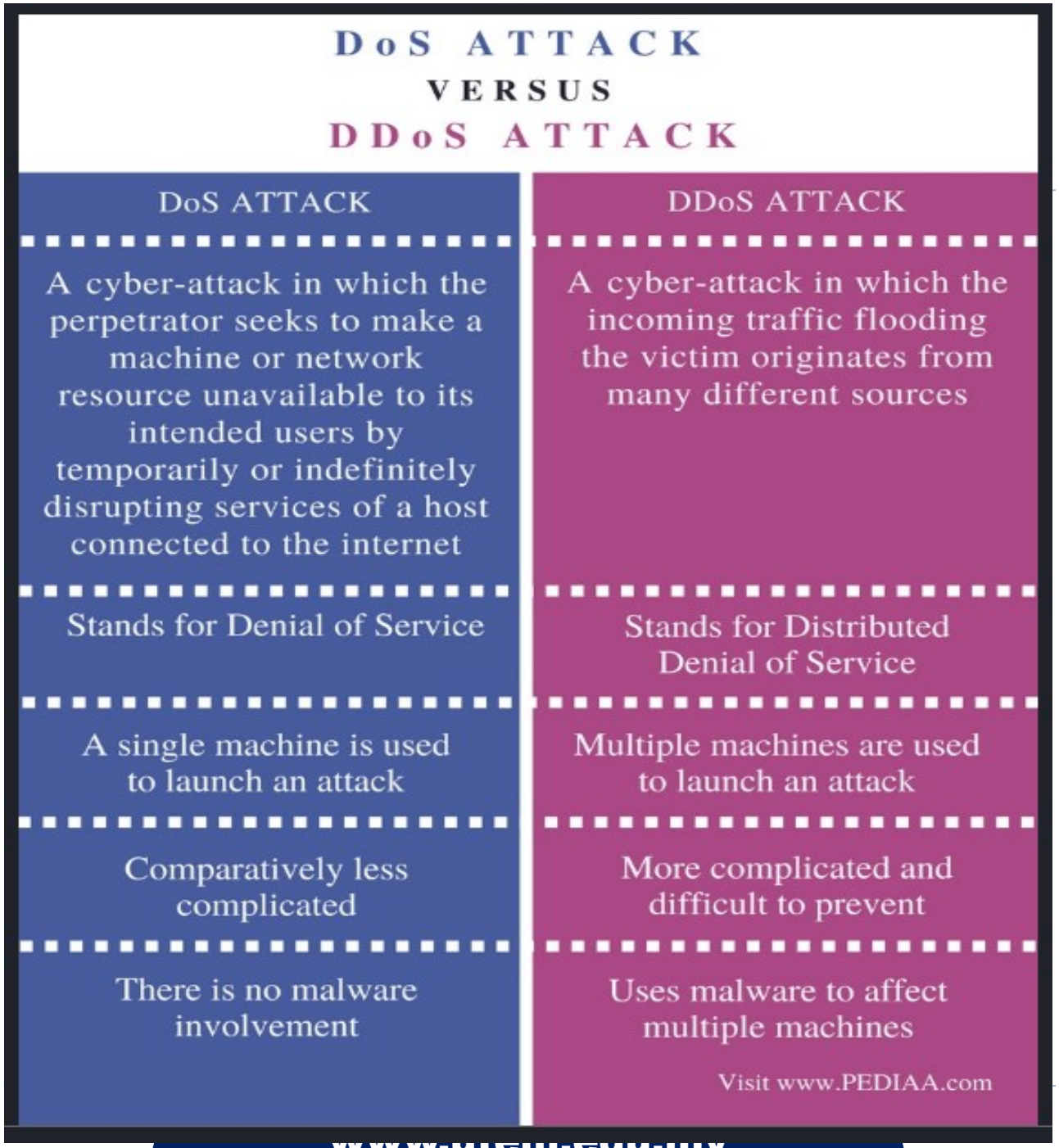
Network Attacks

Denial of service (DoS)

- Attempts to prevent system from performing normal functions
- Ping flood attack
  -Ping utility used to send large number of echo request messages
  -Overwhelms Web server
- Smurf attack
  -Ping request with originating address changed
  -Appears as if target computer is asking for response from all computers on the network
- SYN flood attack
  -Takes advantage of procedures for establishing a connection

Distributed denial of service (DDoS)

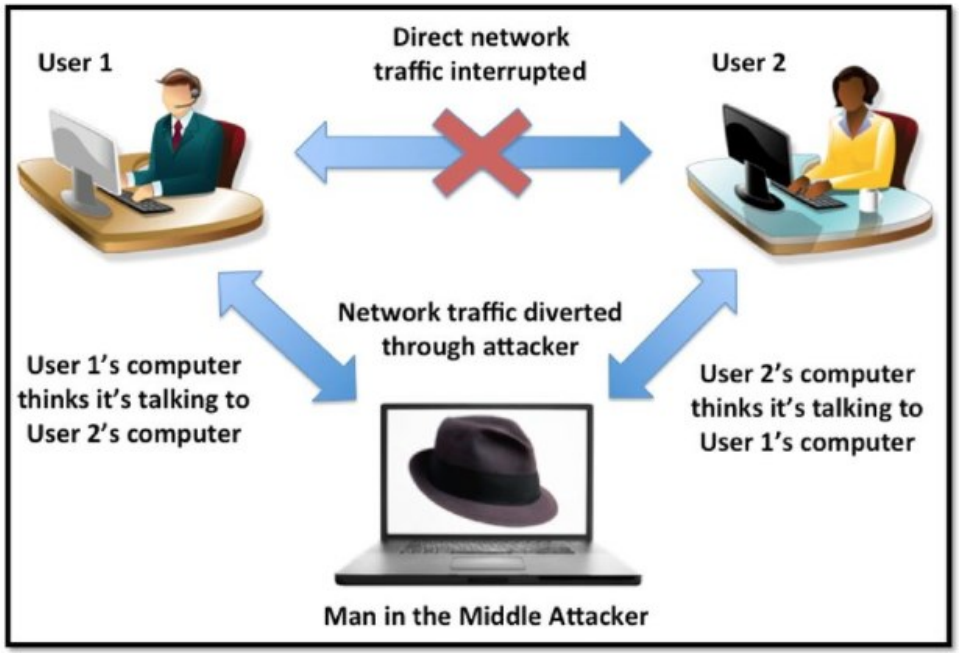
- Attacker uses many zombie computers in a botnet to flood a device with requests
- Virtually impossible to identify and block source of attack



Interception

Man-in-the-middle

- –Interception of legitimate communication
- –Forging a fictitious response to the sender
- –Passive attack records transmitted data
- –Active attack alters contents of transmission before sending to recipient

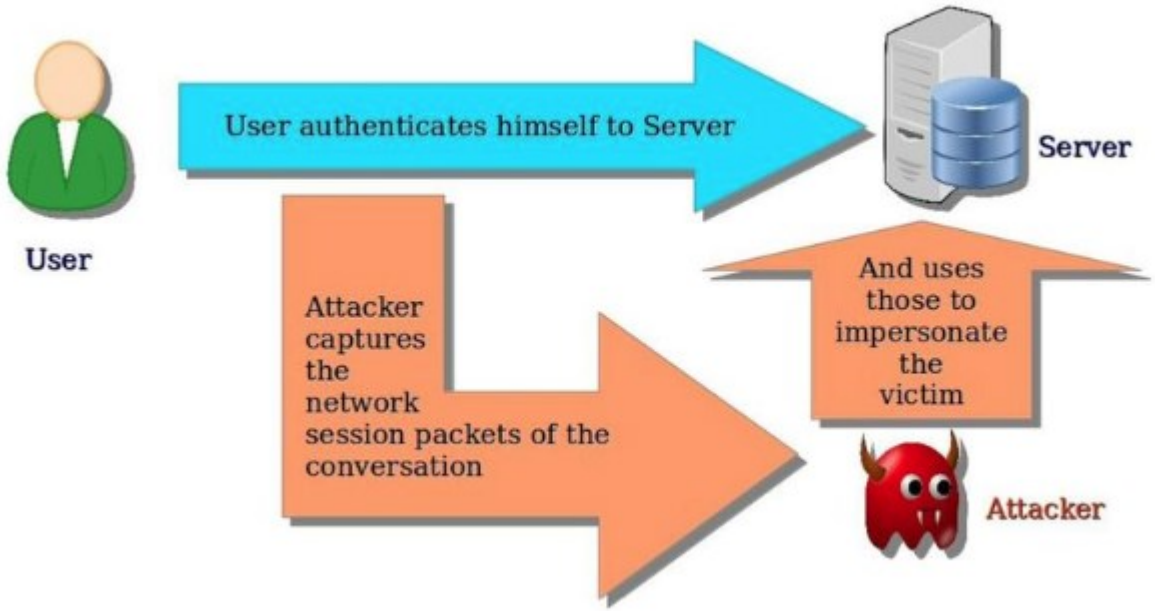


Interception

Replay Attack

–Attacker sniffs packets to get authentication info

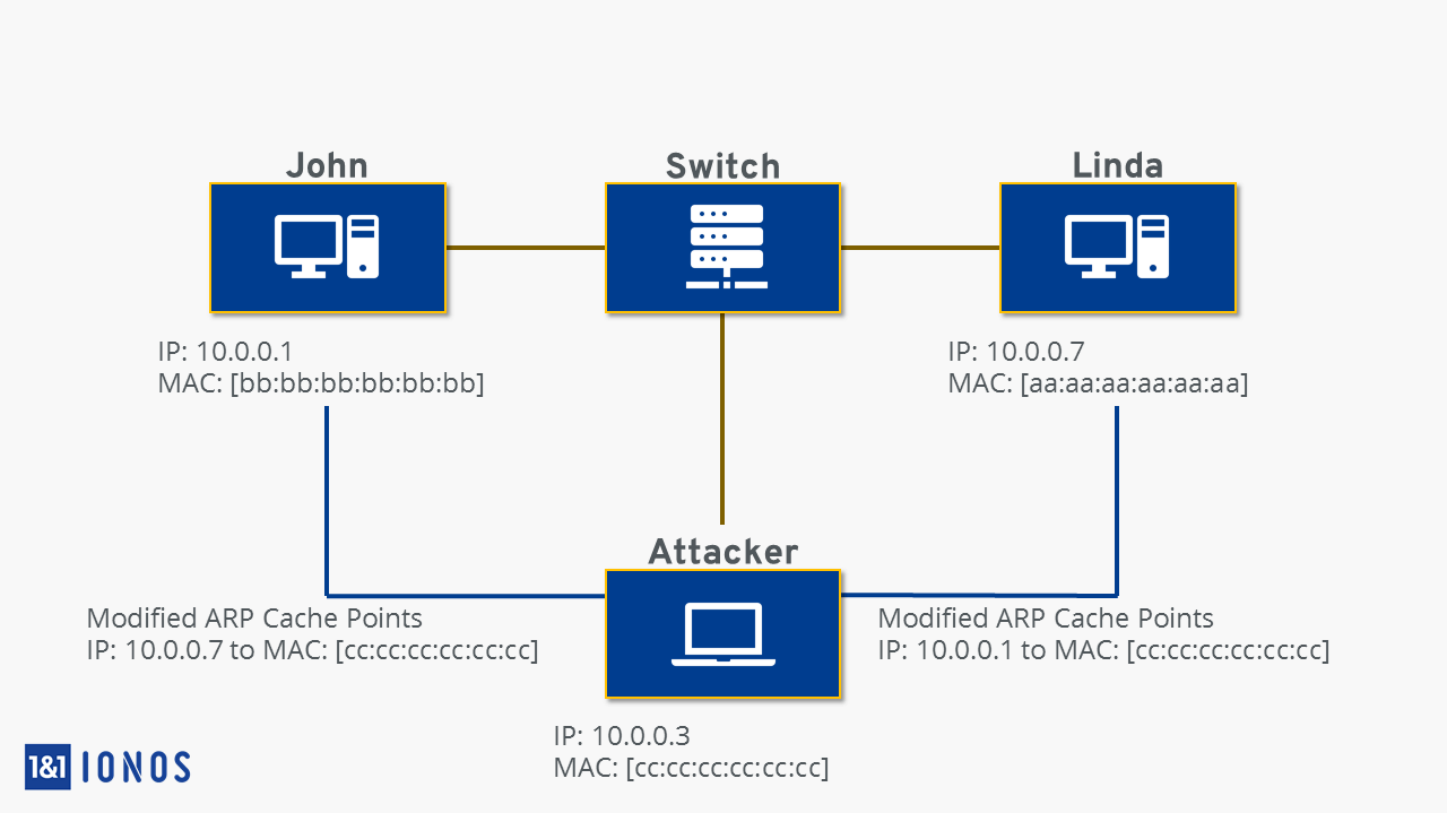
–Then attavker uses info to connect to server



Poisoning

ARP Poisoning

–Attacker modifies MAC address in ARP cache to point to different computer



Poisoning

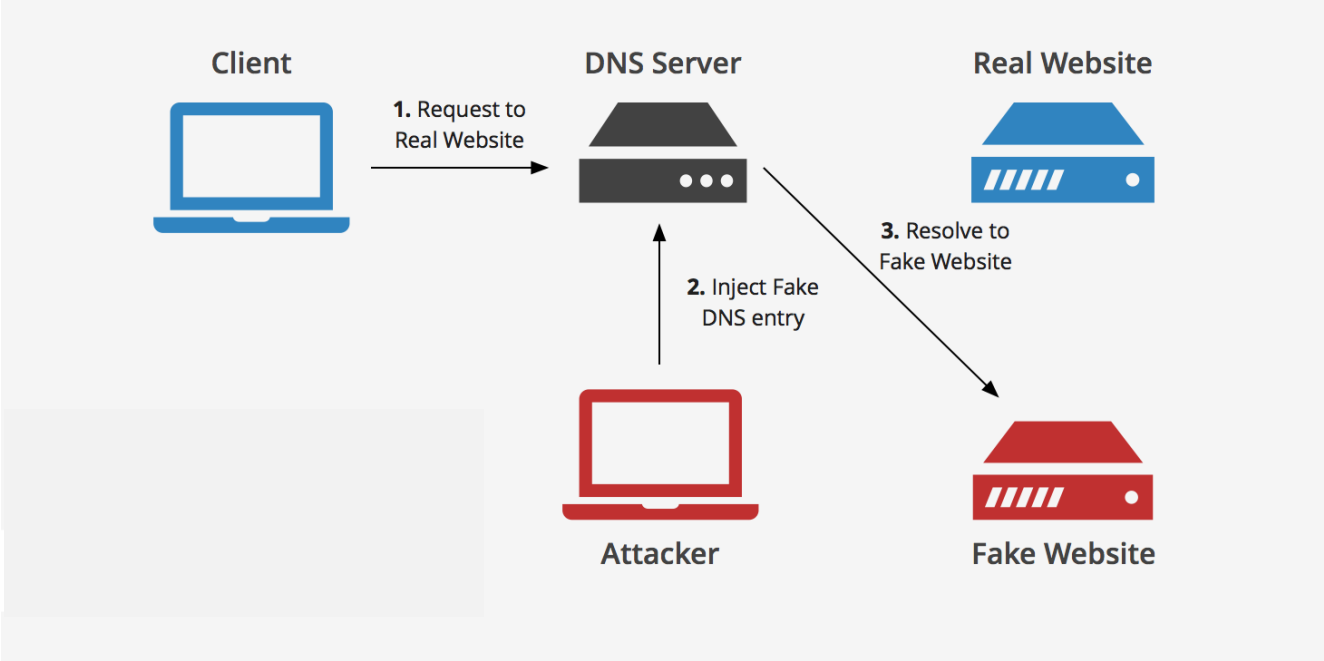
Attack	Description
Steal data	An attacker could substitute their own MAC address and steal data intended for another device
Prevent Internet access	An attacker could substitute an invalid MAC address for the network gateway so that no users could access external networks
Man-in-the-middle	A man-in-the-middle device could be set to receive all communications by substituting that MAC address
DoS attack	The valid IP address of the DoS target could be substituted with an invalid MAC address, causing all traffic destined for the target to fail

Attacks from ARP poisoning

Poisoning

DNS Poisoning

- DNS poisoning substitutes DNS addresses to redirect computer to another device
- Two locations for DNS poisoning
  - –Local host table
  - –External DNS server



Attacks on Access Rights

- Privilege escalation
  - –Exploiting software vulnerability to gain access to restricted data
- Two types of privilege escalation
  - –Lower privilege user accesses functions restricted to higher privilege users
  - –User with restricted privilege accesses different restricted privilege of a similar user

- Transitive access
  - –Attack involving a third party to gain access rights
  - –Has to do with whose credentials should be used when accessing services
    - •Different users have different access rights

Summary

- Web application flaws are exploited through normal communication channels
- XSS attack uses Web sites that accept user input without validating it
  - –Uses server to launch attacks on computers that access it
- Client-side attack targets vulnerabilities in client applications
  - –Client interacts with compromised server
- Session hijacking
  - –Attacker steals session token and impersonates user
- Buffer overflow attack
  - –Attempts to compromise computer by pushing data into inappropriate memory locations
- Denial of service attack attempts to overwhelm system so that it cannot perform normal functions
- In ARP and DNS poisoning, valid addresses are replaced with fraudulent addresses
- Access rights and privileges may also be exploited