The Demand for Security

LESSON 2

Course Intended Learning Outcomes

- Demonstrate that information security is business necessity for enterprises;
- Describe why an organization's general management and IT management are equally responsible for an effective information security program;
- Recognize the dangers to information security and the most typical attacks associated with those threats, as well as the differences between threats to data within systems and attacks on data within systems;
- Describe problems that software developers face, as well as the most typical mistakes they make, and describe how software development programs can help developers create more safe and reliable software.

Introduction

- The core aim of an information security program, unlike any other information technology program, is to ensure that systems and their contents remain the same.
- Attacks on information systems, on the other hand, happen on a regular basis, and the demand for information security rises in tandem with the sophistication of such attacks.

Business Needs First

Four critical functions:

1. Keeping the company's ability to function safe.
2. Ensure that applications operating on the organization's IT platforms are safe to use.
3. Keeping the data that the company obtains and utilizes safe.
4. Keeping the company's technological assets safe.

Protecting Organization's Functionality

- The implementation of information security that safeguards the organization's ability to function is the responsibility of both general management and IT management.
- Managing information security is more about policy and enforcement than it is about the technology used to achieve it, much as managing payroll is more about management than quantitative wage computations.

Providing Safe Environment for Applications to Run

- A modern company must develop an environment that protects the applications, especially those that are critical to the company's infrastructure

Protecting Data Collected and Used by Organizations

- Information systems are essential for any business, educational institution or government body that operates in the modern world of connected and responsive services.

Keeping Organizational Technology Assets Safe

- Organizations must use secure infrastructure services that are appropriate for their size and breadth in order to function properly.

Threats

	Category of Threat	Examples
1.	Compromises to intellectual property	Piracy, copyright infringement
2.	Software attacks	Viruses, worms, macros, denial of service
3.	Deviations in quality of service	ISP, power, or WAN service issues from service providers
4.	Espionage or trespass	Unauthorized access and/or data collection
5.	Forces of nature	Fire, flood, earthquake, lightning
6.	Human error or failure	Accidents, employee mistakes
7.	Information extortion	Blackmail, information disclosure
8.	Missing, inadequate, or incomplete	Loss of access to information systems due to disk in place drive failure without proper backup and recovery plan organizational policy or planning
9.	Missing, inadequate, or incomplete controls	Network compromised because no firewall security controls
10.	Sabotage or vandalism	Destruction of systems or information
11.	Theft	Illegal confiscation of equipment or information
12.	Technical hardware failures or errors	Equipment failure
13.	Technical software failures or errors	Bugs, code problems, unknown loopholes
14.	Technological obsolescence	Antiquated or outdated technologies

Intellectual Property Compromises

- The ownership of ideas and control over the tangible or virtual expression of those ideas.

Software Attacks on Purpose

- VIRUS is made up of code segments that carry out destructive behaviors.
- WORMS named after Tapeworm are harmful programs that endlessly duplicate themselves without the need for another program environment.
- TROJAN HORSES are software programs that conceal their true nature until they are activated, at which point they reveal their intended function.

Software Attacks on Purpose

- BACK DOOR or TRAP DOOR allows the attacker to access the systems with special rights whenever they want.
- POLYMORPHIC TREATS is one that alters its appearance to antivirus software programs over time, rendering it undetected by techniques that seek for predefined signatures.
- VIRUS AND WORM HOAXES consumes more time and resources.
- VARIATIONS IN SERVICE QUALITY outages can significantly reduce the availability of information in firms that rely heavily on the internet and the www.

Software Attacks on Purpose

- COMMUNICATIONS AND OTHER SERVICE PROVIDER ISSUES likewise have other utility services have an impact on business.
- POWER IRREGULARITIES are prevalent, and they can cause oscillations such as power surpluses, power shortages and power outages.
- ESPIONAGE or TRESPASS is a well-known and comprehensive range of electronic and human behaviors that might compromise information confidentiality.

Hackers

- Are the archetypal offender of espionage or trespass.
- 2 groups:
  - EXPERT HACKER who creates software scripts and program exploits that are employed by the beginner or unskilled hacker in the second category.
  - PROFESSIONAL HACKER are exceptionally capable persons who typically dedicate a significant amount of time and work attempting to break into the other people's information systems.

Forces of Nature

- Natural disasters, force majeure and acts of God can pose some of the most catastrophic hazards since they frequently strike without note and are beyond people's control.

Forces of Nature

- Fire
- Flood
- Earthquake
- Lightning
- Landslide or mudslide
- Tornado or strong windstorm
- Hurricane or typhoon
- Tsunami
- Electrostatic discharge (ESD)
- Dust Contamination

Human Error or Failure

- Contains actions taken by an authorized user without malice or intent. People make mistakes when they use information systems.
- Employees are one of the most significant dangers to an organization’s information security.
- Training and continuing awareness efforts, procedures and practices can help prevent human error or failure.

Information Extortion

- When an attacker or trusted insider steals information from a computer system, they demand money or a promise not to reveal it.

Information Extorsion

- Missing, Inadequate or Incomplete Organizational Policy or Planning
  - When other threats lead to attacks, an organization's information assets are subject to loss, damage, or disclosure due to lack or incomplete organizational policy or strategy
- Missing, Inadequate or Incomplete Controls
  - Dangers lead to assaults, organizations with missing, inadequate, or incomplete controls – that is security measures and information asset protection systems that are absent, misconfigured, obsolete or poorly designed suffer losses

Information Extorsion

- Sabotage or Vandalism
  - Intends to destroy an asset or harm an organization's image.
- Theft
  - Unauthorized taking or another's physical, technological,
- Technical Hardware Failures or Errors
  - When a manufacturer distributes equipment with a known or undisclosed fault, technical hardware failures or mistakes may occur

Information Extorsion

- Technical Software Failures or Errors
  - Combinations of specific software and hardware can occasionally uncover new flaws – computer codes are being produced, debugged, published and sold
- Technological Obsolescence
  - Infrastructure that is old or out-of-date can lead to unreliable and untrustworthy systems

Information Extorsion

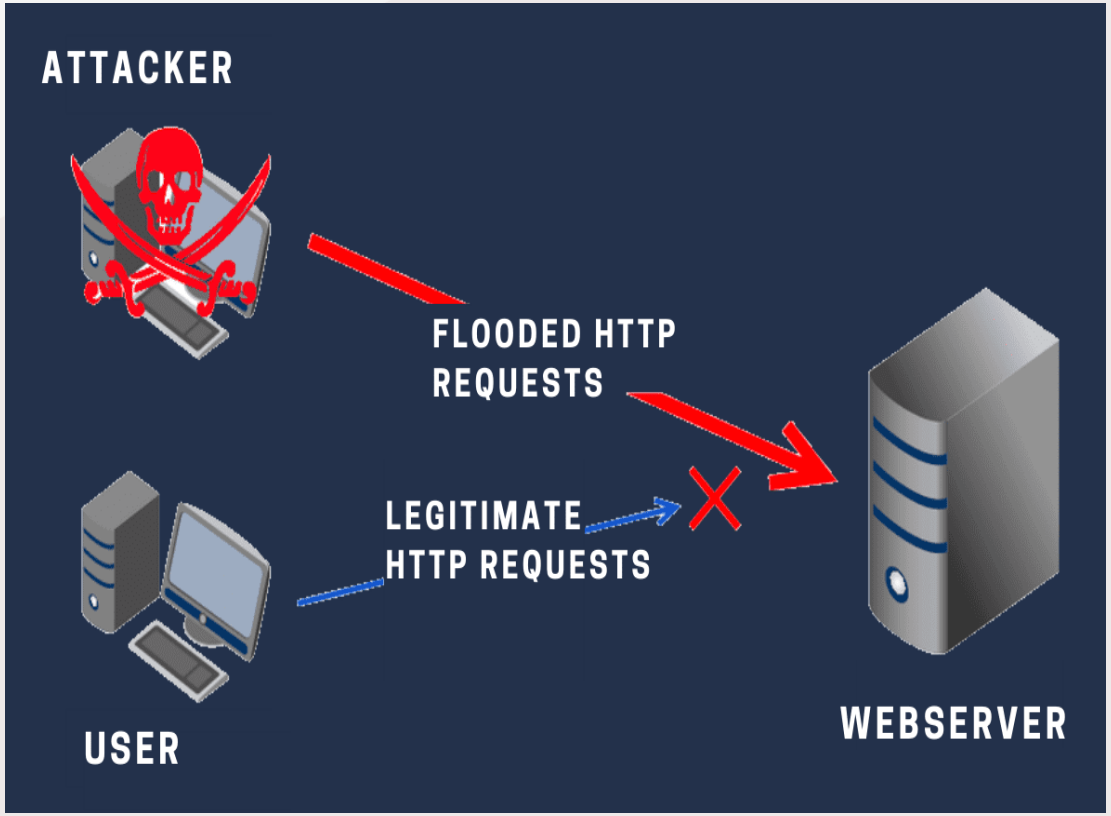
- Attack
  - A method of compromising a controlled system by exploiting vulnerability.
- Malicious Code
  - Viruses, worms, trojan horses, active web scripts are examples of harmful code that are used to destroy or steal information.

Information Extorsion

- Hoaxes
  - Transmission of virus fake with a real virus attached
- Brute Force
  - An attack when computing and network resources are used to try every conceivable password combination.
- Dictionary
  - Variant of brute force assaults that narrows the field by picking specific target accounts and using a dictionary of widely used passwords instead of random variations.

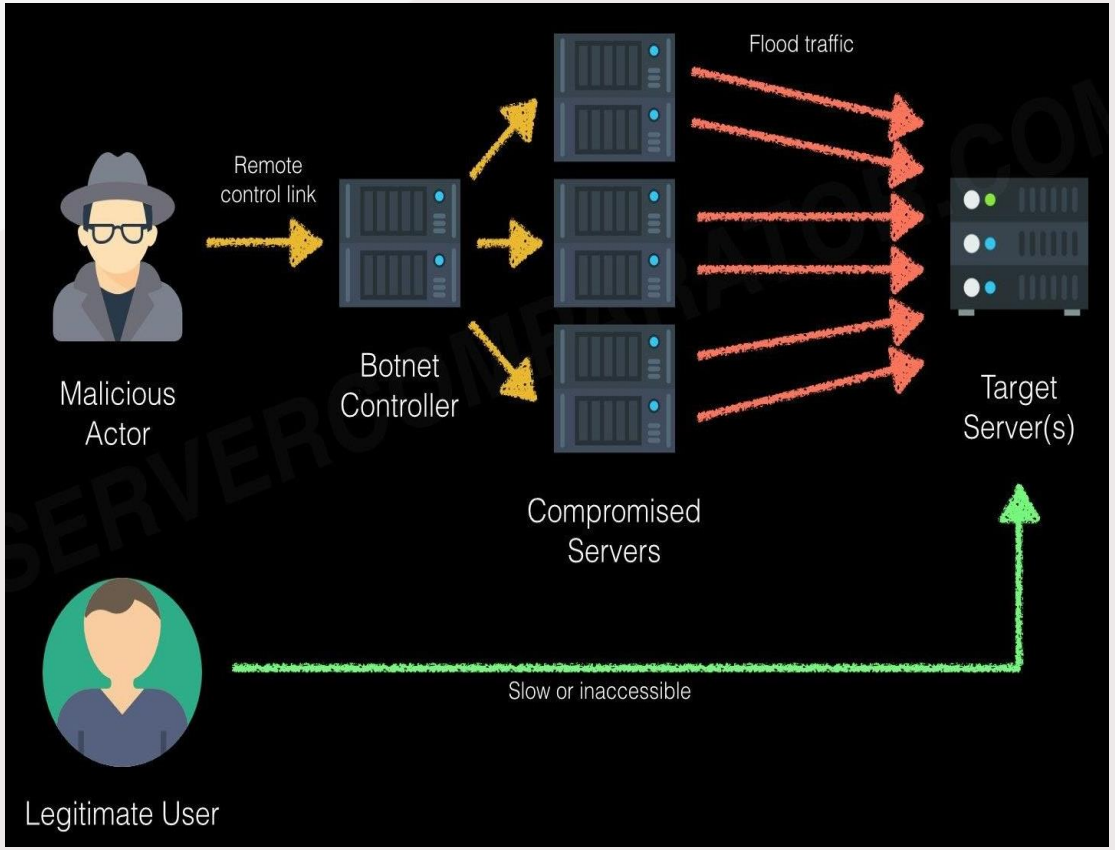
Denial-of-Service(DoS)

- Assault occurs when an attacker bombards a target with a huge number of connection or information request.



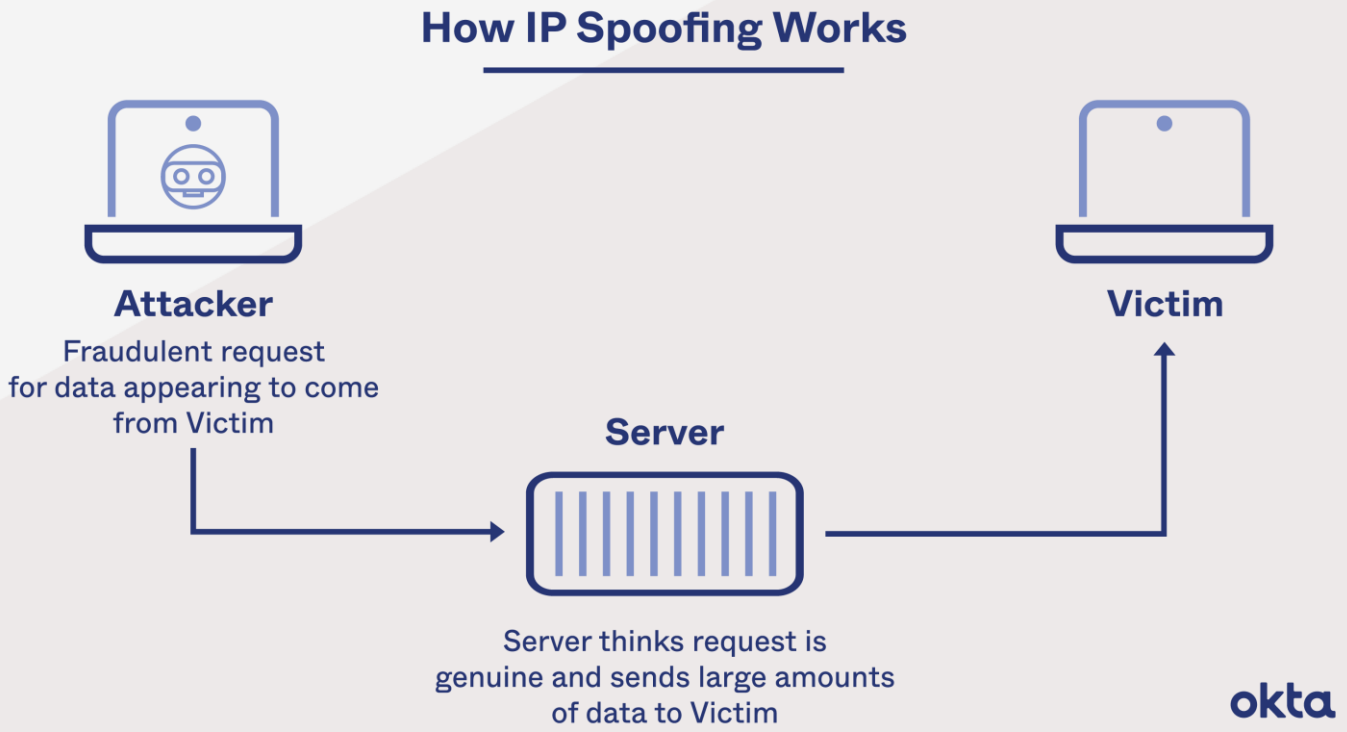
Distributed Denial-of-Service (DDoS)

- An assault in which a coordinated flood of request is sent at the same time against target from multiple places.



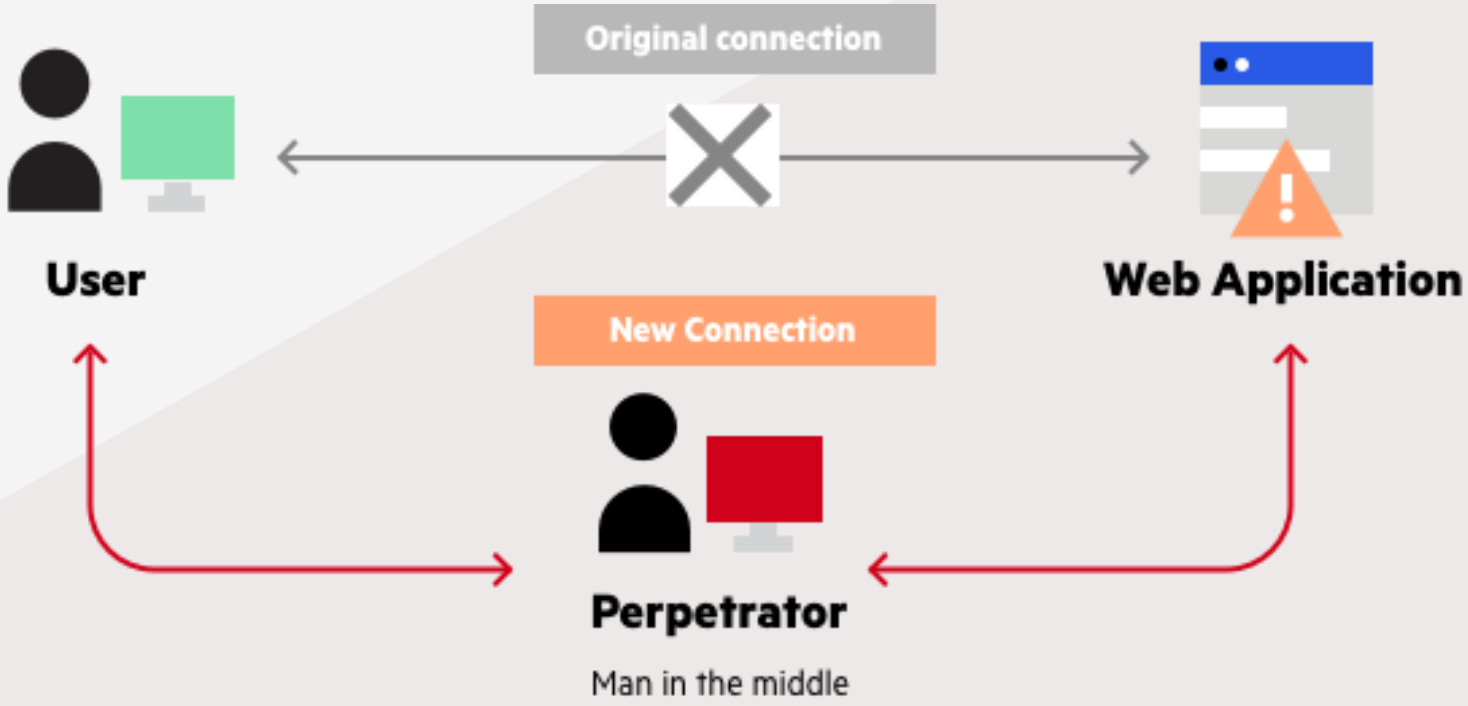
Spoofing

- A method of gaining unauthorized access to computers in which an intruder sends messages using a fake IP address to make it appear as if the messages are coming from a trustworthy host.



Man-in-the-Middle

- Ab attacker observes (or sniffs) packets from networks, alters them and re-inserts them into the network in a well-known man-in-the-middle or TCP hijacking attack.



Mail Bombing

- Attacker sends massive amounts if e-mail to the victim. The victim will receive overwhelming amount of unsolicited e-mail.

Sniffers

- A program or device that can track data as it moves over a network; used for both unlawful network administration purposes and information theft; damaging security network

Social Engineering

- Process of utilizing social skills to persuade someone to provide access credentials or other important information to an attacker in the context of information security.

Phone Phishing

- Attackers use credentials to carry out operations such as money transfers, bill payments, and loan requests.

Pharming

- Routing of legitimate web traffic to an authorized site in order to gain private information
- Uses trojans, worms, and other virus technologies

Timing Attack

- Looks through the contents of web browser's cache and places a malicious cookie on the client's computer.

Secure Software Development

- ✓Software components
- ✓System Development Life Cycle
- ✓Software Assurance
- ✓Software Design Principles

Software Development Security Problems

- ✓Buffers
- ✓Command Injection
- ✓Cross-site Scripting
- ✓Failure to Handle Errors
- ✓Failure to Protect Network Traffic
- ✓Failure to Store and Protect Data Securely
- ✓Failure to Use Cryptography Strong Random Numbers
- ✓Format Strong Problems

Software Development Security Problems

- ✓Neglecting Change Control
- ✓Improper File Access
- ✓Improper Use of SSL
- ✓Information Leakage
- ✓Integer Bugs
- ✓Race Conditions
- ✓SQL Injection
- ✓Domain Name Systems


ThankYou!