CS306: Introduction to IT Security

Fall 2020

Lab 1

September 10, 2020

1870

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

CS306: Lab sections schedule

- labs
  - CS306-Lx Thursdays

x	B	C	D	E	F
time	9:30 - 10:20	11:00 - 11:50	12:30 - 13:20	14:00 - 14:50	15:30 - 16:20
Zoom ID	91573945614	93061161569	94976630644	92834271191	94520991826
TAs	Dean, Joseph, Joshua, Uday	Dean, Devharsh, Joseph, Joshua	Dean/Devharsh, Joshua, Mohammad, Uday	Devharsh, Joseph, Mohammad, Uday	Dean, Joseph, Mohammad, Uday

Recall: The ‘IT-security’ game

- **Defenders**
  - system owners (e.g., users, administrators, etc.)
  - seek to **enforce** one or more **security properties** or **defeat** certain **attacks** → **property-based view**
- **Attackers**
  - external entities (e.g., hackers, other users, etc.)
  - seek to launch attacks that **break** a **security property** or **impose** the system to certain **threats** → **attack-based view**

Recall: Security properties

- General statements about the value of a computer system
- Examples
  - The C-I-A triad
    - **confidentiality**, **integrity, availability**
  - (Some) other properties
    - **authentication / authenticity**
    - **non-repudiation / accountability / auditability**
    - **anonymity**

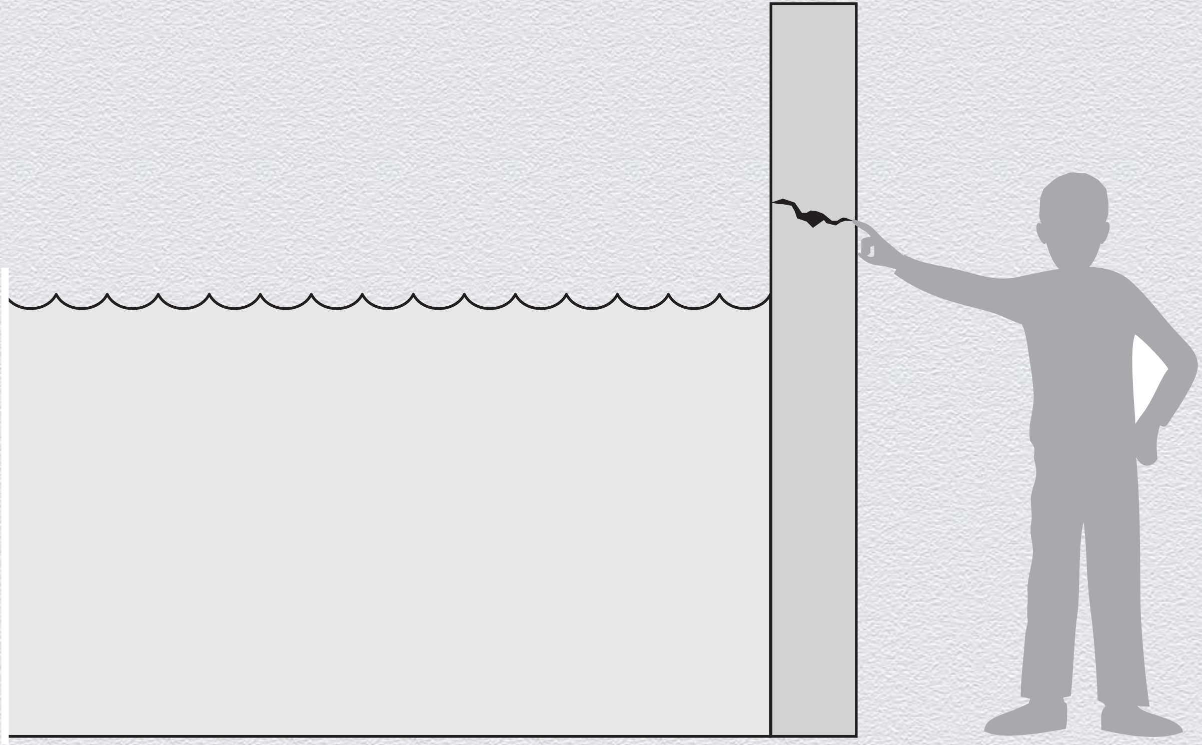
The “Vulnerability - Threat - Control” paradigm

- A **vulnerability** is a weakness that could be exploited to cause harm
- A **threat** is a set of circumstances that could cause harm
- A **security control** is a mechanism that protects against harm
  - i.e., countermeasures designed to prevent threats from exercising vulnerabilities

Thus

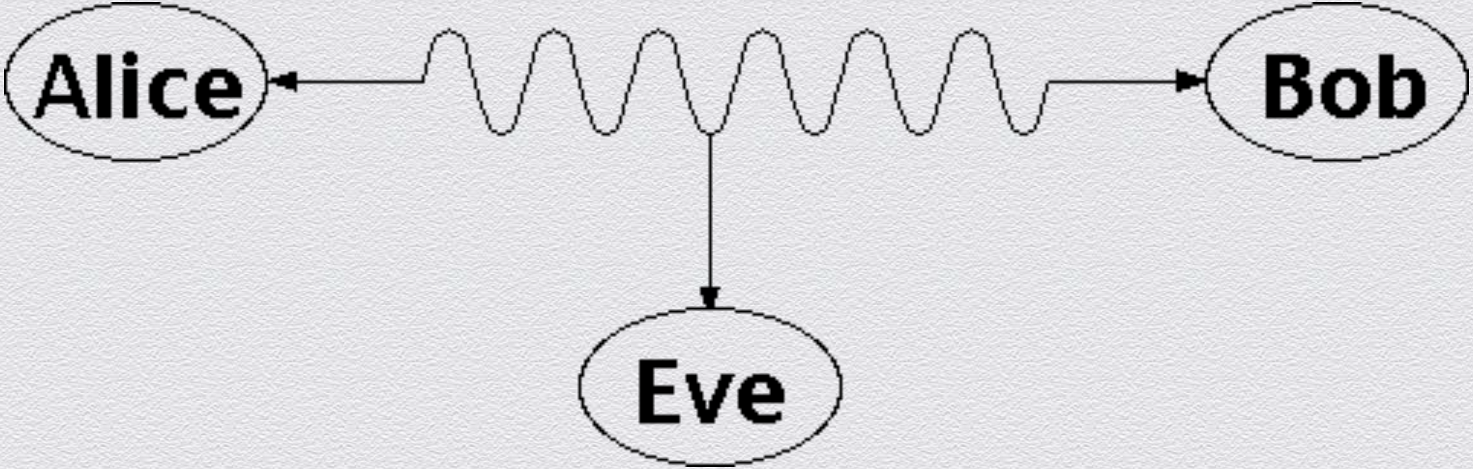
- **Attackers** seek to **exploit** vulnerabilities in order to **impose** threats
- **Defenders** seek to **block** these threats by **controlling** the vulnerabilities

A “Vulnerability - Threat - Control” example



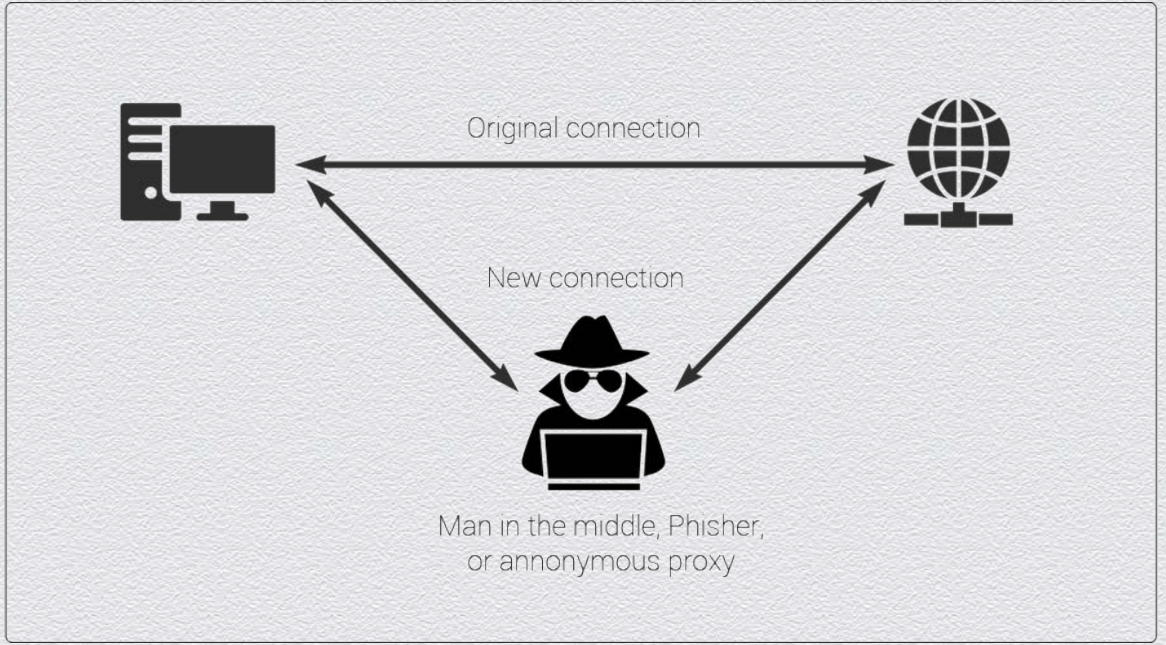
Example of threat

- **Eavesdropping:** the interception of information intended for someone else during its transmission over a communication channel



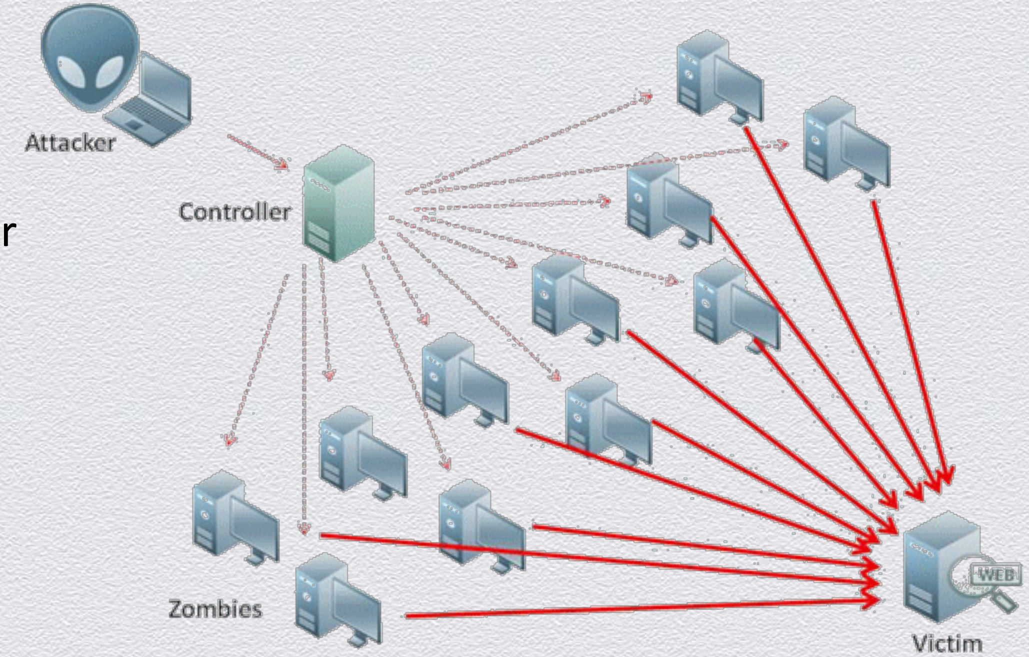
Example of threat

- **Alteration:** unauthorized modification of information
  - **Example:** the man-in-the-middle attack, where a network stream is intercepted, modified, and retransmitted



Example of threat

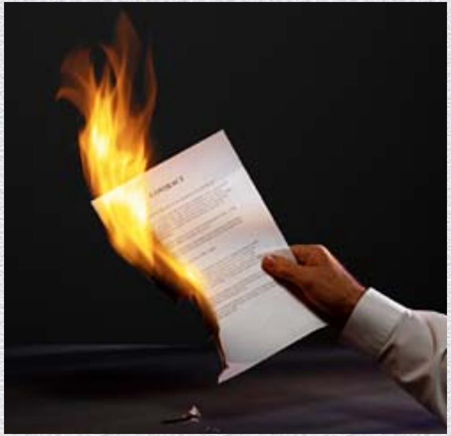
- **Denial-of-service:** the interruption or degradation of a data service or information access
  - **Example:** email **spam,** to the degree that it is meant to simply fill up a mail queue and slow down an email server



Examples of threats

- **Masquerading**: the fabrication of information that is purported to be from someone who is not actually the author
  - e.g., IP spoofing attack: maliciously altering the source IP address of a message

- **Repudiation:** the denial of a commitment or data receipt
  - this involves an attempt to back out of a contract/protocol that, e.g., requires the different parties to provide receipts acknowledging that data has been received



Example of vulnerability

- **Software bugs:** Code is not doing what is supposed to be doing
  - **Example:** Some application code is mistakenly using an algorithm for encryption that has been broken
  - **Example:** There is no checking of array bounds

Example of control: HTTPS protocol

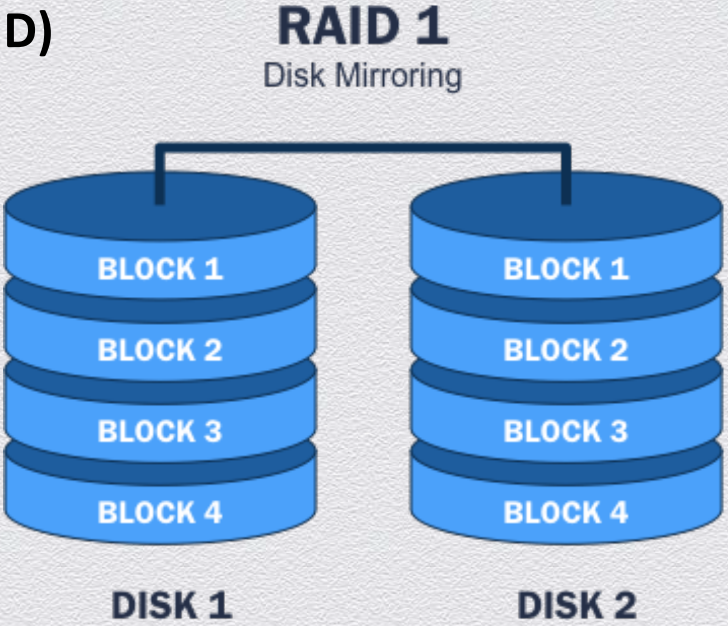
Hypertext Transfer Protocol Secure (HTTPS)

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity

Example of control: RAID technology

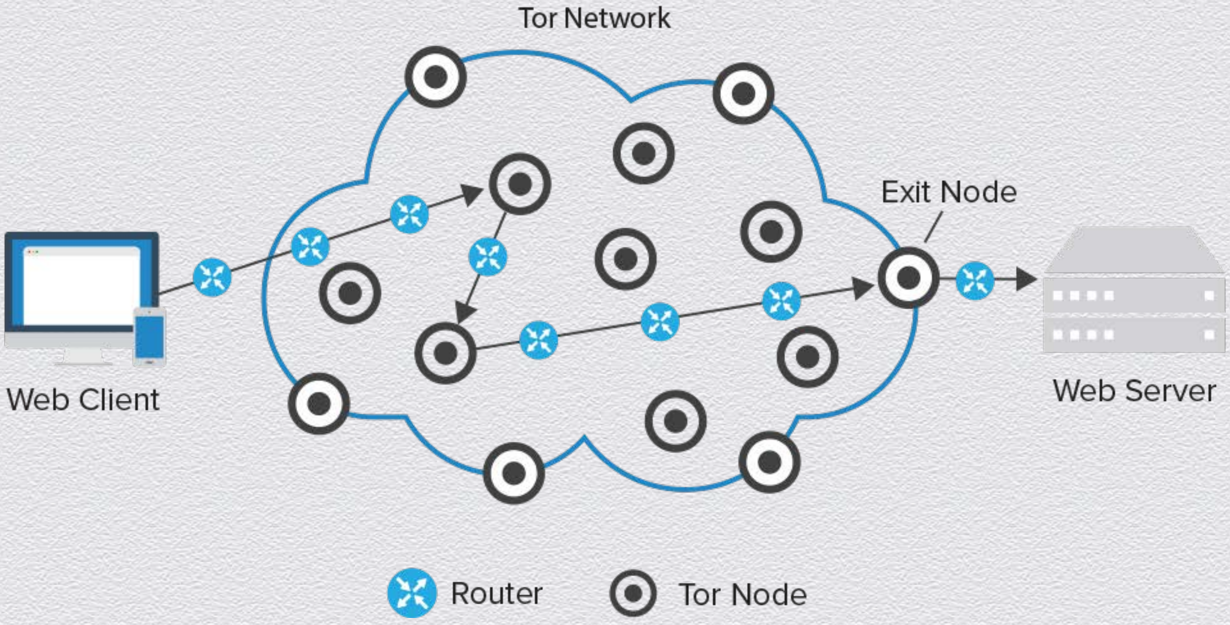
Redundant Array of Independent Disks (RAID)

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity



Example of controls: TOR protocol

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity


Tor Network
Exit Node
Web Client
Web Server
Router
Tor Node