CS306: Introduction to IT Security

Fall 2018

Lecture 1: Introduction

Instructor: **Nikos Triandopoulos**

August 28, 2018

STEVENS
INSTITUTE of TECHNOLOGY
THE INNOVATION UNIVERSITY®

Today

- Course logistics
- Introduction to the field of IT security
  - in-class discussion with a real-world example
  - coverage of basic concepts & terms

1.1 Course logistics

CS306: Topic of study

"Introduction to IT Security"

- "IT" = Information Technology
  - the study or use of information systems (especially computers, the Internet and telecommunications) for storing, retrieving, and sending information
- "IT security" = "computer security" = "cyber security"
  - the protection of information systems from theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide
- "Introduction to IT Security"
  - introductory course, broad topics w/ focus on basic tools & applications

CS306: Who can take it

- **Undergraduate** course
- Prerequisite course is **CS135** or **MA134** (i.e., discrete math)
- **Required** course for Cyber-security & Computer Science concentrations
  - in study plans of CyS sophomores & CS seniors
- **Full-credit** course (w/ grade)

PLEASE contact me any of the above does not apply to you

CS306: Lectures & labs

CS306 is offered in **2 required sessions**, each offered in **multiple sections**

- lectures
  - *Skip lunch* CS306-A, Tue 12:00pm - 14:30pm, Kidde 360 12/60
  - *Skip dinner* CS306-B, Tue 18:15pm - 20:45pm, Babbio 104 7/60
- labs
  - *Stay focused* CS306-Lx, sometime & somewhere on Thursdays

x	A	B	C	D	E	F
time	8 - 8:50	9:25 - 10:15	10:50 - 11:40	12:15 - 13:05	13:40 - 14:30	15:05 - 15:55
place	NB101	Morton 105	Kidde 360	Babbio 220	Babbio 304	Burchard 514
capacity	13/20	6/20	0/20	0/20	0/20	0/20

PLEASE contact me if you cannot enroll to any lab section

Disclaimer

- Lectures take place in 2.5h slots
  - *Skip lunch* CS306-A, Tue 12pm - 2:30pm, Kidde 360 (capacity = 60)
  - *Skip dinner* CS306-B, Tue 18:15pm - 20:45pm, Babbio 104 (capacity = 60)
- This lecture format **is highly problematic** and **undesirable for both the students and the instructor**
- It is unfortunately **unavoidable due to** existing **scheduling restrictions**
  - namely, finding two time slots that *allow both CyS sophomores and CS seniors to enroll*, without conflicting with other required CS courses, is nearly impossible
  - let alone satisfying other Institute–wide policies and finding high-capacity rooms

Please provide suggestions on what can make class experience better despite 2.5h lectures

CS306: Lectures & labs (continued)

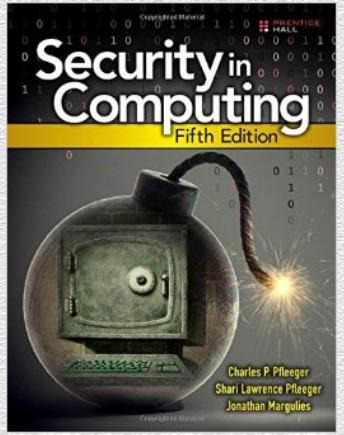
- Lecture/lab sections will cover the same materials
- Changes in lecture sections
  - **highly discouraged** due to classroom capacity
- Changes in lab sections
  - **strictly not permitted**
  - exception
    - a change is needed **due to emergency/health issues** & 2 students **can swap** labs
    - in this case, you **must notify TAs** in advance

CS306: Staff

- Instructor
  - **Nikos Triandopoulos**, ntriando@stevens.edu
  - course organization / management, lectures, assignments, grades, …
    - all mistakes will be also mine ☺
  - office hours: Tuesdays 4 – 6pm or by appointment, office: North 321
- Teaching assistants
  - TBA
  - assistance w/ labs, assignments, “help sessions” as needed, grading
  - office hours: TBA

CS306: Learning materials

- Lectures
  - lecture notes: slides in pdf available online before / after class
  - additional materials covered on whiteboard or during in-class discussions
- Required textbook
  - Security in Computing, 5th edition, by Pfleeger, Pfleeger & Margulies, Prentice Hall
  - available as hardcopy or e-book
  - available in bookstore



CS306: Course organization – what is offered

- Weekly lectures
  - materials covered w/ presentations, on whiteboard or through in-class discussions
  - two ~10 min breaks (on the 50min marks in the lecture)
- Weekly labs
  - recitation of basic concepts, discussions, preparation of homework sets
- 4 homework sets
  - revision and application of covered materials
- TA hours
- office hours by instructor

CS306: Grading (tentative*)

- 20% Participation (labs attendance & in-class quizzes)
- 20% 4 homework assignments
- 60% 2 exams (midterm & final)
- 110% Total (w/ extra credit opportunities via homework assignments)
- grading scheme (tentative*)

A	90-100
B	80-89
C	70-79

*adapted after final exam as needed to benefit the class

CS306: Course workload – what is expected from you

- Come to class regularly & participate
  - e.g., you are expected to ask questions and provide comments
- Attend weekly labs
- Hand-in homework assignments
- Pass exams
- Work independently (unless otherwise explicitly specified)
  - collaboration policy is governed by Honor System
- Provide feedback

CS306: Policies (not complete list)

- All class matters will be handled through Canvas
- Attendance of lectures & labs is required
  - only one missed lab is allowed
- Use of smartphones or other devices is not allowed in lectures/labs
  - recording of lectures/labs is not allowed
  - laptops: allowed in lectures for note taking, required in labs for assignments
- There are no make-up labs or quizzes
- Late assignments
  - 3 free late days, after which 10% per-day reduction
  - an exception may be granted by the instructor, if there is an important reason

CS306: Announcements

- Course materials will appear on Canvas
  - we'll make any effort to be complete, consistent and accurate in our updates
  - please be patient as we set up our processes and finalize course materials
  - communication (e.g., questions about course materials, announcements, etc.)
- No lab session this week
- TA hours & office hours will start next week

CS306: Tentative Syllabus

Week	Date	Topics	Reading	Assignment
1	Aug 28	Introduction	Chapter 1	-
2	Sep 4	Symmetric-key crypto I		
3	Sep 11	Symmetric-key crypto II		
4	Sep 18	Public-key crypto I		
5	Sep 25	Public-key crypto II		
6	Oct 2	Access control & authentication		
–	Oct 9	**No class** (Monday schedule)		
7	Oct 16	**Midterm** (closed books)	All materials covered	

CS306: Tentative Syllabus (continued)

Week	Date	Topics	Reading	Assignment
8	Oct 23	Software & Web security		
9	Oct 30	Network security		
10	Nov 6	Database security		
11	Nov 13	Cloud security		
12	Nov 20	Privacy		
13	Nov 27	Economics		
14	Dec 4	Legal & ethical issues		
15	Dec 11 (or later)	**Final** (closed books)	All materials covered*	

* w/ focus on what covered after midterm

CS306: Course outcomes

- Terms
  - describe common security terms and concepts
- Cryptography
  - state basics/fundamentals about secret and public key cryptography concepts
- Attack & Defense
  - acquire basic understanding for attack techniques and defense mechanisms
- Impact
  - acquire an understanding for the broader impact of security and its integral connection to other fields in computer science (such as software engineering, databases, operating systems) as well as other disciplines including STEM, economics, and law
- Ethics
  - acquire an understanding for ethical issues in cyber-security

Questions?

- Please ask questions during class!

Today

- Course logistics
  - topic of study, enrollment eligibility, sessions
  - staff, learning materials, course organization
  - expectations, grading, policies, announcements
  - syllabus overview, course objectives/outcomes
- Introduction to the field of IT security
  - in-class discussion with a real-world example
  - coverage of basic concepts & terms

1.2 Secure outsourced computation

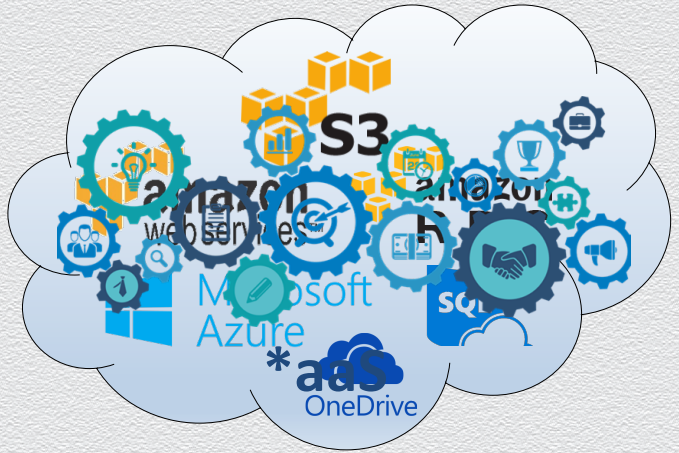
Another example: Tax return preparation…

Involves information collection & processing

- calculate financial data
  - payroll, profits, stock quotes, …
- manage data
  - search emails, store records, …
- submit – done!

… by many unknown machines!

Data & computation outsourcing



Cloud-based services

- hardware, OS, software, apps, …
- storage, computation, databases, analytics, …

Transformative multi-platform technology

- businesses, organizations or individuals
- client-server, distributed, P2P, Web-based, …

Internet protocols

social networks

big-data analytics

sharing economy

FinTech

Security consequences

Fact: Untrusted interactions

- information is processed outside one's administration control or "trust perimeter"

Risk: Falsified / leaked information

- information may unintentionally altered by or shared with unauthorized entities

Goal: Integrity / privacy safeguards for outsourced assets

- need to protect information against change, damage / unauthorized access

What can go wrong?

Fact: Untrusted interactions

- information is processed outside one's administration control or "trust perimeter"

Risk: Falsified / leaked information

- information may unintentionally altered by or shared with unauthorized entities

Goal: Integrity / privacy safeguards for outsourced assets

- need to protect information against change, damage / unauthorized access

Threats:

- misconfigurations, erroneous failures, limited liability
- economic incentives of cost-cutting providers
- compromises, attacks, advanced persistent threats (APTs)

Limited liability

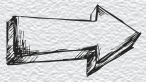
"[We will] not be responsible for any damages arising in connection with any unauthorized access to, alteration of, or the deletion, destruction, damage loss or failure to store any of your content or other data."

Amazon Web Services customer agreement

Advanced Persistent Threats (APTs)

Sophisticated well-targeted cyber-attack campaigns

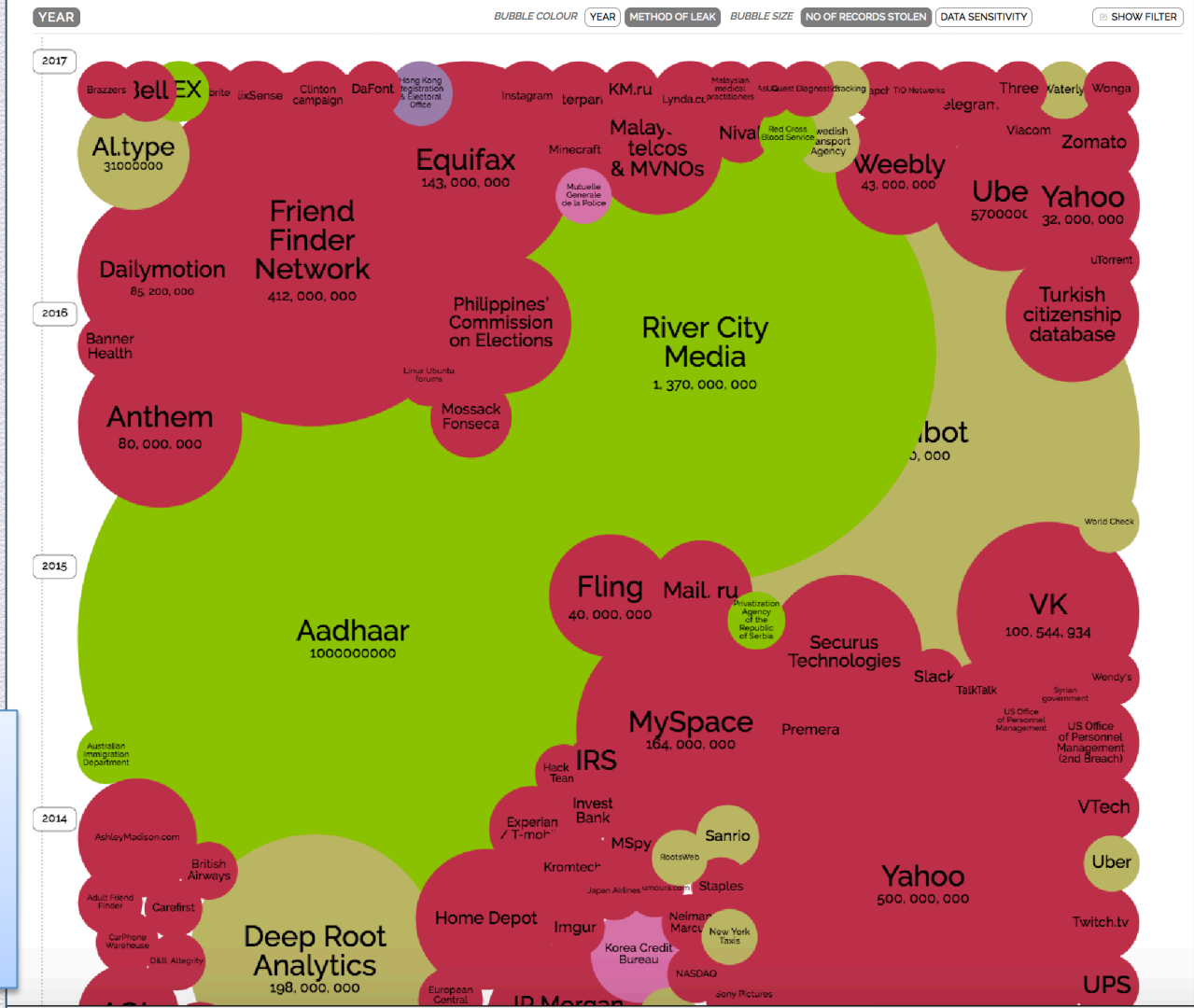
- aim for unauthorized data manipulation or exfiltration
- employ rich attack vectors & highly adaptive strategies
  - social engineering
  - zero-day vulnerabilities
  - low-and-slow progression
  - intelligence



extremely hard-to-defend
or even hard-to-detect

…	
RSA	(2011)
Bit9	(2013)
Dyn	(2016)
Equifax	(2017)
…	

World's biggest data breaches



"Information is beautiful"
by David McCandless

- world's biggest data breaches
  - losses > 30K records
  - up to 2/2/18

Real cases: Threats against integrity Vs. confidentiality

Figure 6: VERIS A⁴ grid depicting associations between actors, actions, assets, and attributes

	External.Malware	External.Hacking	External.Social	External.Misuse	External.Physical	External.Error	External.Env	Internal.Malware	Internal.Hacking	Internal.Social	Internal.Misuse	Internal.Physical	Internal.Error	Internal.Env	Partner.Malware	Partner.Hacking	Partner.Social	Partner.Misuse	Partner.Physical	Partner.Error	Partner.Env
Server.Conf	35%	48%	23%	2%	.	1%		.	2%	2%	5%	1%	2%		.	.	.	1%		.	
Server.Integ	35%	41%	23%	2%	.	1%		.	2%	2%	3%	1%	2%		.	.	.	.			
Server.Avail	1%	2%	1%			.		.	.		.	.	.								
Network.Conf	.	.	.	.	1%	.		.	.		.		.								
Network.Integ	.	.	.	.	1%	.		.	.		.		.								
Network.Avail		.	.			.			.				.								
User.Conf	35%	36%	22%	1%	32%	.		.	.	.	3%	1%	.					.			
User.Integ	35%	34%	22%	1%	32%	.		.	.	.	1%	1%	.					.			
User.Avail	.	.	.	.	1%			.	.		1%	.									
Media.Conf	.	.	2%	2%	1%					2%	5%	2%	.					.			
Media.Integ	.	.	2%	2%	1%					2%	3%	1%	.								
Media.Avail			.	.	1%	✓				.	.	1%									
People.Conf	22%	24%	29%	4%	1%			.		4%	4%	1%				.	.	.			
People.Integ	22%	24%	29%	4%	1%			.		4%	4%	1%				.	.	.			
People.Avail	.	2%	2%	1%	1%			.		.	1%	1%									

Data Breach Investigations Report by Verizon (2013)

- servers are a high-value target
- compromises / attacks affect both confidentiality and integrity

The “new” big threat: Data manipulation

Newest cyber threat will be data manipulation, US intelligence chief says

theguardian

- James Clapper calls data deletion or manipulation ‘next push of the envelope’
- US digital networks currently threatened by wide-scale data theft

Cyber security chief: Manipulation of data by hackers may be next threat

PITTSBURGH TRIBUNE-REVIEW

Cybersecurity

Former NSA chief: Data manipulation an 'emerging art of war'

FCW THE BUSINESS OF FEDERAL TECHNOLOGY

But what happens when suddenly our data is manipulated, and you no longer can believe what you’re physically seeing?

THE WALL STREET JOURNAL WSJ

a Digital Pearl Harbor

US Officials’ View

- data manipulation is the new big threat

Today

- Course logistics
  - topic of study, enrollment eligibility, sessions
  - staff, learning materials, course organization
  - expectations, grading, policies, announcements
  - syllabus overview, course objectives/outcomes
- Introduction to the field of IT security
  - in-class discussion with a real-world example
  - coverage of basic concepts & terms

1.3 Basic security concepts & terms

What is IT security?

IT security is the prevention of, or protection against

- access to information by unauthorized recipients
- intentional but unauthorized destruction or alteration of that information

Definition from: *Dictionary of Computing,* Fourth Ed.
(Oxford: Oxford University Press 1996).

IT security (informal definition)

- the protection of information systems from
  - theft or damage to the hardware, the software, and to the information on them, as well as from disruption or misdirection of the services they provide
  - any possible threat

The 'IT-security' game: What's at stake?

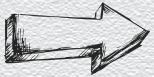
- Computer systems comprise assets that have (some) **value**
  - e.g., laptops store vast personal or important information (files, photos, email, …)
  - personal, time dependent and often imprecise (e.g., monetary Vs. emotional)
- Valuable assets deserve **security protection**
  - to **preserve** their **value**, ⇒ expressed as a **security property**
    - e.g., personal photos should always be accessible by their owner
  - or to **prevent** (undesired) **harm** ⇒ examined as a concrete **attack**
    - e.g., permanent destruction of irreplaceable photos

The ‘IT-security’ game: Who are the players?

- **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

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**

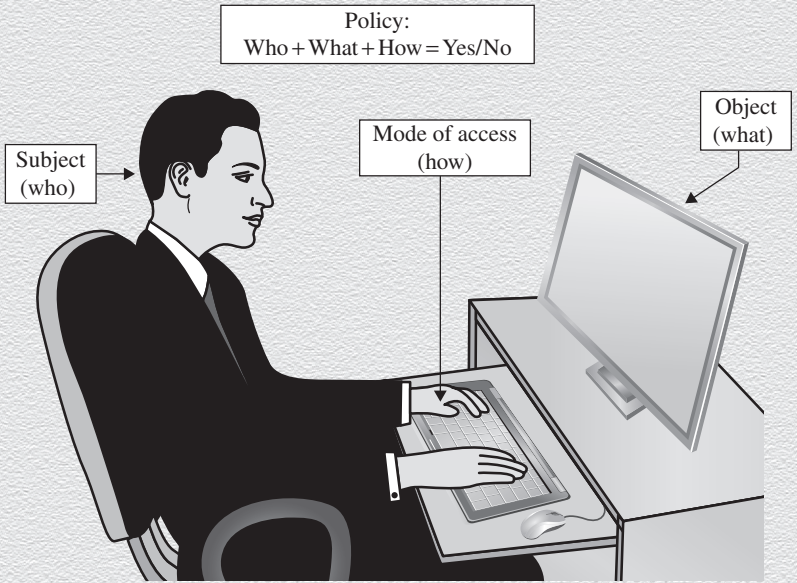
The C-I-A triad

- Captures the three fundamental properties that make any system valuable

Computer security seeks to prevent unauthorized viewing (confidentiality) or modification (integrity) of data while preserving access (availability)

Confidentiality

- An asset is viewed only by authorized parties
  - e.g., conforming to originally-prescribed “read” rules <subject, object, access mode, policy> via access control
  - some other tools
    - encryption, obfuscation, sanitization, …



Integrity

- An asset is modified only by authorized parties
  - beyond conforming to originally-prescribed “write” access-control rules
  - precise, accurate, unmodified, modified in acceptable way by authorized people or processes, consistent, meaningful and usable
  - authorized actions, separation & protection of resources, error detection & correction
  - some tools
    - hashing, MACs

Availability

- An asset can be used by any authorized party
  - usable, meets service's needs, bounded waiting/completion time, acceptable outcome
  - timely response, fairness, concurrency, fault tolerance, graceful cessation (if needed)
  - some tools
    - redundancy, fault tolerance, distributed architectures

Authenticity

- The ability to determine that statements, policies, and permissions issued by persons or systems are genuine
  - some tools
    - digital signatures (cryptographic computations that allow entities to commit to the authenticity of their documents in a unique way)
      - achieve non-repudiation (authentic statements issued by some person or system cannot be denied)

Anonymity

- The property that certain records/transactions cannot be attributed to any individual
- some tools
  - aggregation
    - disclosure of statistics on combined data from many individuals that cannot be tied to any individual
  - proxies
    - trusted agents interacting on behalf on an individual in untraceable way
  - pseudonyms
    - fictional identities, known only to a trusted party, that fill in for real identities

Discussion

1. Cloud-based storage
2. e-banking
   - What is a **valued asset**?
   - What does it mean to **preserve** this value?
   - What is a corresponding desired **security property**?
   - What is a **harm** that must be prevented?

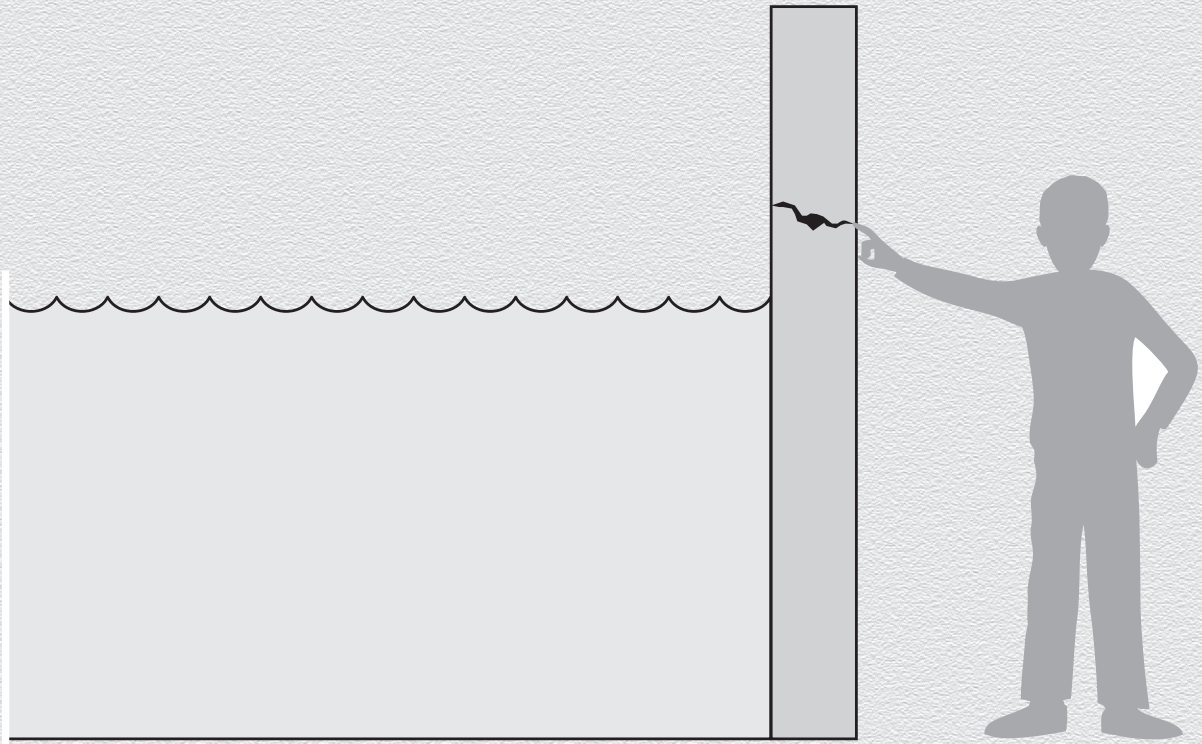
The “Vulnerability - Threat - Control” paradigm

- 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

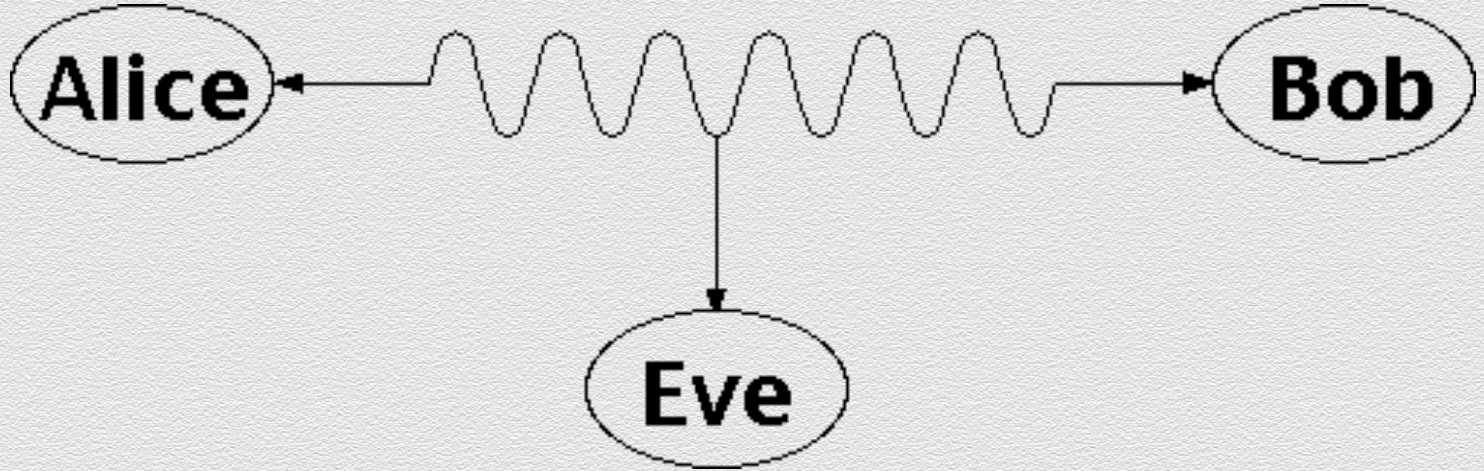
- **Attackers** seek to **exploit** vulnerabilities in order to **impose** threats
- **Defenders** seek to **block** these threats by **controlling** the vulnerabilities

A “Vulnerability - Threat - Control” example



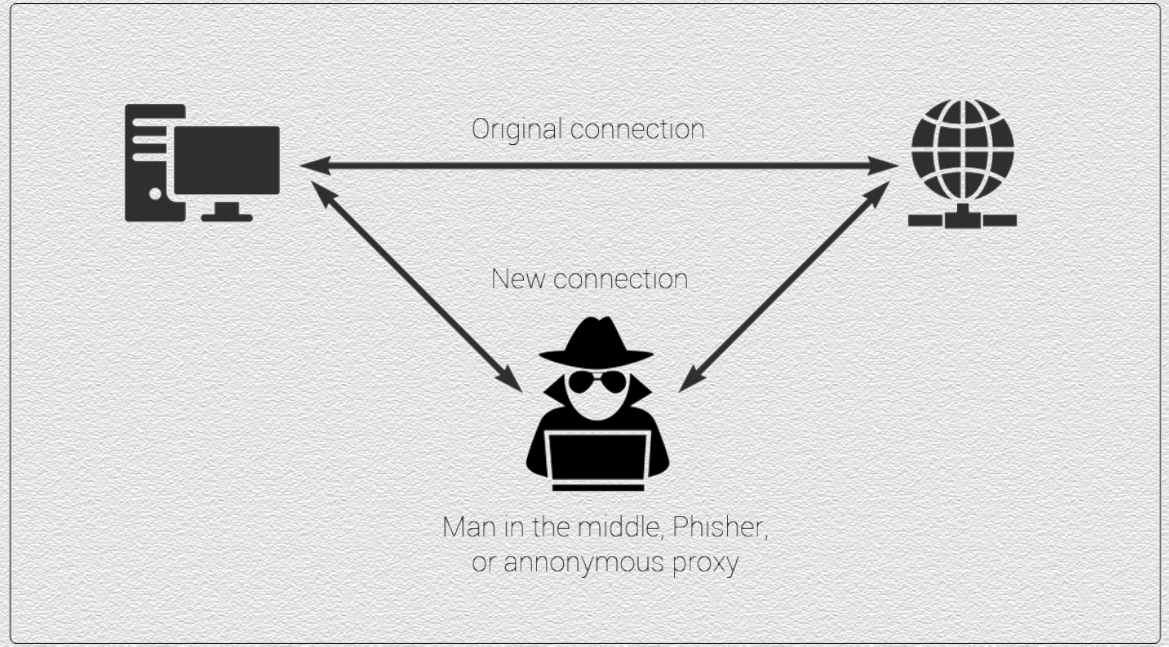
Example of threat

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



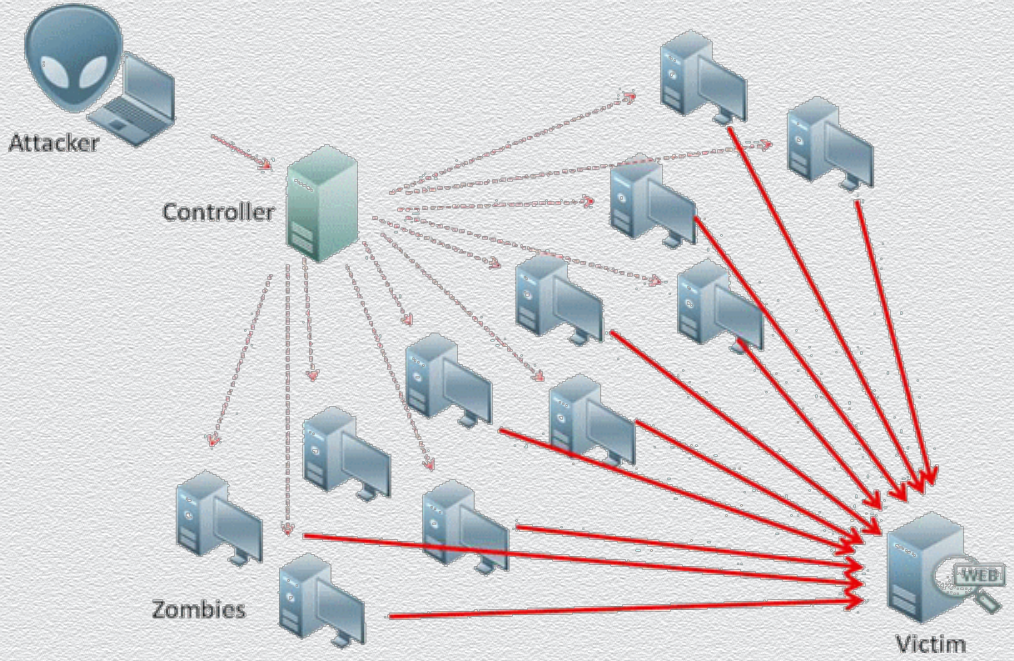
Example of threat

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



Example of threat

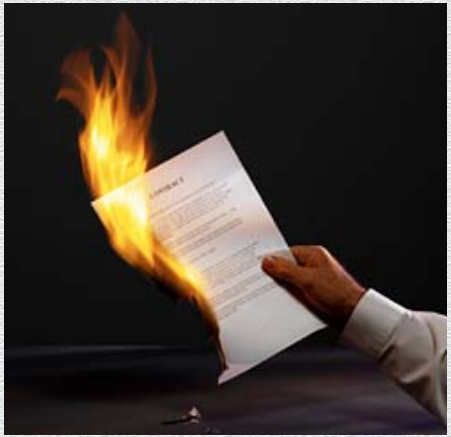
- **Denial-of-service:** the interruption or degradation of a data service or information access
  - **Example:** email **spam,** to the degree that it is meant to simply fill up a mail queue and slow down an email server



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



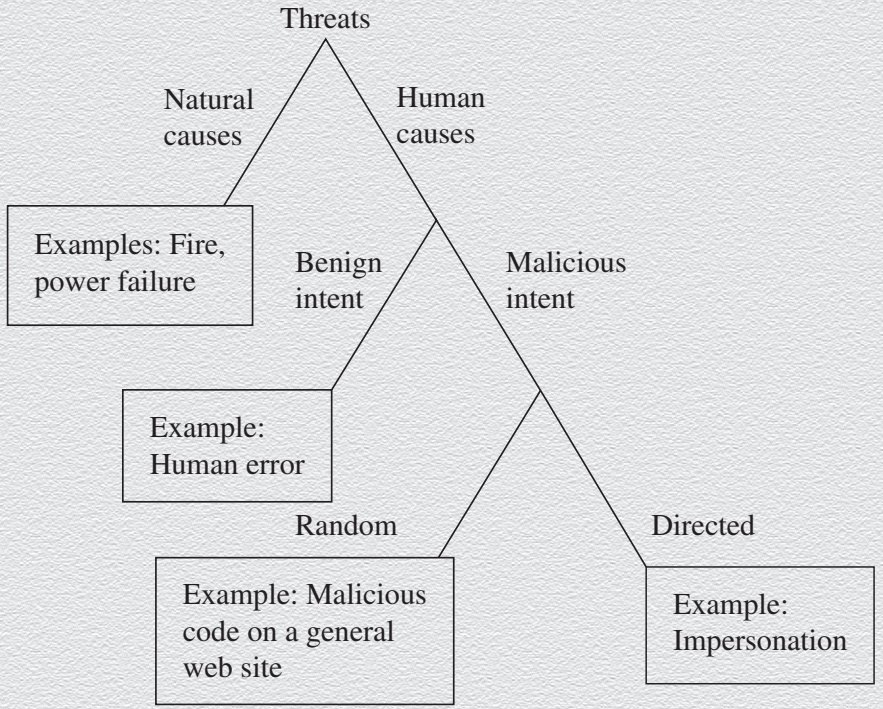
Example of vulnerability

- **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

An hard-to-win game: Varied threats

Threats

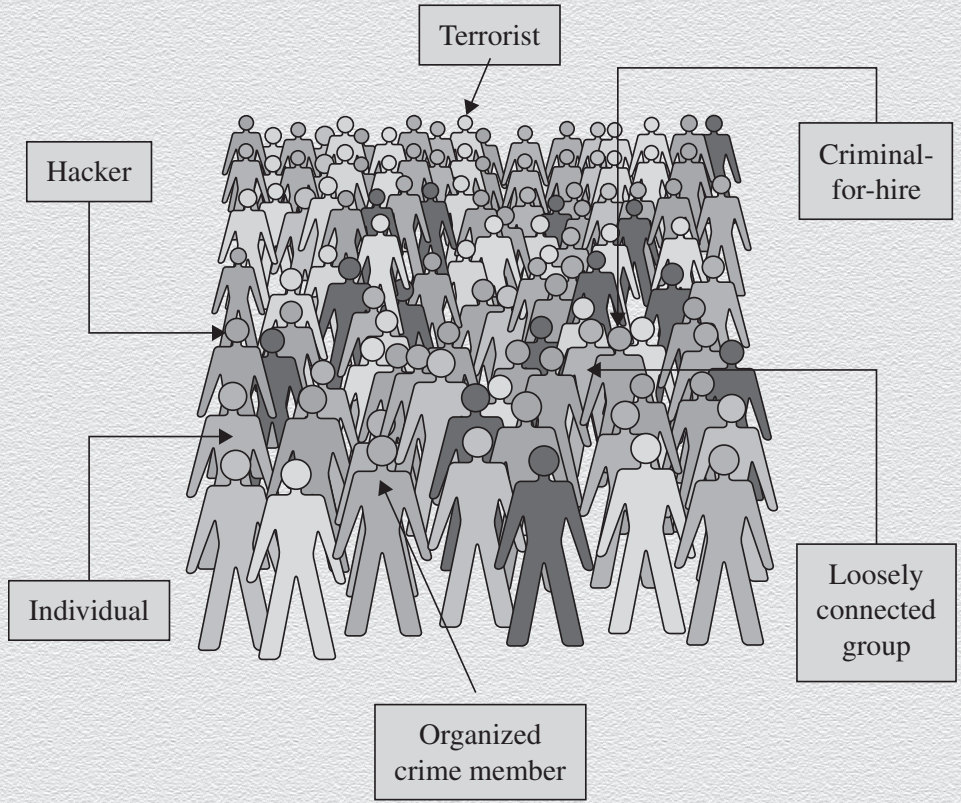
- from natural to human
- from benign to malicious
- from random to targeted (APTs)



A hard-to-win game: Unknown enemy

Attackers

- beyond isolated “crazy” hackers
- organized groups/crime
  - may use computer crime (e.g., stealing CC#s) in order to finance other crimes
- terrorists
  - computers/assets as target, method, enabler, or enhancer

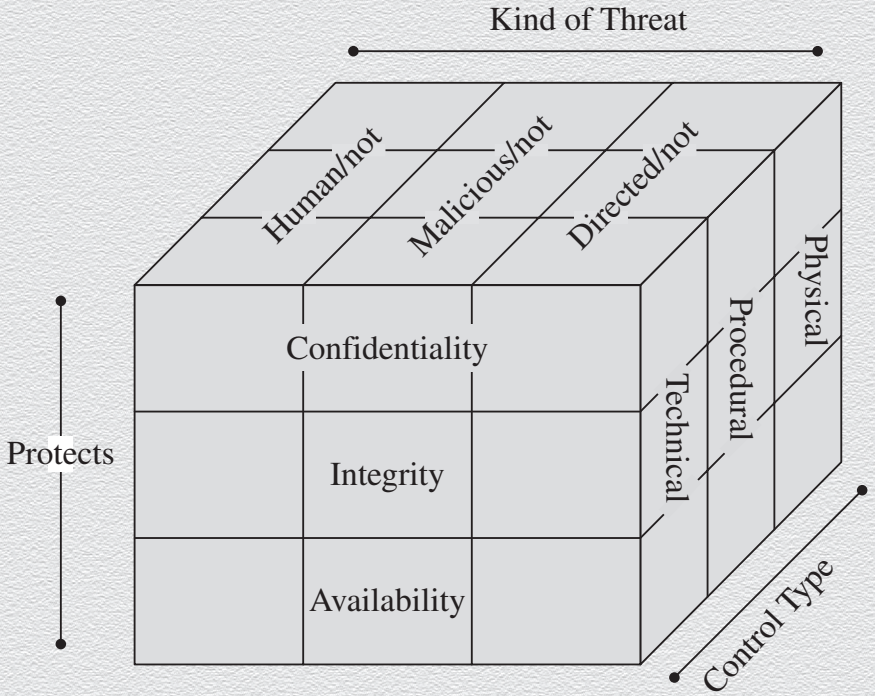


A hard-to-win game: Choose your battle

Risk management

- choose priorities
  - which threats to control
    - estimate possible harm & impact
  - what / how many resources to devote
    - estimate solution cost & protection level
- consider trade-offs balancing cost Vs. benefit
- compute the residual risk
  - decide on transfering risk or doing nothing

Never a “one-shot” game



A hard-to-win game: Best-effort approach

Deciding on controls relies on incomplete information

- likelihood of attack and impact of possible harm is impossible to measure perfectly
- full set of vulnerabilities is often unknown
  - weak authentication, lack of access control, errors in programs, etc.
- system's attack surface is often too wide
  - physical hazards, malicious attacks, stealthy theft by insiders, benign mistakes, impersonations, etc.

A useful strategy: The "method – opportunity – motive" view of an attack

- **deny any of them and the attack will (likely) fail**

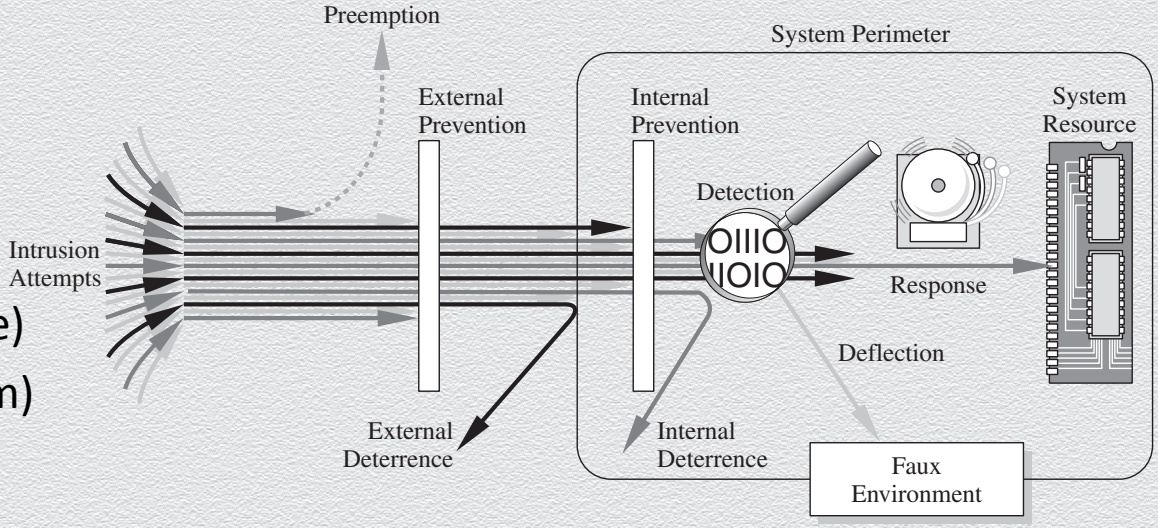
A hard-to-win game: Best-effort approach (continued)

Controls offer a wide range of protection level / efficacy

- they counter or neutralize threats or remove vulnerabilities in different ways

Types of controls

- prevent (attack is blocked)
- deter (attack becomes harder)
- deflect (change target of attack)
- mitigate (make impact less severe)
- contain (stop propagation of harm)
- detect (real time/after the fact)
- recover (from its effects)



Hard to balance cost/effectiveness of controls with likelihood/severity of threats

Example of control: HTTPS protocol

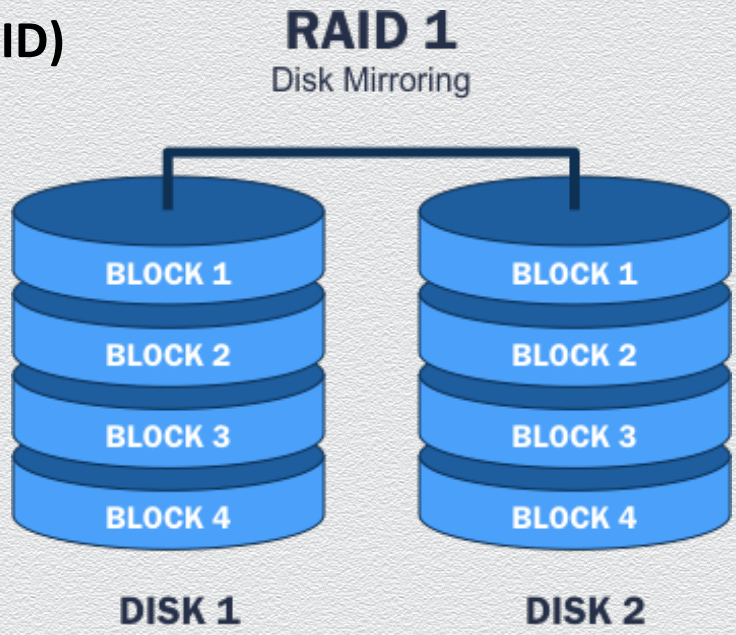
Hypertext Transfer Protocol Secure (HTTPS)

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity

Example of control: RAID technology

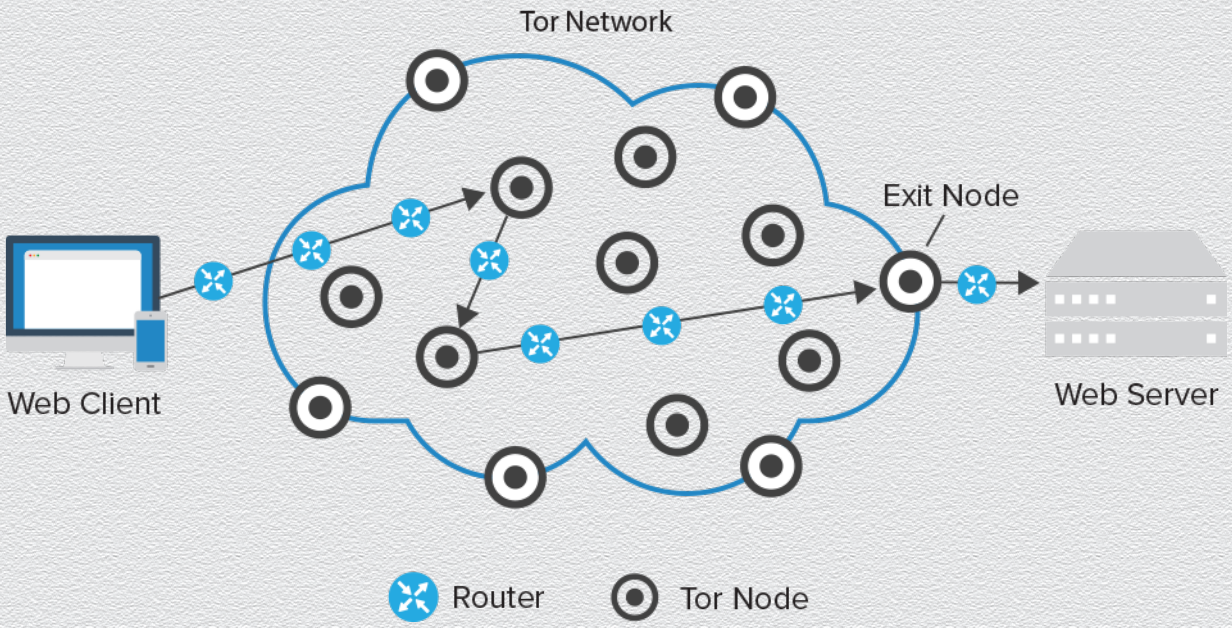
Redundant Array of Independent Disks (RAID)

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity



Example of controls: TOR protocol

- Confidentiality
- Integrity
- Availability
- Authenticity
- Anonymity



As we will see: Exciting times to study (or work in) IT Security!

Relevance to practice & real-world importance

- plethora of real-world problems & real needs for security solutions
- combination of different research areas within CS and across other fields
- multi-dimensional topic of study
  - protocol design, system building, user experience, social/economic aspects
- wide range of perspectives
  - practical / systems – foundations / theory, attacker's Vs. defender's view