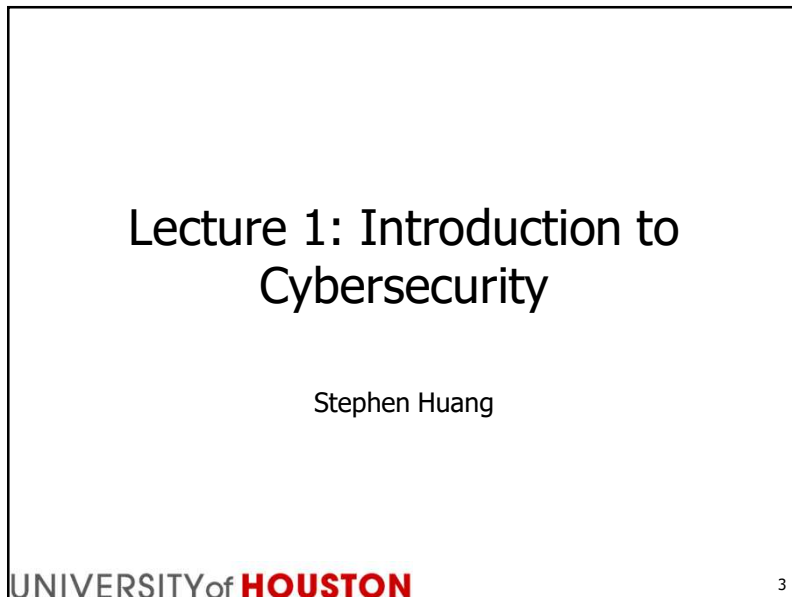




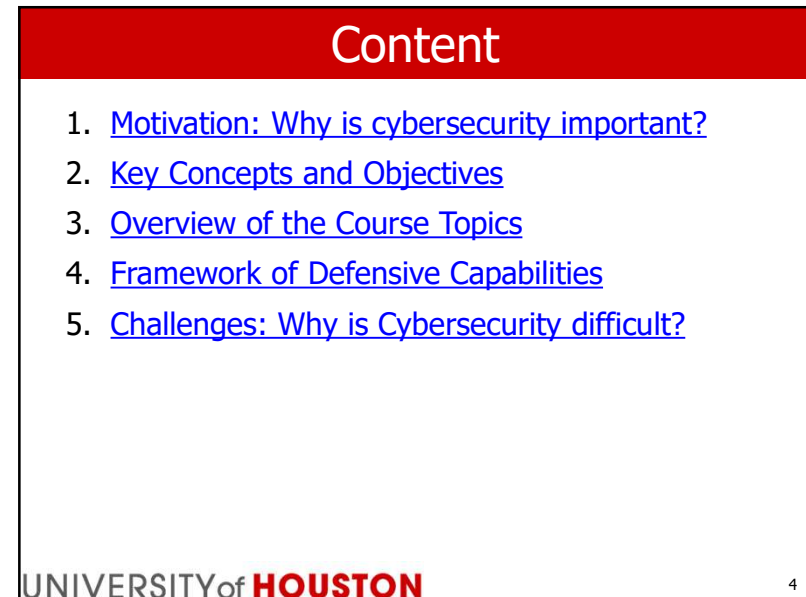
1



2 encryption



3



4

## 1. Motivation



## 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)
- 2021 Healthcare data breaches
  - more than 40 million U.S. healthcare records were compromised ([https://ocrportal.hhs.gov/ocr/breach/breach\\_report.jsf](https://ocrportal.hhs.gov/ocr/breach/breach_report.jsf))

## Physical Impact

- Stuxnet worm
  - targeted Iranian uranium enrichment facilities in 2010
  - subtly increased the pressure on spinning uranium one-fifth of Iran's nuclear centrifuges
- Ukrainian power grid
  - on December 23, 2015, three Ukrainian power companies suffered a sophisticated and targeted cyber-attack
  - attackers first compromised corporate networks using Word documents with malicious macros sent in e-mail
  - using credentials harvested from the corporate networks, attackers could remotely log into control systems
  - by opening circuit breakers at substations, attacked residents
- "Hackers Remotely Kill a Jeep on the Highway" (WIRED, 2015)
  - demonstration of remote wireless attack by security researchers



## 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...)

## 2. Key Concepts & Objectives

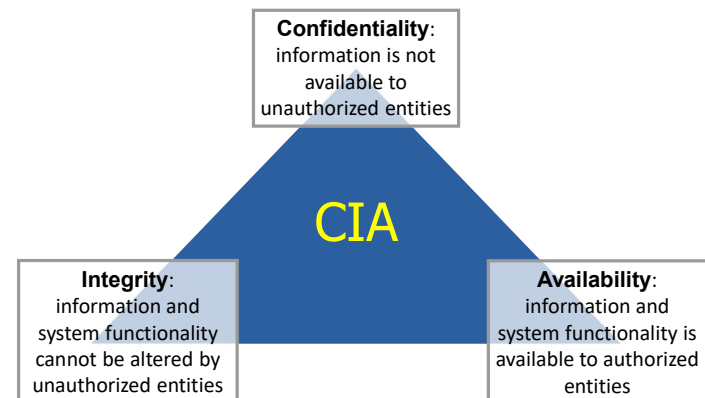
**Computer Security:** The protection afforded to an automated information system in order to attain the applicable objectives of preserving the **integrity**, **availability**, and **confidentiality** of information system resources (includes hardware, software, firmware, information/data, and telecommunications).

—NIST Computer Security Handbook

## Terminology

- **Vulnerability:** a weakness in the system that allows an attacker to compromise confidentiality, integrity, or availability
  - can be in the design, implementation, or configuration
- **Exploit:** a way or tool by which a vulnerability can be used
- **Attack:** an action using a vulnerability to compromise the system
- **Threat agent/adversary/attacker:** an entity that mounts an attack
- **Security policy:** statement as to what is allowed or not (i.e., which entity has what permission for which objects)
- **Security mechanism:** method, tool, or procedure to enforce policy

## Security Objectives



## Security Objectives

- 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 undetected way.
- System integrity: The system performs its intended function.

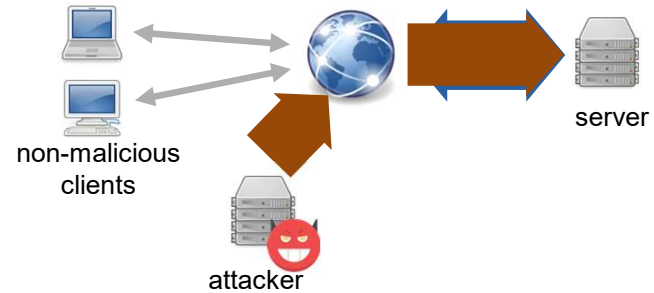


- In communications security, modification attacks are often impossible to prevent; our goal is to detect any unauthorized modification.
- An attacker may meaningfully modify information/messages even if the attacker cannot read them, confidentiality does not ensure integrity.

## 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)

## Resource Exhaustion




## 3. Overview of Course Topics


Week	Topic
1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	

Week	Topic
10	Access control
11	Software security
12	
13	Counter-measures
14	
15	

## Communication Security

1	Introduction	
2	Cryptography	
3		
4		
5		
6	Security protocols	
7		
8		
9		

## Communication Security

1	Introduction	
2	Cryptography	
3		
4		
5		
6	Security protocols	
7		
8		
9		

## Communication Security

1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	

UNIVERSITY of HOUSTON

21

## Communication Security

1	Introduction
2	Cryptography
3	
4	
5	
6	Security protocols
7	
8	
9	

UNIVERSITY of HOUSTON

22

## System Security

Week	Topic
10	Access control
11	Software security
12	Counter-measures
13	
14	

UNIVERSITY of HOUSTON

23

## System Security

Week	Topic
10	Access control
11	Software security
12	Counter-measures
13	
14	

UNIVERSITY of HOUSTON

24



## System Security

Week	Topic
10	Access control
11	Software security
12	
13	Counter-measures
14	

*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(...);
```

UNIVERSITYof HOUSTON

25

## System Security

Week	Topic	
10	Access control	<p>firewalls, intrusion detection systems, sandboxing, denial-of-service countermeasures, etc.</p>
11	Software security	
12		
13	Counter-measures	
14		

## Course Objectives

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

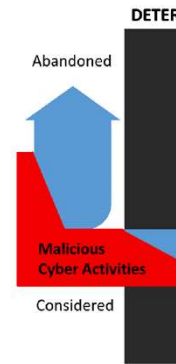


## 4. Framework of Defensive Capability

- To realize a secure cyberspace, the Federal Cybersecurity R&D Strategic Plan, identified a framework of four defensive capabilities:
  - Deter
  - Protect
  - Detect
  - Respond

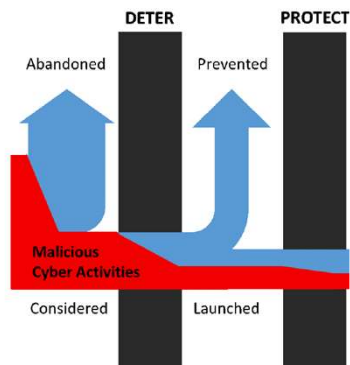
<https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf>

## Cyber Defensive Elements



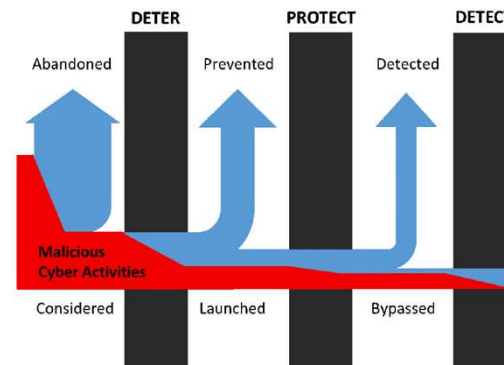
<https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf>

## Cyber Defensive Elements



<https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf>

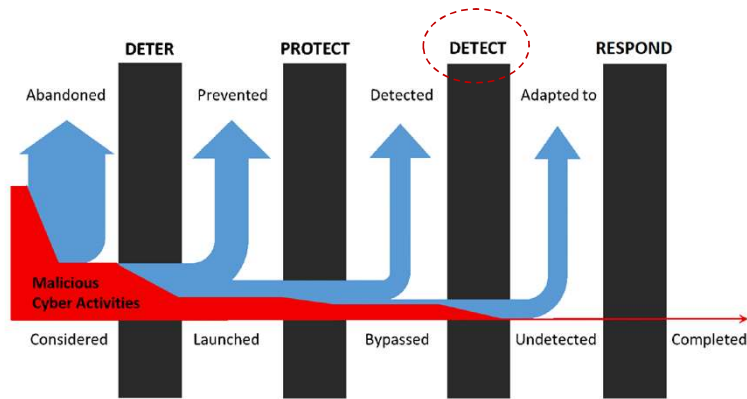
## Cyber Defensive Elements



<https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf>



## Cyber Defensive Elements



<https://www.nitrd.gov/pubs/Federal-Cybersecurity-RD-Strategic-Plan-2019.pdf>

## 5. 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?

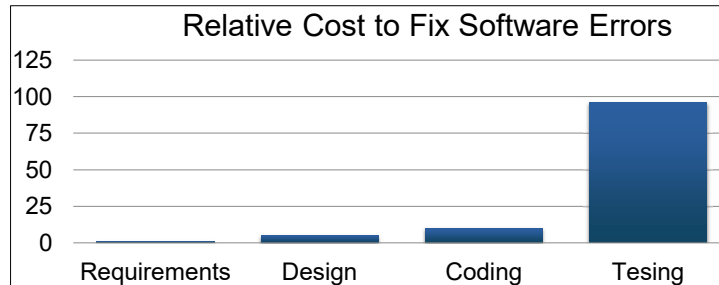
## Weakest Link

- 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



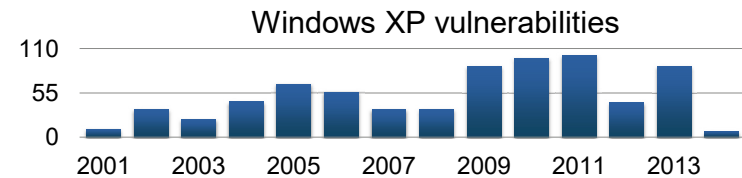
## Security is Often an Afterthought

- 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 do we measure the value of security investments?
  - compliance with 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

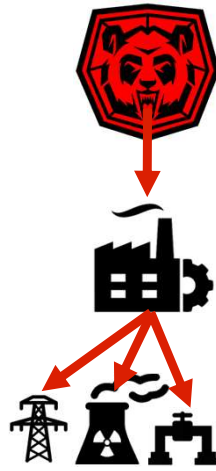
- Car manufacturers, construction companies, restaurants, etc. can be held liable for incidents (e.g., for unsafe cars, collapsing buildings, food poisoning)
- Software is often provided “as is”
  - developers cannot be held liable
- Without liability, software companies have little incentive to produce 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



## There is No Perfect Security

- “Unfortunately, the only way to 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 Topic

- Intro. to Cybersecurity
- Intro. to Cryptography
- Stream Ciphers