

ECE 509: Cyber Security: Concept, Theory and Practices

Salim Hariri

Fall 2023

Today's Lecture Outline

- Administrative Issues
- Cybersecurity Motivation and objectives
- Cybersecurity Challenges
- Define Cybersecurity

Administrivia

- Meet Tuesday 4:00-6:30pm, Building - Modern Languages, Room 310.
- Cyber Security Lab as a Service (CLaaS)
 - www.askcypert.org
- Office hours, By Appointment, questions via email are encouraged
 - hariri@ece.arizona.edu
- Class Support
 - **Clarisa Grijalva Lugo**, Office: ECE 251, email: clarisagl@arizona.edu

Course Evaluation

- Homework - 10%
- Quiz (every two weeks) - 10%
- Labs - 10%
- Midterm – 25%
- Project – 20%
- Final Exam– 25%

Important Deadlines:

Project September 12, 2023

Proposal:

Project Report: December 06, 2023

Midterm: October 10, 2023

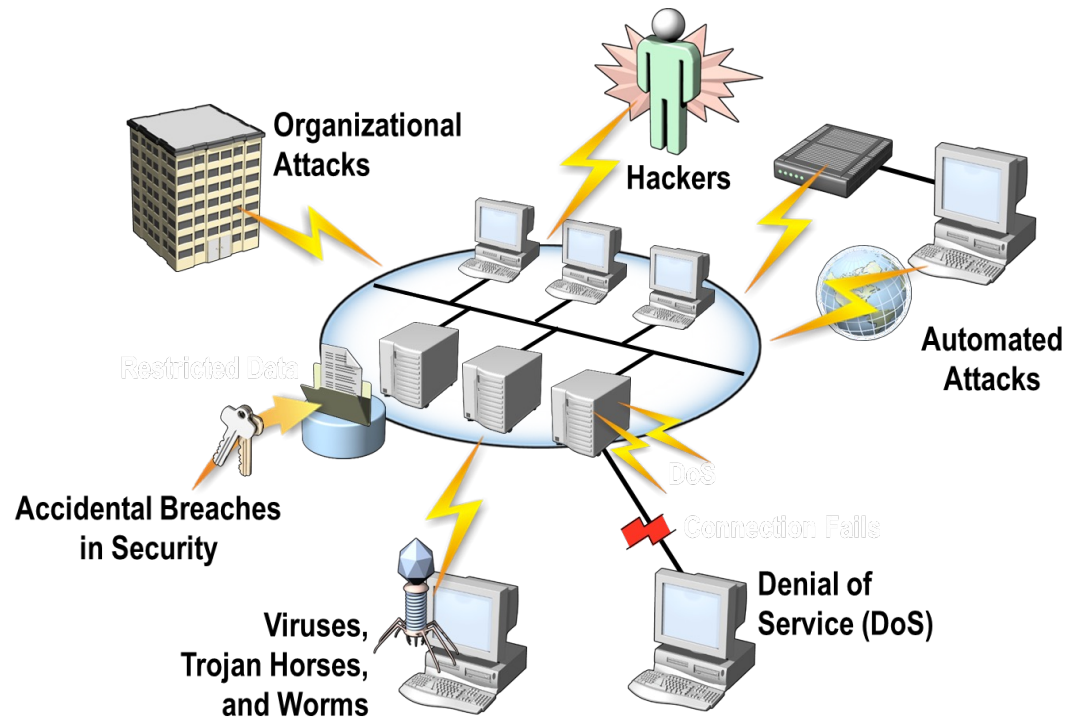
Final: According to University Final Exam Schedule.

What will be covered in this class?

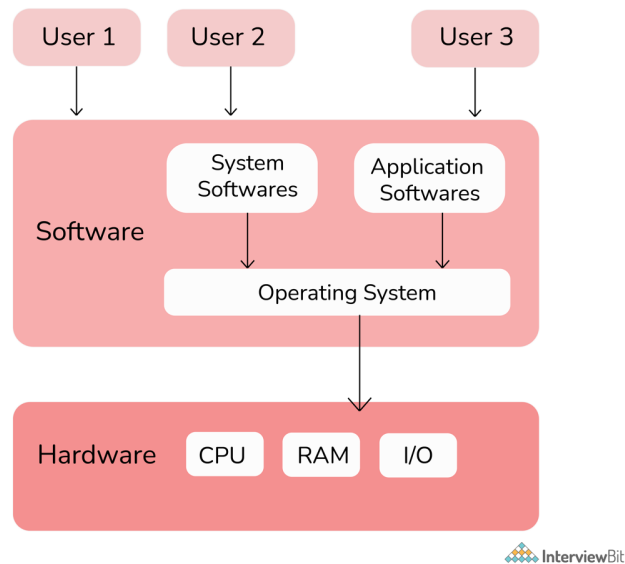
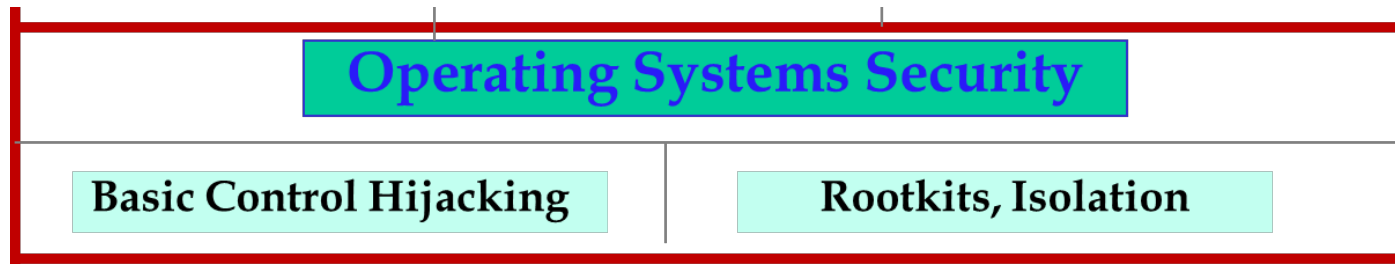
Application Security & Resilience			
User and Web Applications		Mobile Platforms	Web Protocols
Encryption	Forensic Analysis	Insider Threats	
Operating Systems Security			
Basic Control Hijacking		Rootkits, Isolation	
Computer Networks and Protocols Security			
Computer Networks		Communication Protocols	
Wireless	Wired	IP Based	Non IP Based

What will be covered in this class?

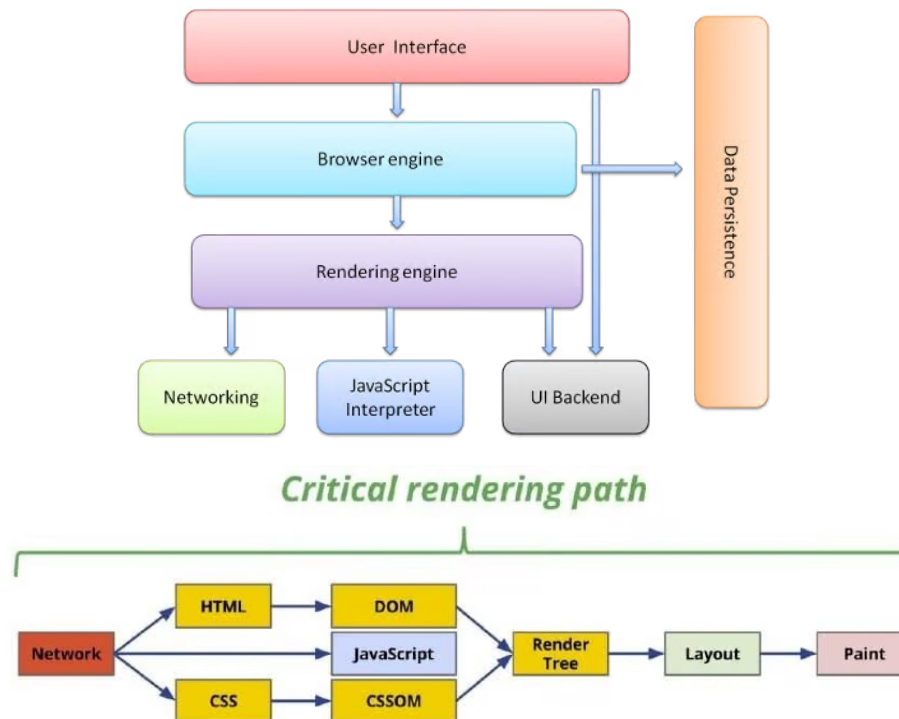
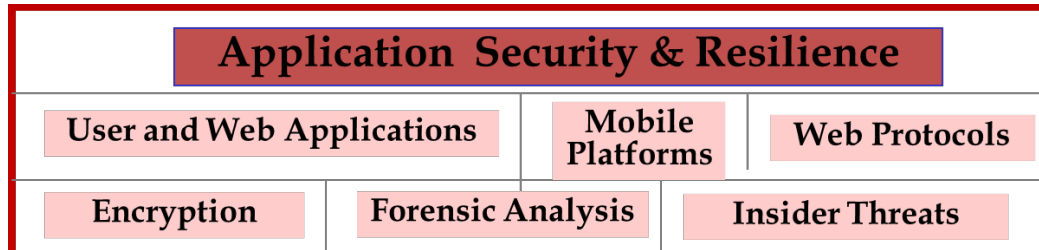
Computer Networks and Protocols Security			
Computer Networks		Communication Protocols	
Wireless	Wired	IP Based	Non IP Based



What will be covered in this class?



What will be covered in this class?








Course Outline

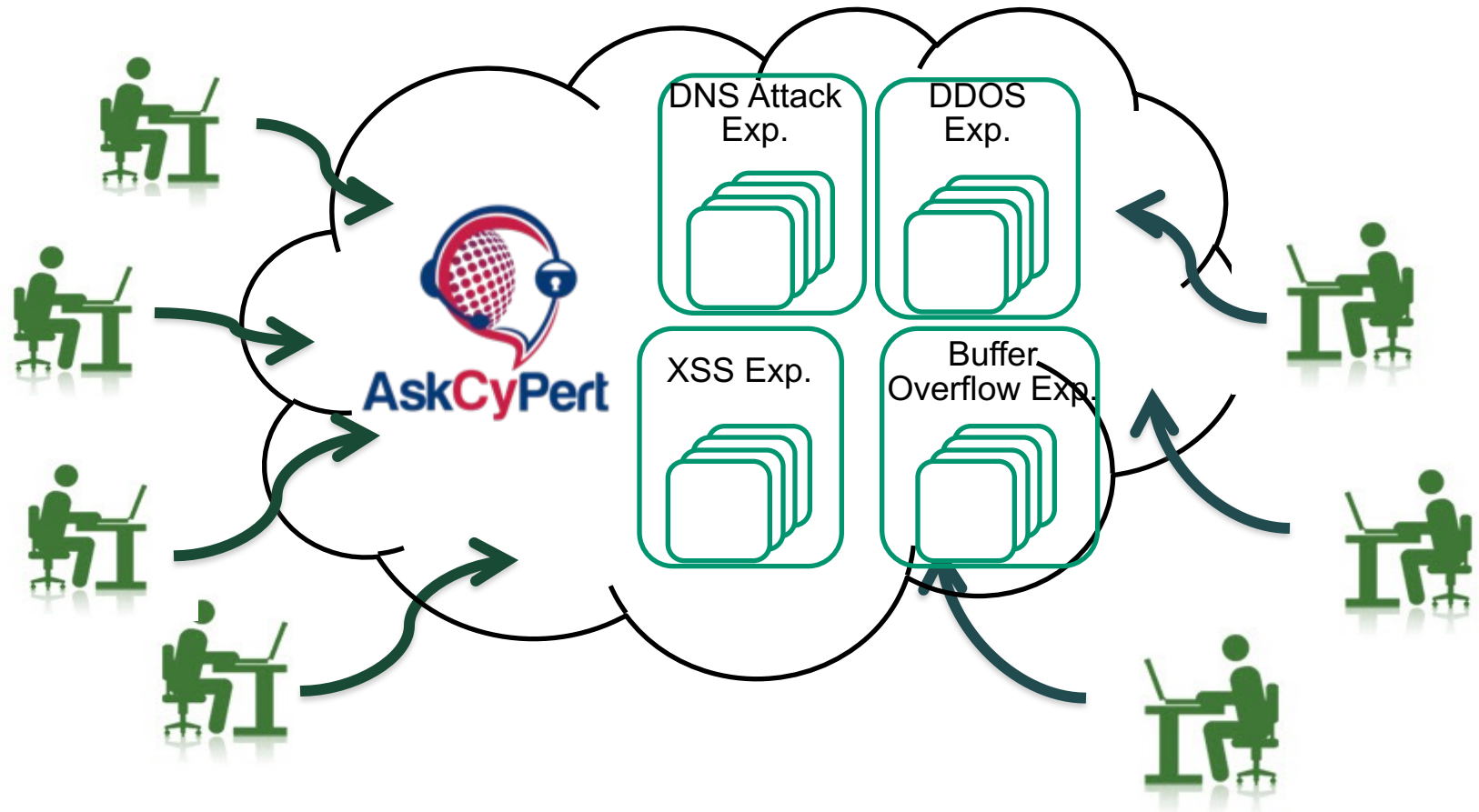
Date	Lecture	Topic
Aug. 22, 2023	Lecture 1	<ul style="list-style-type: none"> ▪ Introduction to Cybersecurity and Threat Modeling ▪ Introduction CLaaS: Virtual Cybersecurity Lab
Aug. 29, 2023	Lecture 2	<ul style="list-style-type: none"> ▪ Threat Modelling and Analysis of Cyber-Systems ▪ Internet of Things/ICS Threat Modeling – Use Case Discussion
Sep. 05, 2023	Lecture 3	<ul style="list-style-type: none"> ▪ Intrusion detection Systems (IDS) ▪ IDS for Industrial Control – Differences between IT-IDS and ICS-IDS
Sep. 12, 2023	Lecture 4	<ul style="list-style-type: none"> ▪ Intrusion detection Systems (IDS) ▪ Host and network-based IDS & SIEM Tools
Sep. 19, 2023	Lecture 5	<ul style="list-style-type: none"> ▪ Network Security (Part 1) ▪ Introduction to Machine Learning for Cybersecurity
Sep. 26, 2023	Lecture 6	<ul style="list-style-type: none"> ▪ Network Security (Part 2) ▪ Network Anomaly Behavior Analysis
Oct. 03, 2023	Lecture 7	<ul style="list-style-type: none"> ▪ Network Security (Part 3) ▪ Midterm Review
Oct. 10, 2023	Exam	<ul style="list-style-type: none"> ▪ Midterm
Oct. 17, 2023	Lecture 8	<ul style="list-style-type: none"> ▪ Denial of Service (DoS) Mitigation Techniques ▪ Wireless Protocols Anomaly Behavior Analysis: Wi-Fi
Oct. 24, 2023	Lecture 9	<ul style="list-style-type: none"> ▪ Basic Control Hijacking Attacks ▪ Wireless Protocols Anomaly Behavior Analysis: Bluetooth
Oct. 31, 2023	Lecture 10	<ul style="list-style-type: none"> ▪ Isolation Techniques ▪ ICS Protocols Anomaly Behavior Analysis: ENIP
Nov. 07, 2023	Lecture 11	<ul style="list-style-type: none"> ▪ Cryptography Overview ▪ ICS Protocols Anomaly Behavior Analysis: Modbus
Nov. 14, 2023	Lecture 12	<ul style="list-style-type: none"> ▪ Browser Security ▪ Penetration testing: Vulnerability analysis (<i>in-class lab session</i>)
Nov. 21, 2023	Lecture 13	<ul style="list-style-type: none"> ▪ Website Security ▪ Penetration testing: Exploitation (<i>in-class lab session</i>)
Nov. 28, 2023	Lecture 14	<ul style="list-style-type: none"> ▪ Mobile Security ▪ Penetration testing: Post-Exploitation and Reporting
Dec. 05, 2023	Lecture 15	<ul style="list-style-type: none"> ▪ Mobile Security ▪ Final Review



CLaaS: Cybersecurity Lab as a Service

-  Cybersecurity Lab as a Service (CLaaS)
-  Cybersecurity Knowledgebase Repository
-  Training and Teaching Programs (ongoing)
-  Cybersecurity Tools (ongoing)
-  Cybersecurity Research Repository (ongoing)

CLaaS Architecture



MOTIVATION: CYBERSECURITY

Problem Statement

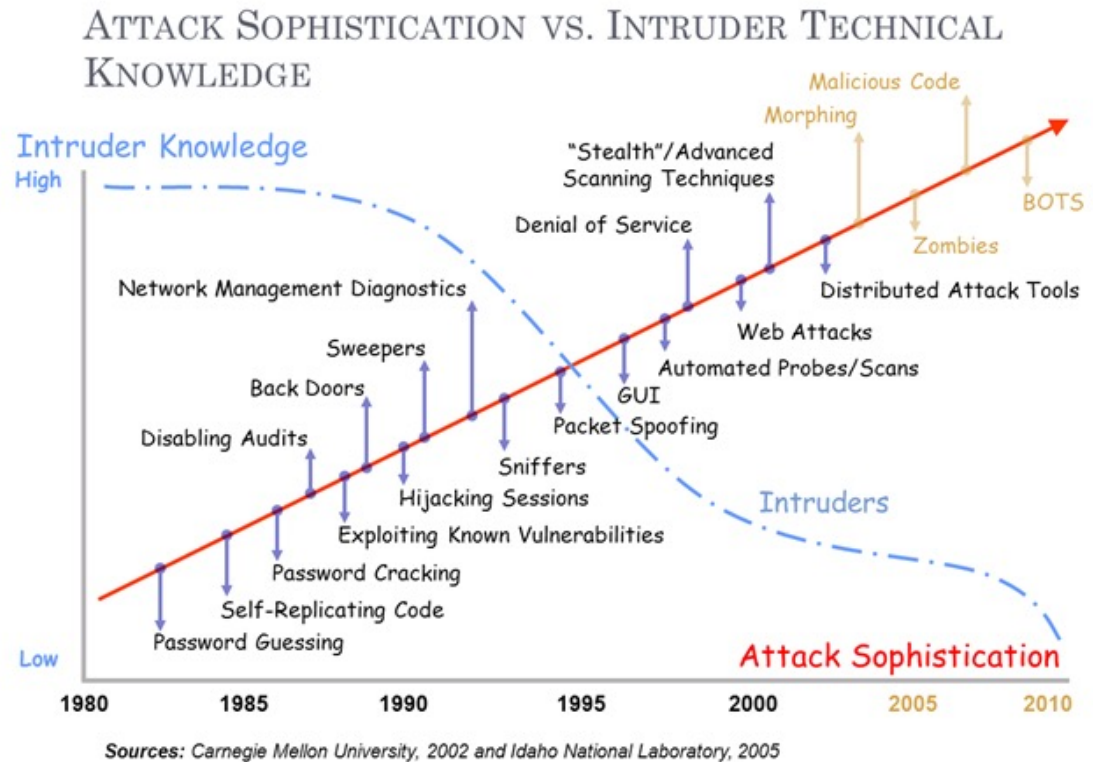
- We rapidly moving toward completely digital world, society, government, and economy
 - The evolution of cloud, mobile devices and IoT makes cybersecurity at the forefront of concerns for consumers, businesses and government alike.
- Factors contributing to this cybersecurity challenge is the exponential growth in number of human and digital targets
 - There are more than 4.66 billion Internet users out of 7.83 billion global population, up from 2 billion in 2015
 - There are more than 1.986 billion websites, and 15.14 billion IoT smart devices are connected.
- Cyber crime and cyber IT damage is projected to cost \$8 Trillion in 2023 and is expected to grow to 10.5 Trillion in 2025
 - The US GDP was 23 Trillion in 2021, China GDP 17 Trillion, Japan 4.9 Trillion

1: CSO. "Top 5 cybersecurity facts, figures, and statistics for 2018." Jan. 2018

8/18/23

Problem - 1

- Exponential Growth in Attacks Complexity, Speed, Damaging and Scale
 - In April 2019, a research organization, registered more than 350,000 new malware samples *per day*,
 - According to Symantec's 2019 Internet Security Threat Report, cyberattacks targeting supply chain vulnerabilities increased by 78% in 2018

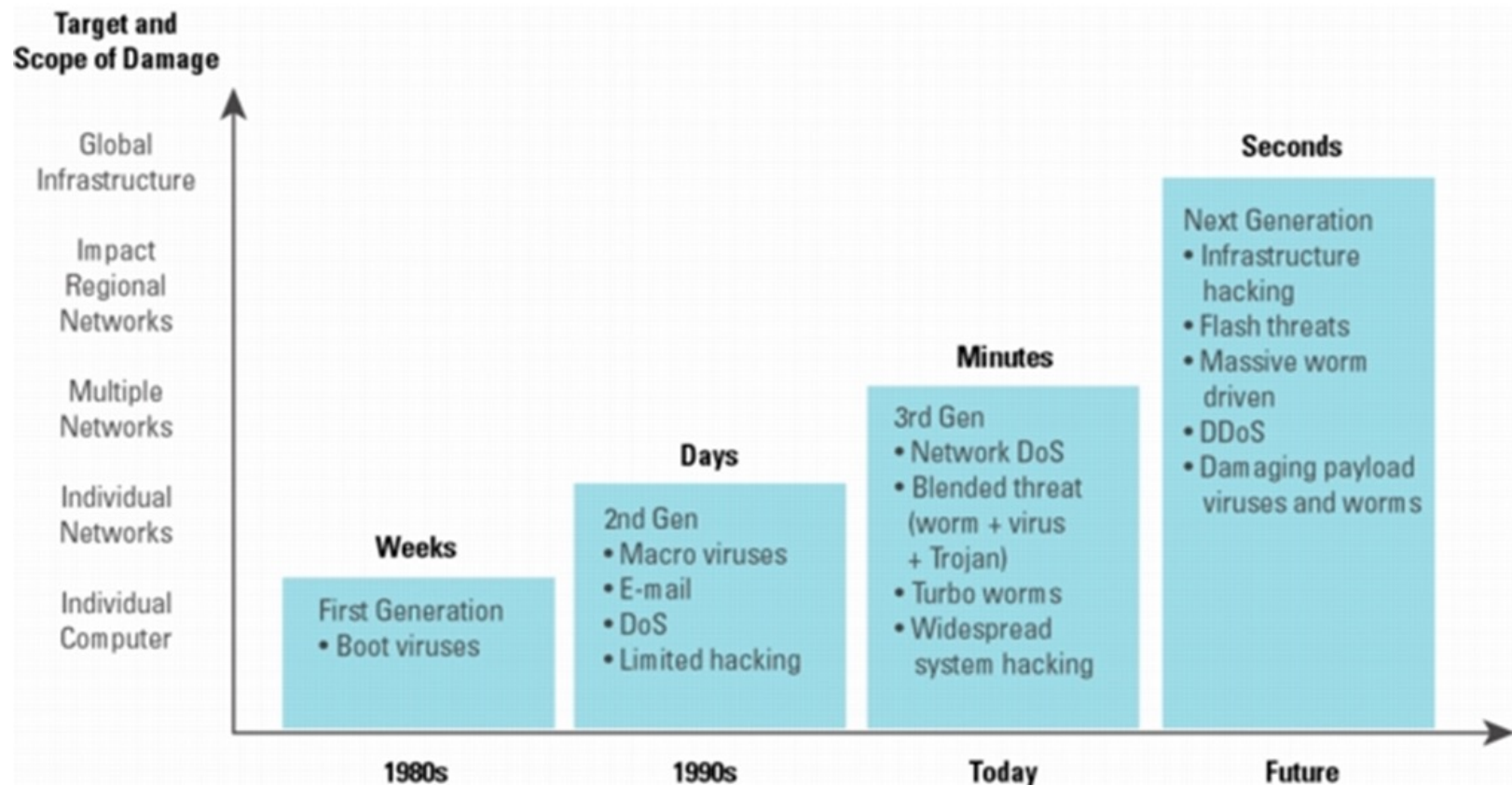


Problem – 2: Dark Web Services

- Dark Web Hosts Cyberattack as a Service (CAaaS)
 - Cybercriminals can use the dark web to develop and sell the components to launch attack

NAME	DESCRIPTION	VALUE CHAIN ACTIVITIES
Vulnerability Discovery as a Service	Discover vulnerabilities within the target system	Primary
Exploit as a Service	Create software to take advantage of a system's vulnerability	Primary
Deception as a Service	Provide fake information to mislead targets	Primary
Payload as a Service	Provide malicious payload such as virus, worm, or ransomware	Primary
Exploit Package as a Service	Combine exploits into exploit kits	Support
Obfuscate as a Service	Provide obfuscation strategies and technologies to reduce being detected	Support
Security Checker as a Service	Verify whether bypassing defensive system is possible	Support
Repackage as a Service	Repack different elements to increase effectiveness of an attack	Support
Botnet as a Service	Provide botnet	Primary
Traffic Redirection as a Service	Redirect traffic to the specific address	Primary
Bulletproof Hosting as a Service	Provide bulletproof hosting servers	Primary
Traffic as a Service	Generate traffic for the given target	Primary
Reputation Escalation as a Service	Craft a fake reputation for the given target	Support
Personal Profile as a Service	Offer personal profile — like passport data, Social Security number, credit card numbers — about targets	Support
Domain Knowledge as a Service	Offer domain knowledge about the target	Support

Problem – 3: Attacks Propagates Fast



Problem – 4: Attackers Use AI

- By using AI, social engineering attack
- We are spending billions of dollars on cybersecurity, to only see attacks are increasing and very successful
- We critically needed a paradigm shift on how to secure and protect our cyber systems

Challenges of Cyber Security

1. The Internet has become the primary computing platform. Standalone apps → Web-based → Cloud computing

Q: What are your most frequently used computer applications these days?

- Gaming ?
- Search engines ?
- Emailing, Texting
- Facebook, LinkedIn, Twitter, ...
- Amazon, eBay, ...
- Word processors
- Wikipedia, Google maps, ...
- Google Docs, SkyDrive, Google Drive, Evernote, ...
- Web browsers (HTTP)



Exponential Growth in Attack Surface

- There were around 6 billion internet users in 2022, and it is estimated to grow to 7.5 billion by 2030.
- There are more than 1.2 billion websites
- Global ransomware costs were set to exceed \$5 billion in 2017, 15X higher than 2015
- Data volumes will be 50 times greater in 2020 than in 2016
- IoT growth: 200 billion “smart” devices on the market by 2020, up from 2 billion in 2006
- 500 million wearable devices sold worldwide by 2021, up from 310 million in 2017
- There will be 300 billion passwords globally to be protected by 2020

Challenges of Cyber Security

3. Rich data types

HTML, XHTML, XML,

MP3, MP4, ...

MPEG4, AVI, WMV, ...

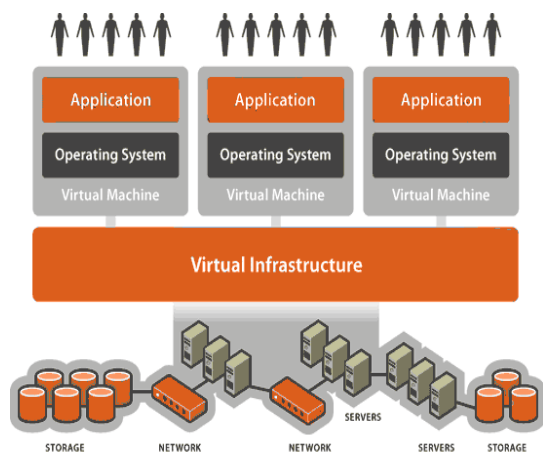
JPEG, GIF, BMP, ...

JavaScripts, Java Applets, ...

Encrypted data (SSL, IPsec, ...)



Challenges of Cyber Security



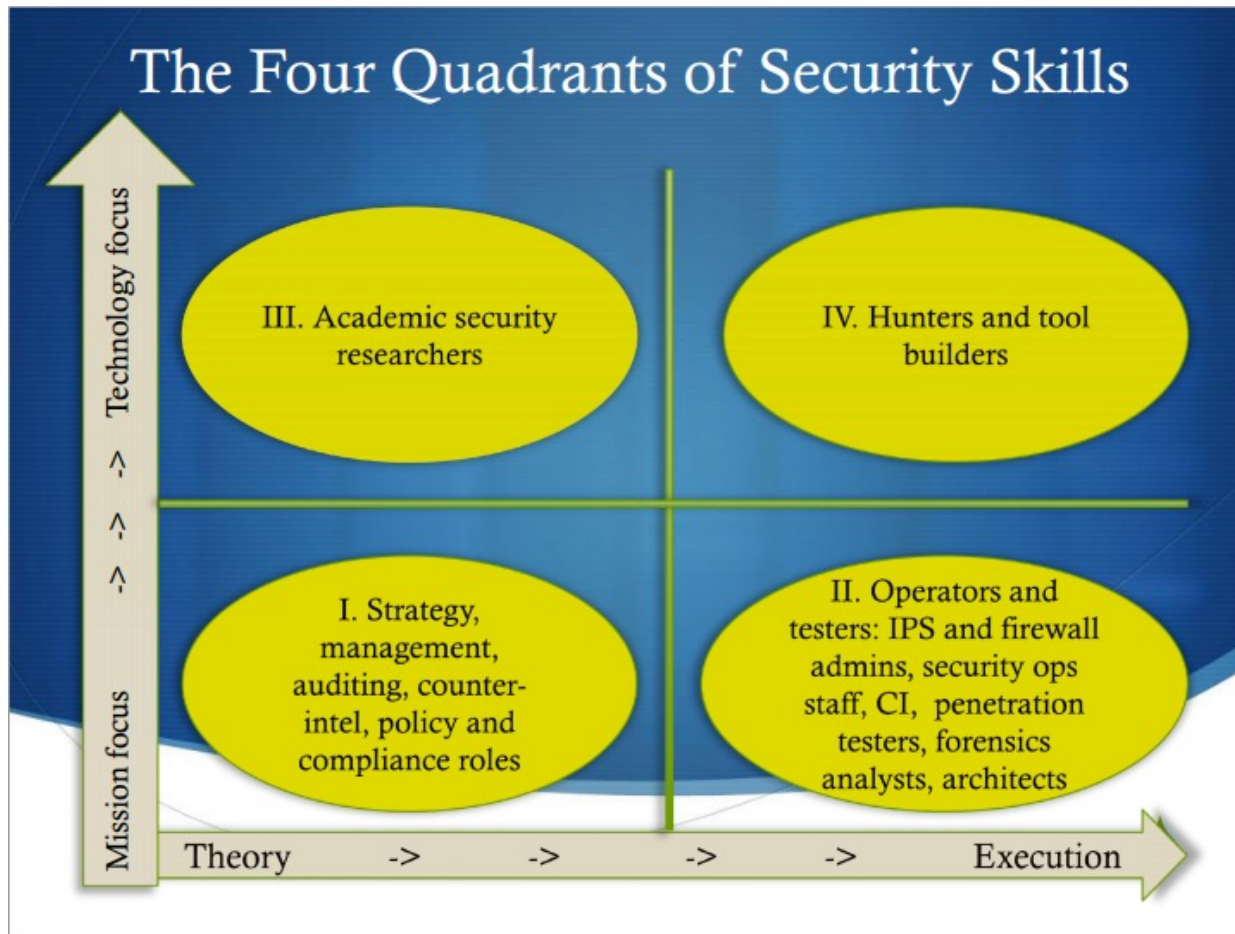
4. Evolving technologies
5. New technology may bring new vulnerabilities!
6. Evolving tactics by attackers



Challenges of Cyber Security

7. Insufficient cyber security workers

- *A zero-unemployment job market?*



Bottomline - Zero unemployment for Cybersecurity Workforce

- There is a significant and growing gap between available corporate and government cybersecurity jobs and the people available to do them.
- Today the US Dept. of Commerce estimates there are around 350,000 cybersecurity jobs currently unfilled. Also, Cybersecurity Ventures estimates 3.5 million cybersecurity jobs will be unfilled globally by 2021
- With cybersecurity jobs in such high demand and skilled professionals in low supply, that makes cybersecurity is an excellent career path
- UA Cybersecurity Courses (ECE 509 and ECE 524) provide you with the knowledge to be qualified to these unfilled cybersecurity jobs!

What is Cybersecurity?

According to S. 1901 “Cybersecurity Research and Education Act of 2002”:

cybersecurity: “information assurance, including scientific, technical, management, or any other relevant disciplines required to ensure computer and network security, including, but not limited to, a discipline related to the following functions:

- (A) Secure System and network administration and operations.
- (B) Systems security engineering.
- (C) Information assurance systems and product acquisition.
- (D) Cryptography.
- (E) Threat and vulnerability assessment, including risk management.
- (F) Web security.
- (G) Operations of computer emergency response teams.
- (H) Cybersecurity training, education, and management.
- (I) Computer forensics.
- (J) Defensive information operations.

Some Definitions

According to S. 1900 “Cyberterrorism Preparedness Act of 2002 ”:

cybersecurity: “information assurance, including information security, information technology disaster recovery, and information privacy.”

One way to think about it

cybersecurity = security of cyberspace

One way to think about it

cybersecurity = security of **cyberspace**



information systems
and networks

One way to think about it

cybersecurity = security of information
systems and networks

One way to think about it

cybersecurity = security of information
systems and networks



+ with the goal of
protecting operations
and assets

One way to think about it

cybersecurity = security of information systems and networks with the goal of protecting operations and assets

One way to think about it

cybersecurity = **security** of information systems and networks with the goal of protecting operations and assets



security in the face of attacks, accidents and failures

One way to think about it

cybersecurity = security of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

One way to think about it

cybersecurity = **security** of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets



availability, integrity
and secrecy

One way to think about it

cybersecurity = availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting operations and assets

In Context

corporate cybersecurity = availability, integrity and secrecy of information systems and networks in the face of attacks, accidents and failures with the goal of protecting a corporation's operations and assets

national cybersecurity = availability, integrity and secrecy of the information systems and networks in the face of attacks, accidents and failures with the goal of protecting a nation's operations and assets

Slides Credited to

1. From “Security Threat Modeling,” presented by Nagaradhika, Old Dominion University
2. From “Threat Modeling – Designing for Security”, by Adam Shostack

What will be covered in this class?

Application Security & Resilience			
User and Web Applications		Mobile Platforms	Web Protocols
Encryption	Forensic Analysis		Insider Threats
Operating System Security			
Basic Control Hijacking		Rootkits, Isolation	
Computer Networks and Protocols Security			
Computer Networks		Communication Protocols	
Wireless	Wired	IP Based	Non IP Based