Cybersecurity

COSC 3371

Instructor: Aron Laszka

Outline for Today

1. Basic information
   - course organization and help
   - materials, textbooks, references
   - grading policy (homeworks and exams)
   - prerequisites
2. Motivation
   Why is security important?
3. Core security concepts and goals
4. Challenges
   Why is security difficult?

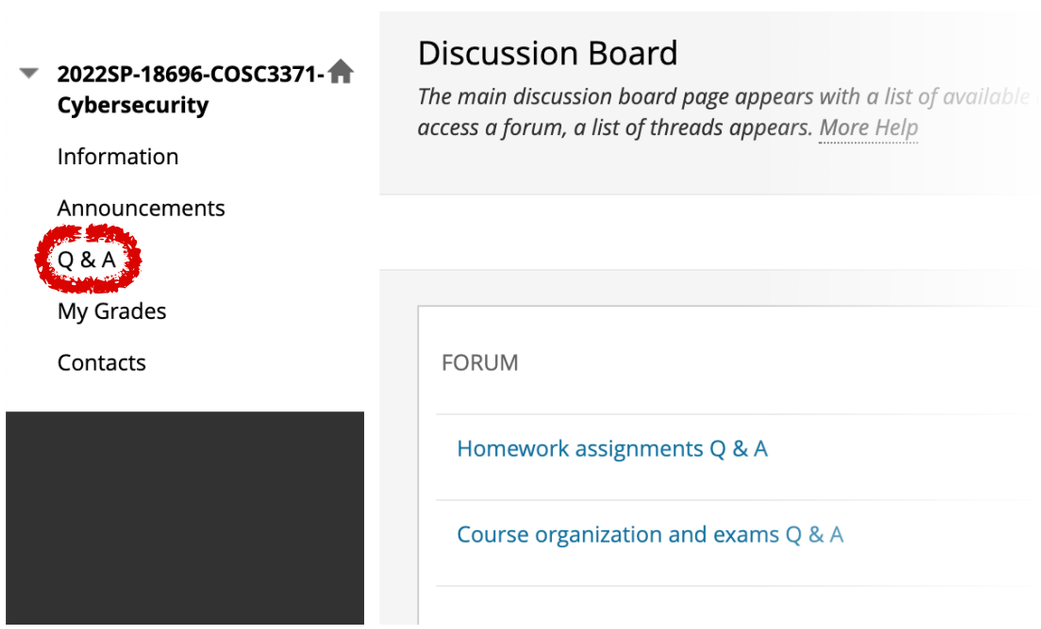
Course Information

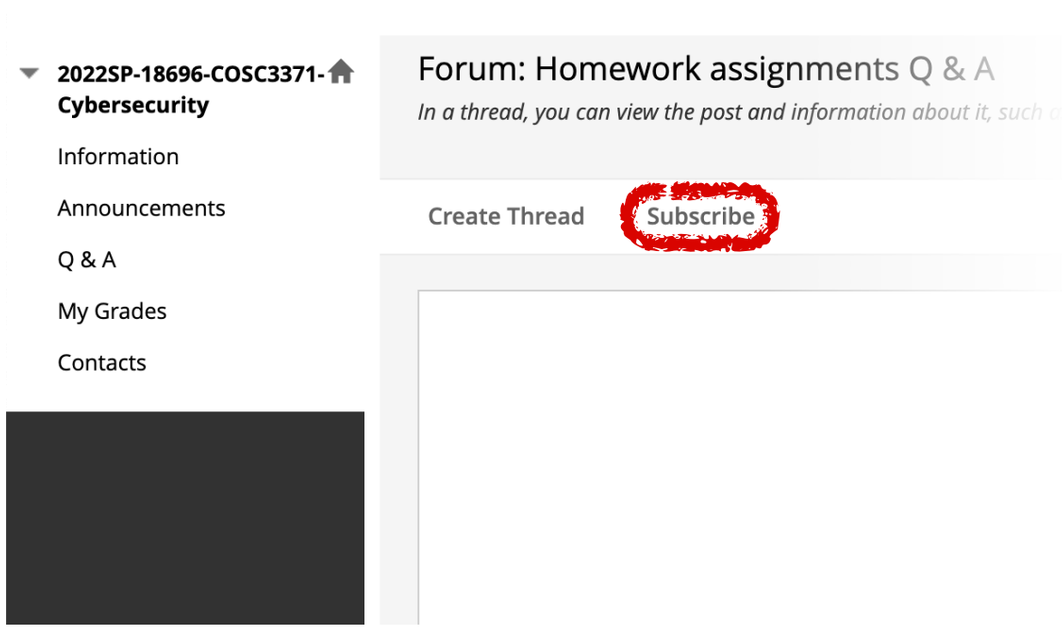
- Lectures
  - **Tuesday** and **Thursday** from **11:30am** to ~1pm

   **face-to-face** in **S105** and, for the first two weeks,  online on **Zoom**
- Blackboard (https://elearning.uh.edu)
  - slides (final version available **after** the lecture) and lecture recordings
  - homework assignments
  - announcements, exam samples, etc.
- Instructor:
  Aron Laszka (alaszka@uh.edu)
- Teaching assistants:
  Farzana Yasmin (fyasmin2@uh.edu) and Shanto Roy (sroy10@uh.edu)

Questions & Help

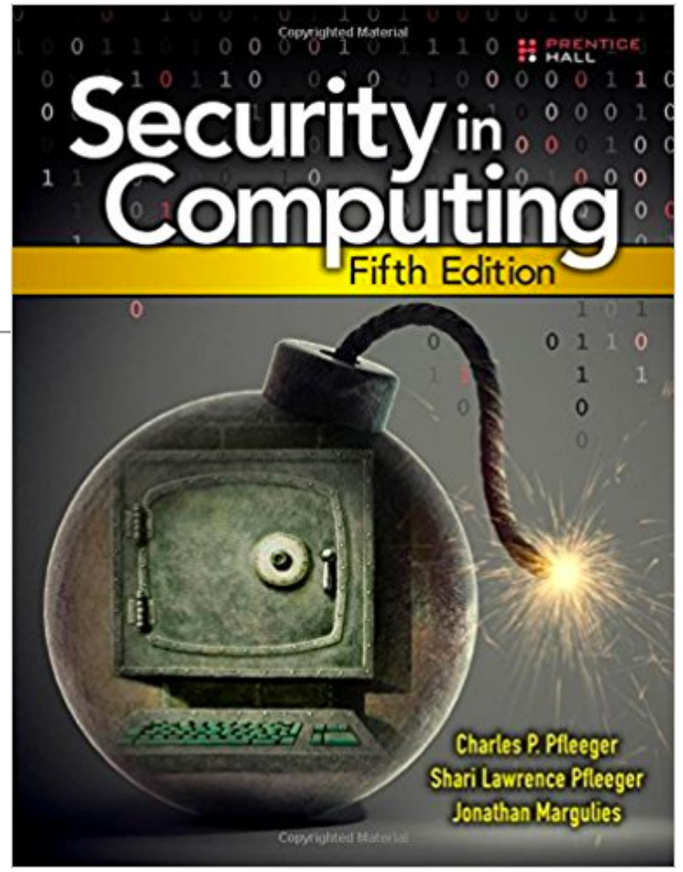
- Office hours (instructor)
  - in person or online (Zoom, Skype, Teams, *etc.*)
  - by appointment (just send an e-mail to alaszka@uh.edu)
- Blackboard Q&A forum





  - please do not post questions about particular solutions
- *Please feel free to ask questions in class!*

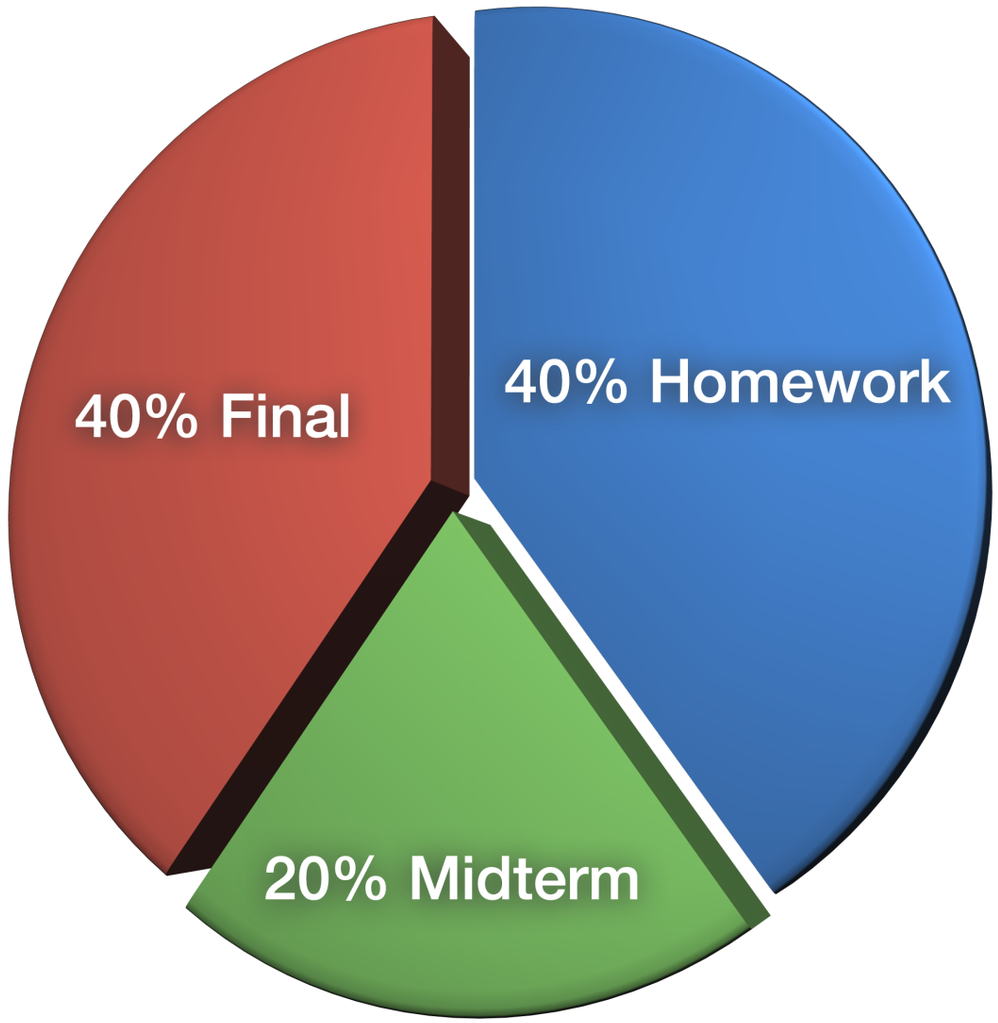
Textbooks and References



- Textbooks (recommended, but **not required**)
  - *Security in Computing* (5th Edition) by Charles P. Pfleeger, Shari Lawrence Pfleeger, Jonathan Margulies
  - *Cryptography and Network Security: Principles and Practice* (6th, 7th, or 8th Edition) by William Stallings
- Reference books
  - *Computer Security: Art and Science*, by Matthew A. Bishop
  - *Network Security: Private Communication in a Public World* (2nd Edition), by Charlie Kaufman, Radia Perlman, Mike Speciner
  - *Security Engineering: A Guide to Building Dependable Distributed Systems* (2nd Edition), by Ross J. Anderson
  - *The Web Application Hacker's Handbook: Discovering and Exploiting Security Flaws* (2nd Edition), by Dafydd Stuttard and Marcus Pinto

Grading Policy

- **Homework assignments: 40%**
  - 5 assignments throughout the semester
  - must be solved **individually**
- Midterm exam: **20%**
  - closed-book
- Final exam: **40%**
  - closed-book



Homework Assignments (40%)

- Five homework assignments (see schedule)
- At least **two weeks** to complete each
- **No deadline extension** (seriously)
- All assignments will be managed through Blackboard

Week	Class Dates	Assignments
1	January 18, 20	
2	January 25, 27	
3	February 1, 3	HW1 out
4	February 8, 10	
5	February 15, 17	HW1 in
6	February 22, 24	
7	March 1, 3	Midterm exam
8	March 8, 10	
9	*Spring break*	
10	March 22, 24	HW2 out
11	March 29, 31	HW3 out
12	April 5, 7	HW2 in, HW4 out
13	April 12, 14	HW3 in
14	April 19, 21	HW4 in, HW5 out
15	April 26, 28	
16		HW5 in
17	May 10	Final exam

Midterm and Final Exams (60%)

- Midterm exam (20%)
  - **March 1** (Tuesday) **during class**
  - covers weeks 1 - 5
  - closed book, no electronic aids
- Final exam (40%)
  - **May 10** (Tuesday) from **11am**
  - covers weeks 6 - 15
  - closed book, no electronic aids

Week	Class Dates	Assignments
1	January 18, 20	
2	January 25, 27	
3	February 1, 3	HW1 out
4	February 8, 10	
5	February 15, 17	HW1 in
6	February 22, 24	
7	March 1, 3	Midterm exam
8	March 8, 10	
9	*Spring break*	
10	March 22, 24	HW2 out
11	March 29, 31	HW3 out
12	April 5, 7	HW2 in, HW4 out
13	April 12, 14	HW3 in
14	April 19, 21	HW4 in, HW5 out
15	April 26, 28	
16		HW5 in
17	May 10	Final exam

Prerequisites

- *Official prerequisite*:
  Operating Systems (COSC 3360)

- Programming skills & languages
  - basic C and Java or Python
  - very basic SQL, Javascript, and PHP
- Basic network and web knowledge
  - IP, TCP, UDP, DNS, HTTP, HTML, SMTP
- Mathematical background
  - basics of probability and number theory

lectures will contain short tutorials on these topics

Examples

- C

```
void func() {
  char buffer[16];
  printf(“Input: “);
  gets(buffer);
}

void main() {
  func();
}
```

- SQL

```
INSERT INTO users (user_id, name) VALUES (0, 'John Doe');
```

- PHP

```
<?php
 $username = $_POST["username"];
 $password = $_POST["password"];
 if (check_password($username, $password))
   echo("Welcome " . $username . "!");
?>
```

Feedback

- *Your feedback is appreciated!*
  - both during and after the semester
- Online survey (anonymous):
  `https://forms.gle/JGbNCmCsU69iWaTv8`
  - available during and after the semester
- Feedback is very welcome in other forms as well
  - for example, via e-email

Foundations of Security

Course objective:

provide an introduction to cybersecurity principles and practices

- understand key concepts in security
- learn widely used security protocols and tools
- know about common security issues and their countermeasures

2. Motivation

Why is cybersecurity important?

Economic and Financial Impact of Cyber Incidents

- Council of Economic Advisers, Exec. Office of the President [2018]: "*We estimate that malicious cyber activity cost the U.S. economy between* ***$57 billion and $109 billion***"

- McAfee (Intel Security Group) [2020]: "*Global losses from cybercrime now total over* ***$1 trillion****, a more than* ***50 percent increase*** *from 2018*"

- CISCO [2018]: "***65%*** *of email is* ***spam***"

- IBM Cost of Data Breach Report [2020]: "*average total cost of a data breach [is]* ***$3.86 million*** *this year*"

- *Example:* 2017 Equifax data breach cost the company around **$1.4 billion** plus legal fees

Privacy Impact

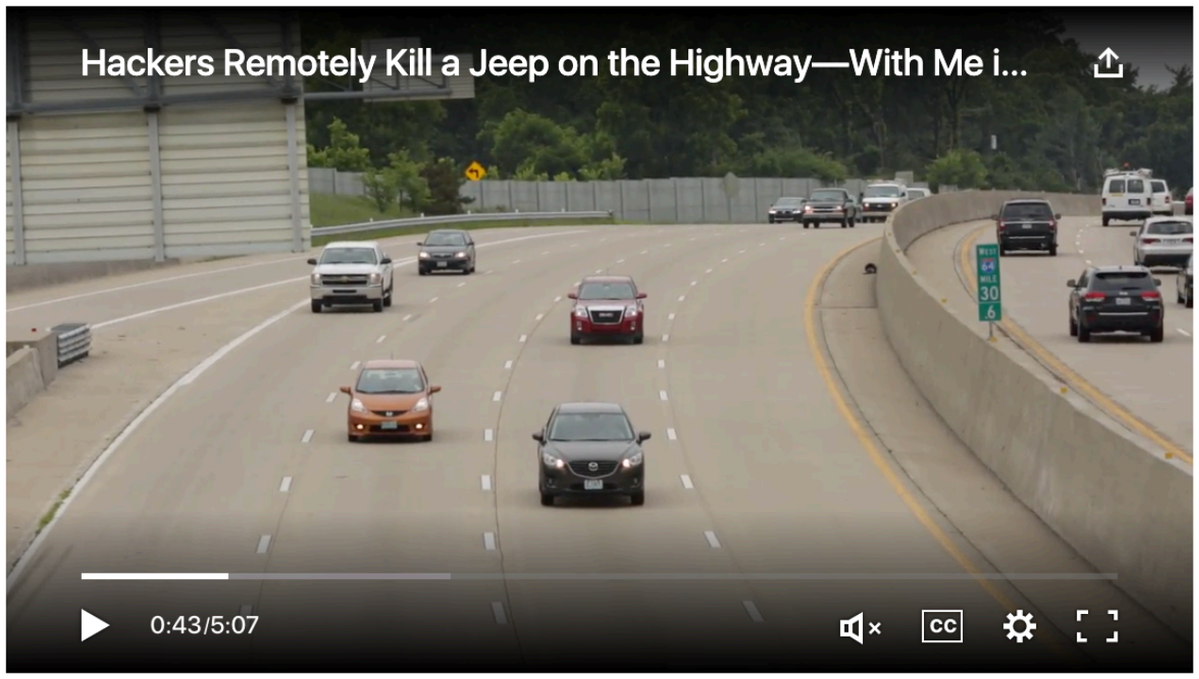
- 2013 Yahoo! data breach
  - **3 billion user accounts** were affected, confirmed in October 2017
  - including names, e-mail addresses, dates of birth, phone numbers, etc.
- 2018 Marriott data breach
  - up to **500 million records**
  - including payment information, names, mailing addresses, phone numbers, e-mail addresses, passport numbers
- 2021 LinkedIn data scraping
  - **700 million user records** scraped (e-mail addresses, phone numbers, geolocation records, genders, and other social media details)
- Healthcare data breaches
  - more than **40 million U.S. healthcare records** compromised in 2021 (`https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf`)

Physical Impact

- Stuxnet worm
  - targeted Iranian uranium enrichment fa
  - subtly increased the pressure on spinni **one-fifth of Iran's nuclear centrifuges**
- Ukrainian power grid
  - on December 23, 2015, three Ukrainian suffered a sophisticated and targeted c
  - attackers first compromised corporate Word documents with malicious macro
  - using credentials harvested from the co attackers could remotely log into contr
  - by opening circuit breakers at substatio
- "*Hackers Remotely Kill a Jeep on the Highway*" (WIRED, 2015)
  - demonstration of remote wireless attack by security researchers

ANDY GREENBERG SECURITY 07.21.15 06:00 AM

HACKERS REMOTELY KILL A JEEP ON THE HIGHWAY—WITH ME IN IT



I WAS DRIVING 70 mph on the edge of downtown St. Louis when the exploit began to take hold.

Though I hadn't touched the dashboard, the vents in the

Security Awareness

- Security depends on **all system / software lifecycle phases**
  - requirements engineering
  - system architecture and design
  - development
  - testing
  - operations
  - maintenance
  - …
- If you work with any information or communications technology, you **should be aware of cybersecurity issues** (or bad things might happen…)

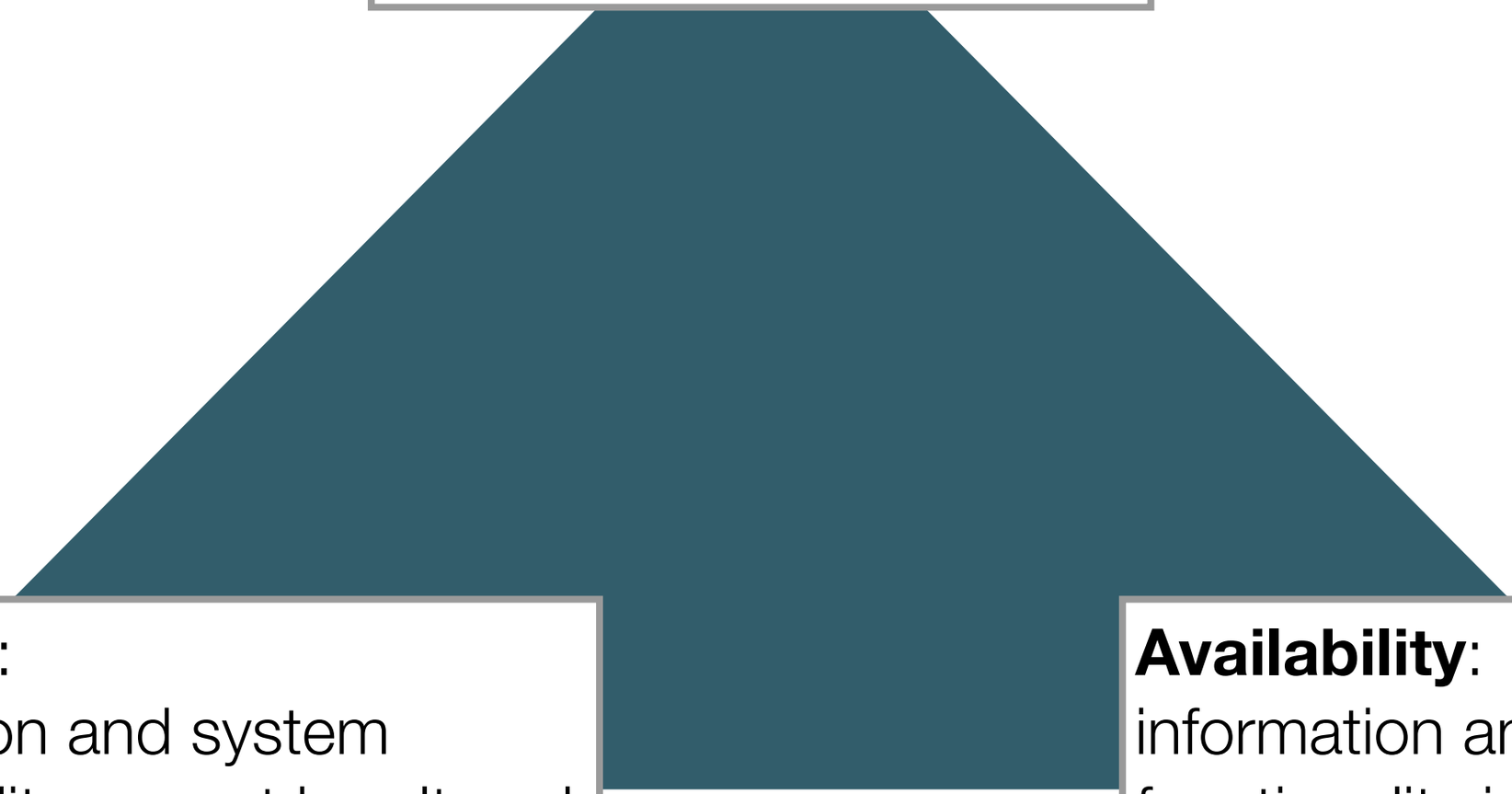
3. Key Concepts and Objectives

Computer Security: The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability**, and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

—NIST Computer Security Handbook

Security Objectives

Confidentiality:
information is not available to unauthorized entities



Integrity:
information and system functionality cannot be altered by unauthorized entities

Availability:
information and system functionality is available to authorized entities

Security Objectives:
Confidentiality, Integrity, and Availability

- Typically abbreviated as **CIA**
- However, their order of importance depends on the application
  - *storing credit card numbers*: confidentiality is the most important → CIA
  - *industrial control system*: availability and integrity are the most important → AIC
- Additional objectives
  - **non-repudiation / accountability**:
    actions can be provably traced back to an entity
  - **authenticity**:
    information comes from verified and trusted sources (*e.g.*, user authentication)
- Each objective may be achieved using multiple mechanisms
  - *example*: providing confidentiality for files on a multi-user system
    - *encryption*: files can be accessed, but the information is protected
    - *access control*: only authorized users can access files

Confidentiality:
Concealment of Information

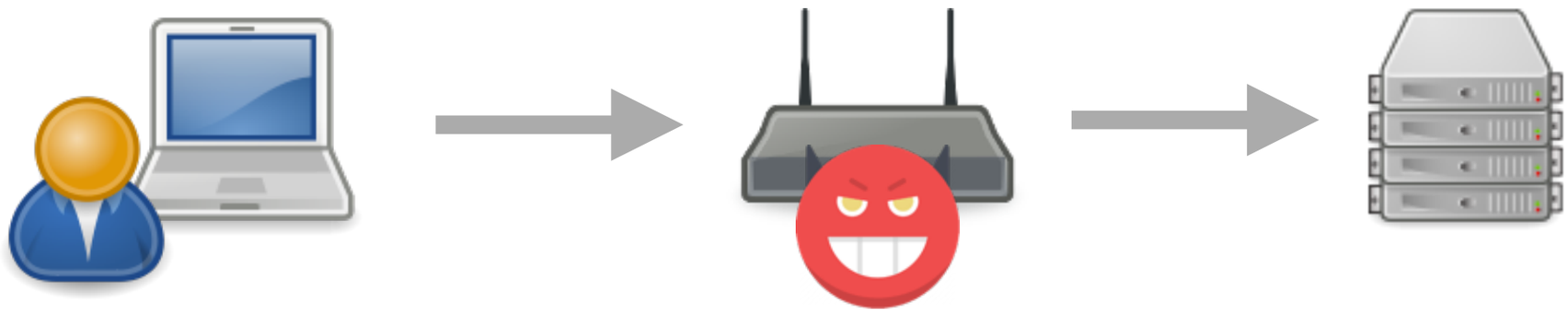
- Traditionally the most important objective
  - existed thousands of years before computers
- *What may be protected?*
  - message contents
  - message length
  - time of message transmission
  - existence of message
- **Privacy**: assures that individuals have control or influence over information related to them
  - confidentiality is often a prerequisite for privacy

Integrity:
Trustworthiness of Information

Data integrity: information cannot be modified in an unauthorized and <u>undetected</u> way

System integrity: system performs its intended function

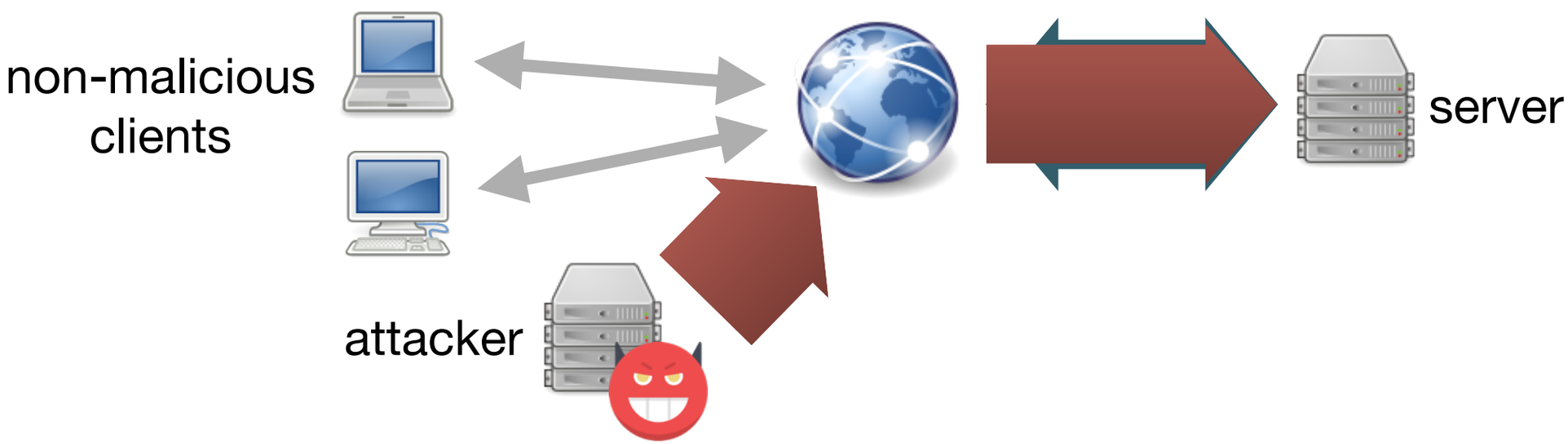
- In communications security, modification attacks are often impossible to prevent → our goal is to detect any unauthorized modification



- Attacker may meaningfully modify information/messages **even if** the attacker cannot read them → confidentiality does not ensure integrity

Availability:
Access to Information

- Attacks against availability are called **denial of service** (DoS) attacks
- Attack methods
  - **vulnerability exploitation**
    - *example of software vulnerability:*
      - CVE-2011-1871 (“Ping of Death”): “*denial of service (reboot) via a series of crafted ICMP messages in Microsoft Windows Vista, Windows Server 2008, and Windows 7 Gold*”
  - **resource exhaustion** (*e.g.*, memory or bandwidth)



Overview of Course Topics

Communication Security

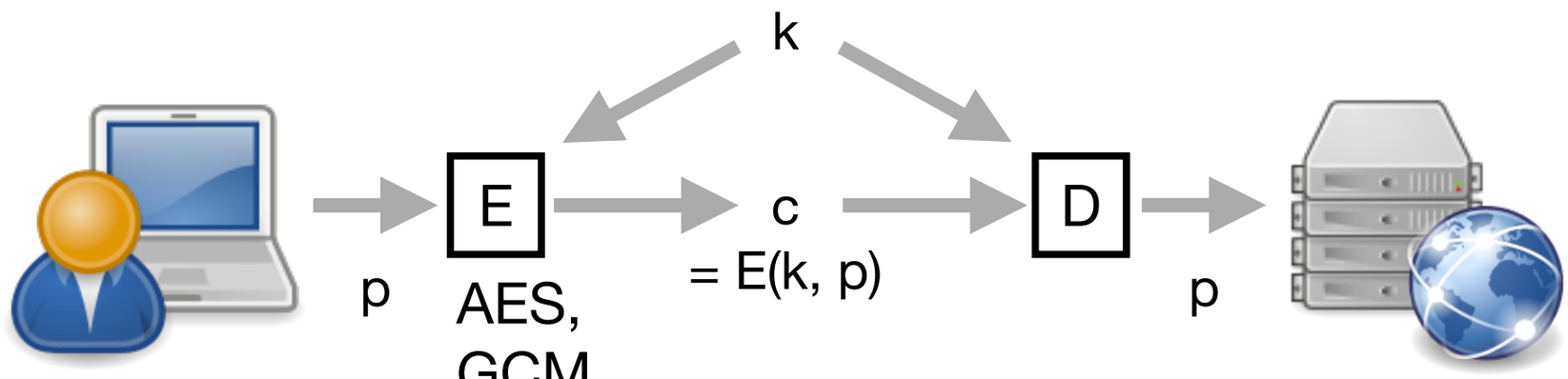
Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	

Communication Security

Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	

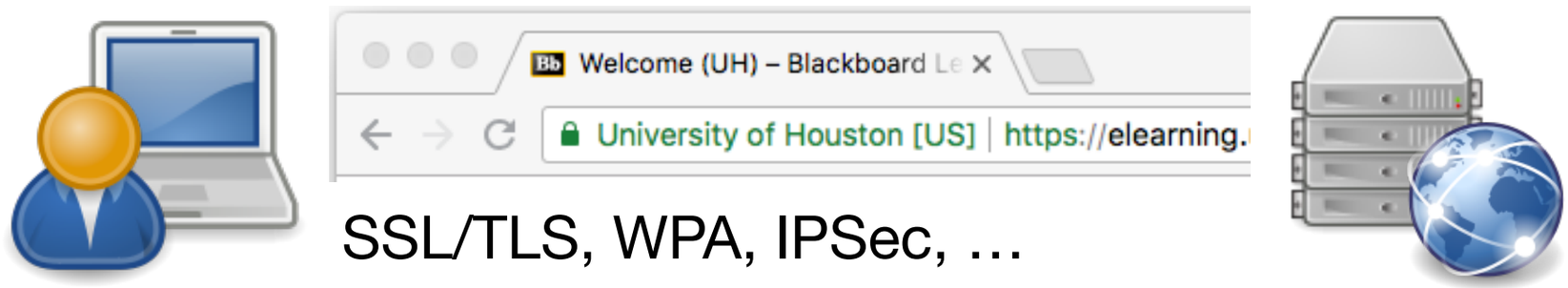
Communication Security

Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	



Communication Security

Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	



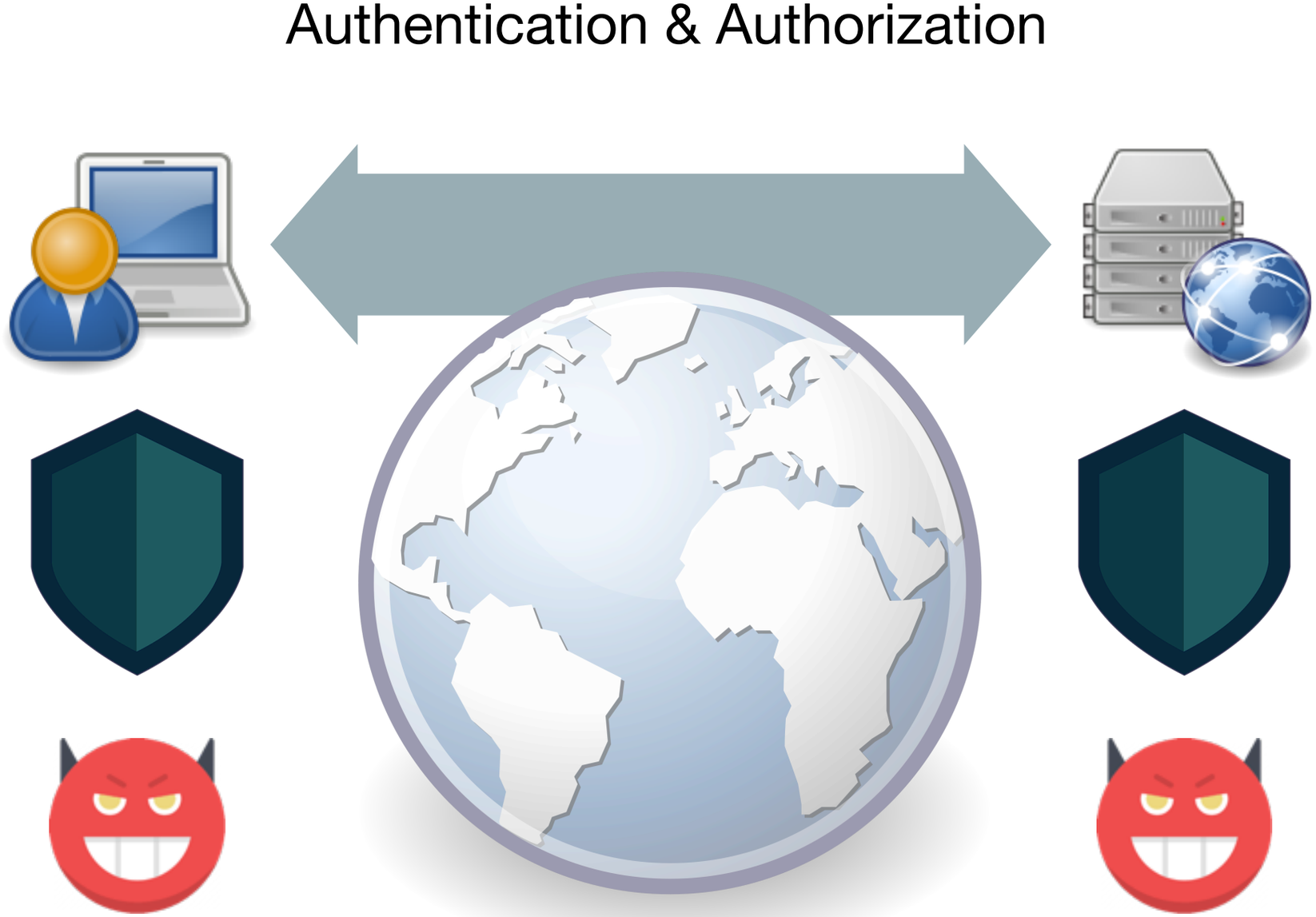
SSL/TLS, WPA, IPSec, …

System Security

Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	

System Security

Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	



System Security

Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	

Example vulnerability: Apple “Goto Fail”

```
if ((err = SSLHashSHA1.update(&hashCtx, &serverRandom)) != 0)
    goto fail;
if ((err = SSLHashSHA1.update(&hashCtx, &signedParams)) != 0)
    goto fail;
    goto fail;  /* THIS LINE SHOULD NOT BE HERE */
if ((err = SSLHashSHA1.final(&hashCtx, &hashOut)) != 0)
    goto fail;

err = sslRawVerify(...);
```

System Security

Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	

firewalls, intrusion detection systems, sandboxing, denial-of-service countermeasures, etc.

Course Objective

Provide an **introduction** to cybersecurity principles and practices

- understand basic concepts in security
- learn widely used security protocols and tools
- know about common security issues and their countermeasures

Beyond the scope of this course:

- ✗ become a security expert or ethical hacker
- ✗ gain comprehensive knowledge of all areas of security

"*Don't try this at home!*"

- Course topics include basic techniques for circumventing security mechanisms, exploiting vulnerabilities, etc.
  - it is impossible to defend a system without knowing what attackers can do
- Do **not** try these techniques on any system without permission!
  - Computer Fraud and Abuse Act (CFAA)
    - "*…intentionally accesses a computer without authorization or exceeds authorized access…*"
    - includes a wide range of computer-related acts

4. Challenges

Why is cybersecurity difficult?

Security Perspective

- Computer science and engineering is mostly concerned with **achieving desired behavior**
- Computer security is concerned with **preventing undesired behavior**

- Fundamentally different way of thinking
- *Example*: software testing
  - in practice, it typically suffices to prove that the system behaves as expected when we use it as intended
  - how can we prove that the system will not behave erroneously when someone uses it in a way that we did not think of?

Weakest Link

- Defender needs to find and fix **all vulnerabilities**

- "*A good attack is one that the engineers never thought of.*"

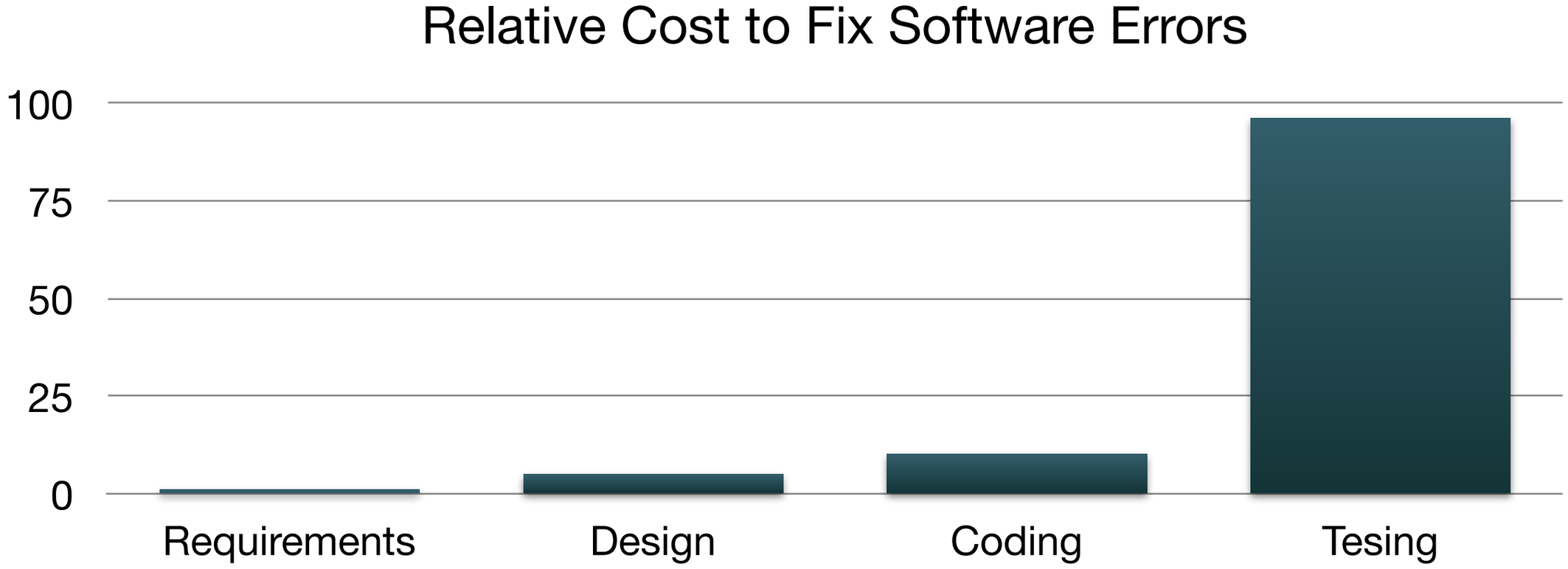
  – Bruce Schneier

- Not finding any vulnerabilities during testing does not prove that there are none

- Attacker needs to find **only one vulnerability**

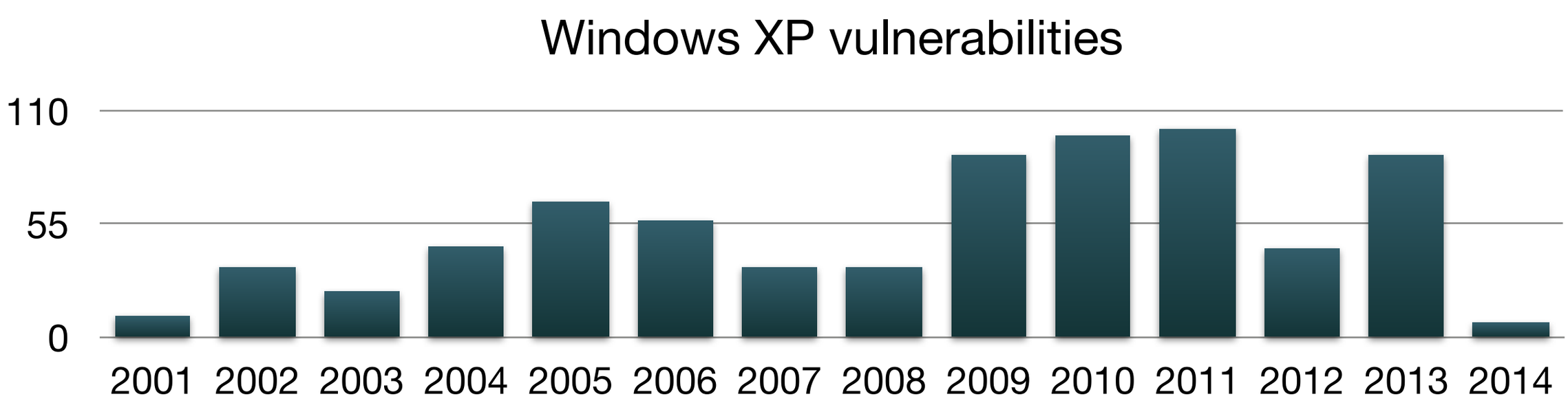
Security is Often an Afterthought

- The primary purpose of a system is to be **useful**
  → security is often secondary
- It is very hard to retrofit security



Security is a Process, Not a Product

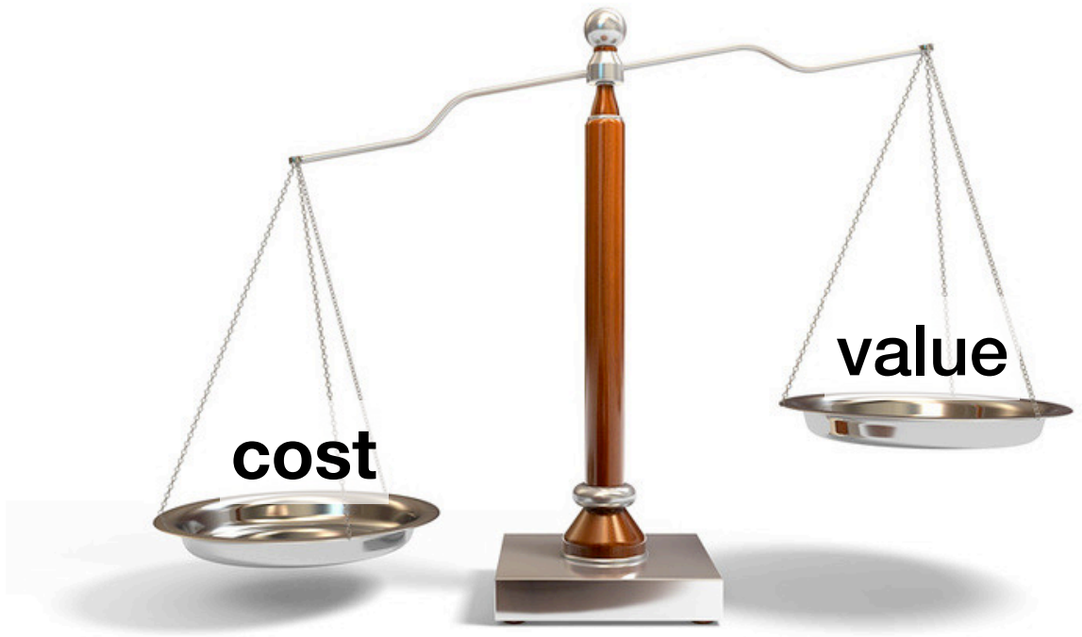
- Attackers are continuously looking for new vulnerabilities



- Systems must be **regularly updated** with security patches and **continuously monitored** for covert intrusions
- Attackers are searching for new attack techniques, while defenders are searching for new countermeasures
  - but attackers are often one step ahead…

Cost of Security

- There is often a tension between security and
  - usability
  - functionality
  - efficiency
  - time-to-market
  - development cost
  - …



- *Example*: password policy
  "*Please create a password. Your password must contain a capital letter, a number, a punctuation character, an emoji, eight elements from the periodic table, and a plot containing a protagonist with some character development and a twist ending.*"

Value of Security

- There is no direct benefit perceived from security
  - most **users perceive only security failures**, but not successes

- How to measure the value of security investments?
  - compliance to security standards
  - penetration testing (i.e., hire someone to see if it is possible to break in)

- Neither of these will provide a quantitative measure…

Lack of Liability

- Car manufacturers, construction companies, restaurants, etc. can be held liable for incidents (*e.g.*, for unsafe cars, collapsing buildings, food poisoning)
- Software is **often provided "as is"**
  - developers cannot be held liable

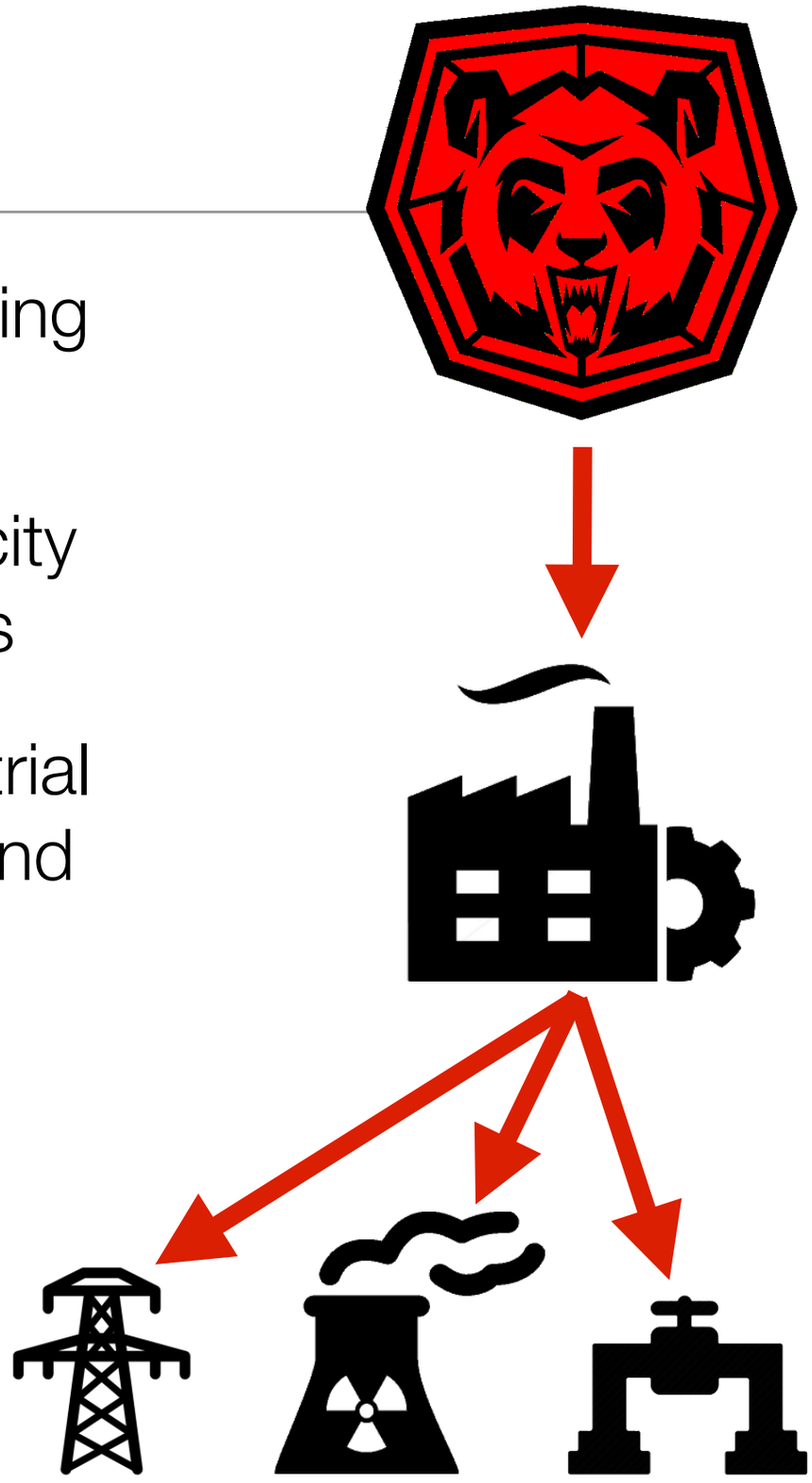
- Without liability, software companies have little incentive to produce secure software
  - customers might not value security
  - customers might be unable to tell if a software product is secure
  - developers incur cost of security

Trust

- When security is not a concern, we can trust
  - *hardware*: CPU will execute instructions exactly as specified
  - *compiler*: high-level language source and compiled code are identical functionally
  - ...
- *What can we trust when it comes to security?*
  - operating systems or applications might have **backdoors** (*e.g.*, Lenovo Superfish)
  - hardware might be “infected” with **hardware trojans**
  - even cryptographic algorithms might have backdoors
    - *Dual_EC_DRBG algorithm*: proposed by the NSA to be a widely used standard, but suspected by many to have a backdoor, which would allow the designer to decrypt traffic (*e.g.*, HTTPS)

Energetic Bear / Dragonfly

- Cyber-attack between 2011 and 2014, targeting **energy firms** in the U.S. and Europe
- Targets included grid operators, major electricity generation firms, petroleum pipeline operators
- Attackers **compromised** three different Industrial Control System **equipment manufacturers**, and inserted malware into software bundles delivered to customers



Bottomline:
There is No Perfect Security

"*Unfortunately the only way to really protect [your computer] right now is to turn it off, disconnect it from the Internet, encase it in cement, and bury it 100 feet below the ground.*"

Prof. Fred Chang, former director of research at NSA (2009)

- In practice, there is no such thing as perfect security, only degrees of insecurity
  - beware claims of perfect security and "unhackable" systems
  - cyber-risks must be managed

Adequacy of Imperfect Security

Is **this** secure?

Or **this**?

- In practice, we need

  cost of breaking in > attacker's gain from breaking in

- Businesses may prosper despite regular incidents
  - shoplifting and return frauds in retail
  - credit card frauds in financial sector

Next lecture:

Introduction to Cryptography