

Epilogue

CS 459/559: Science of Cyber Security
21st Lecture

Instructor:
Guanhua Yan

Agenda

- ~~Quiz 1: September 29 (closed book)~~
- ~~Project 1 (offense): October 10~~
- Course wrapup & presentation lottery:
November 10
- Quiz 2: November 12
- Presentations: 11/17, 11/19, 11/24, 12/1,
12/3
- CTF competition: November 26
- Project 2 (defense): December 5
- Final report: December 15



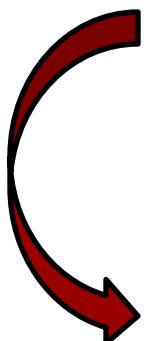
Leaderboard of the day

	User Name	Successful Attack	Score
1	sandworm	Buffer Overflow, DNS Tunneling, Known Plaintext Attack, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	120
2	luffytaro	Buffer Overflow, DNS Tunneling, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	110
3	anitabhagashetti	Buffer Overflow, DNS Tunneling, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	110
4	haritha	Buffer Overflow, DNS Tunneling, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	110
5	JamesRatanDukkipati	Buffer Overflow, DNS Tunneling, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	110
6	dchaganti	Buffer Overflow, DNS Tunneling, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	110
7	slee	Buffer Overflow, DNS Tunneling, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	110
8	jeff	Buffer Overflow, DNS Tunneling, Network Reconnaissance, Program Wrapper, Reverse Proxy, SQL Injection, Tiny Shell Exploit	110

What we have learned so far...



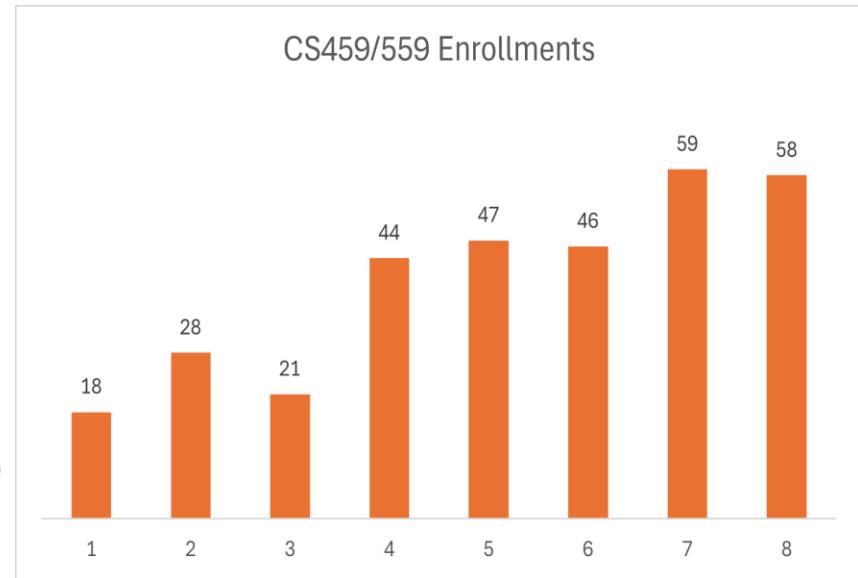
What a journey...



The people involved in CS 459/559
(58 students, TA, and myself)

CS459/559 enrollments

- Spring 2018: 9 CS459 + 9 CS559
- Spring 2019: 15 CS459 + 13 CS559
- Spring 2020: 11 CS459 + 10 CS559
- Fall 2022: 18 CS459 + 26 CS559
- Fall 2023: 13 CS459 + 34 CS559
- Fall 2024: 18 CS459 + 28 CS559
- Spring 2025: 24 CS459 + 35 CS559
- Fall 2025: 18 CS459 + 40 CS559
- Spring 2026: ...



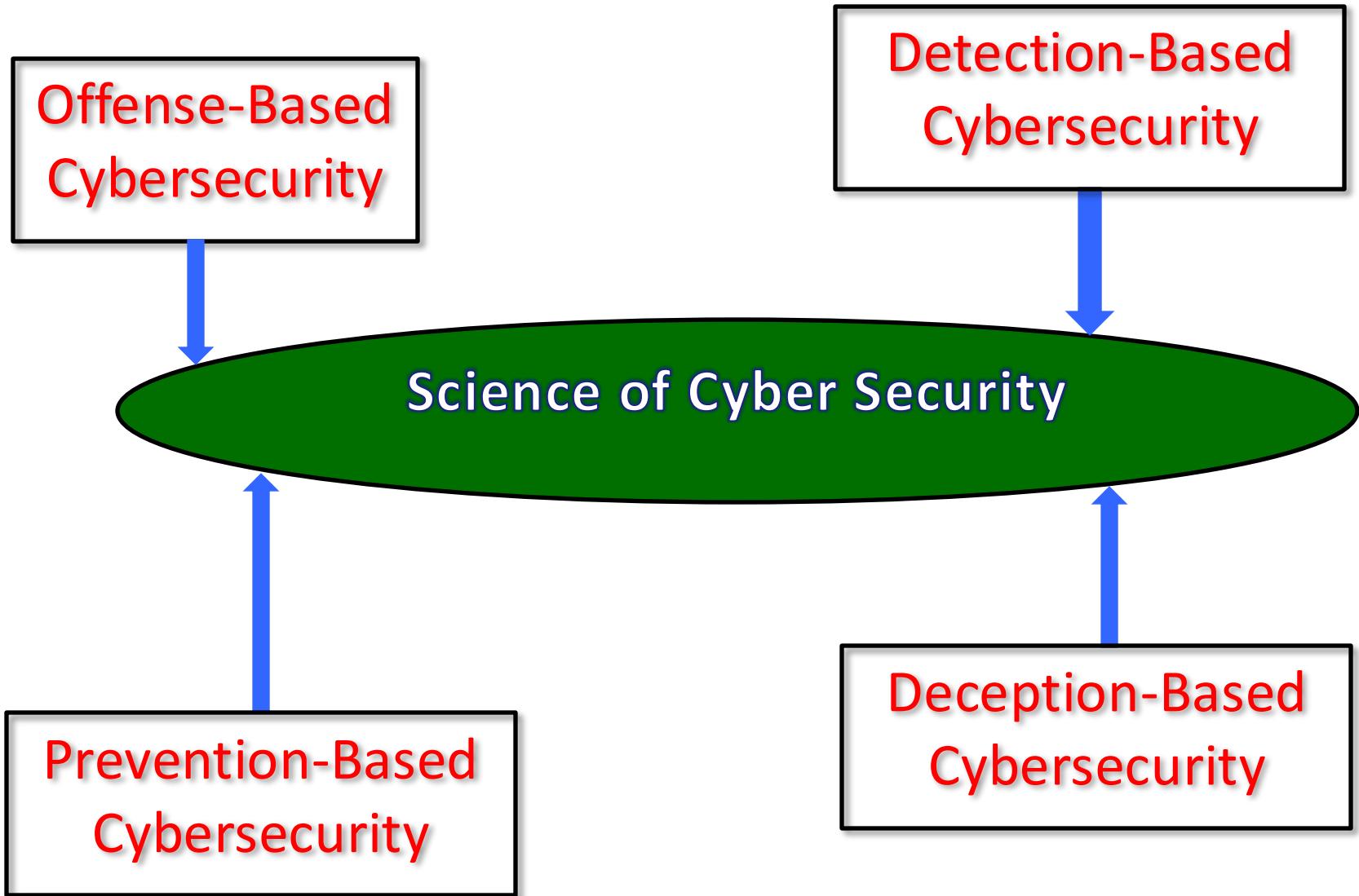
We have done or will do:

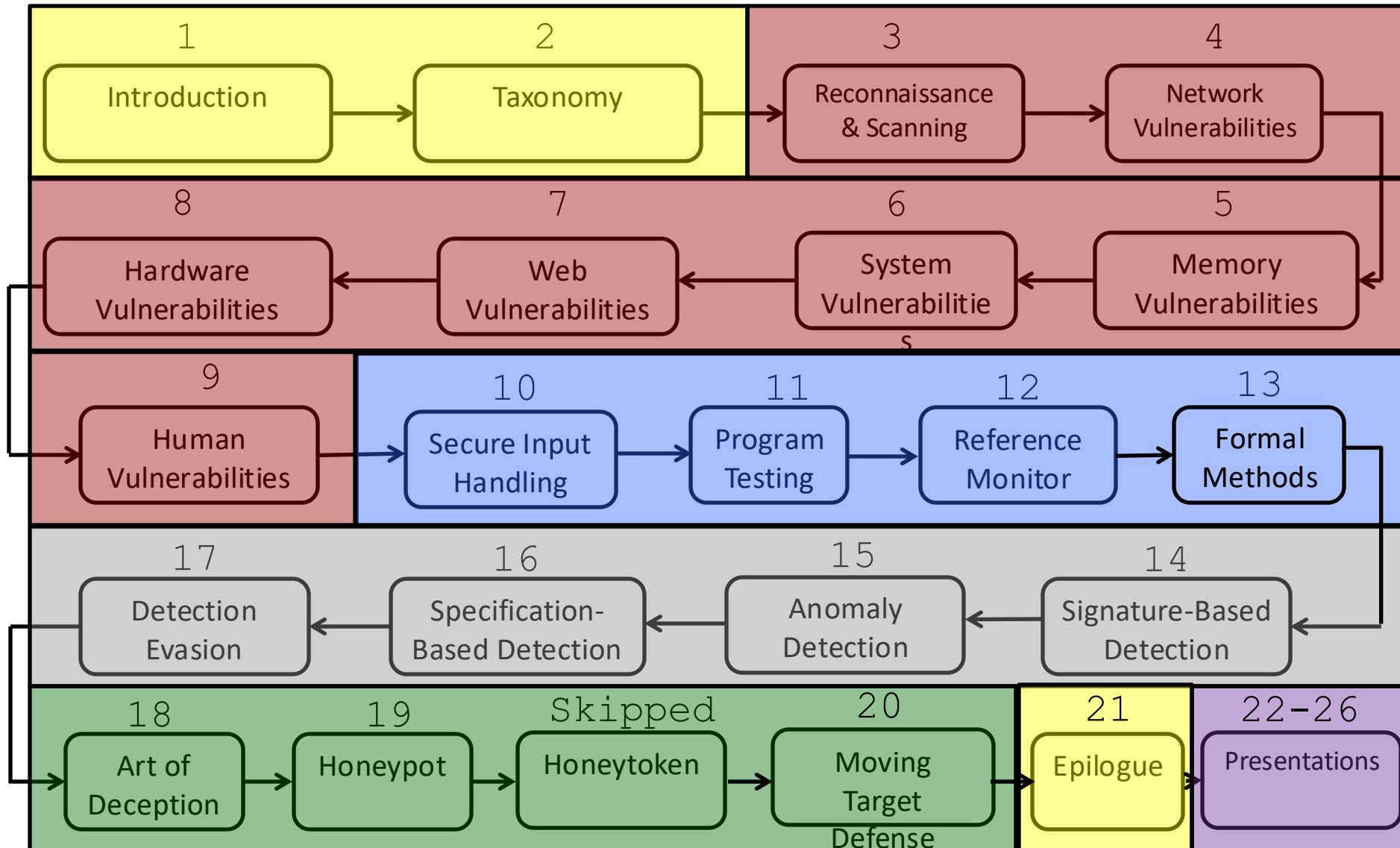
- 21 lectures, this one included
- 2 quizzes
- 2 individual project reports/demo
- 1 final project report
- 1 presentation project
- 1 CTF contest

Flashback of lectures



Overview





At this point, you should feel proud of yourself

- We have covered major methodologies used for cybersecurity (except cryptography)
- If you do well on this course, hopefully you can land a decent cyber security job



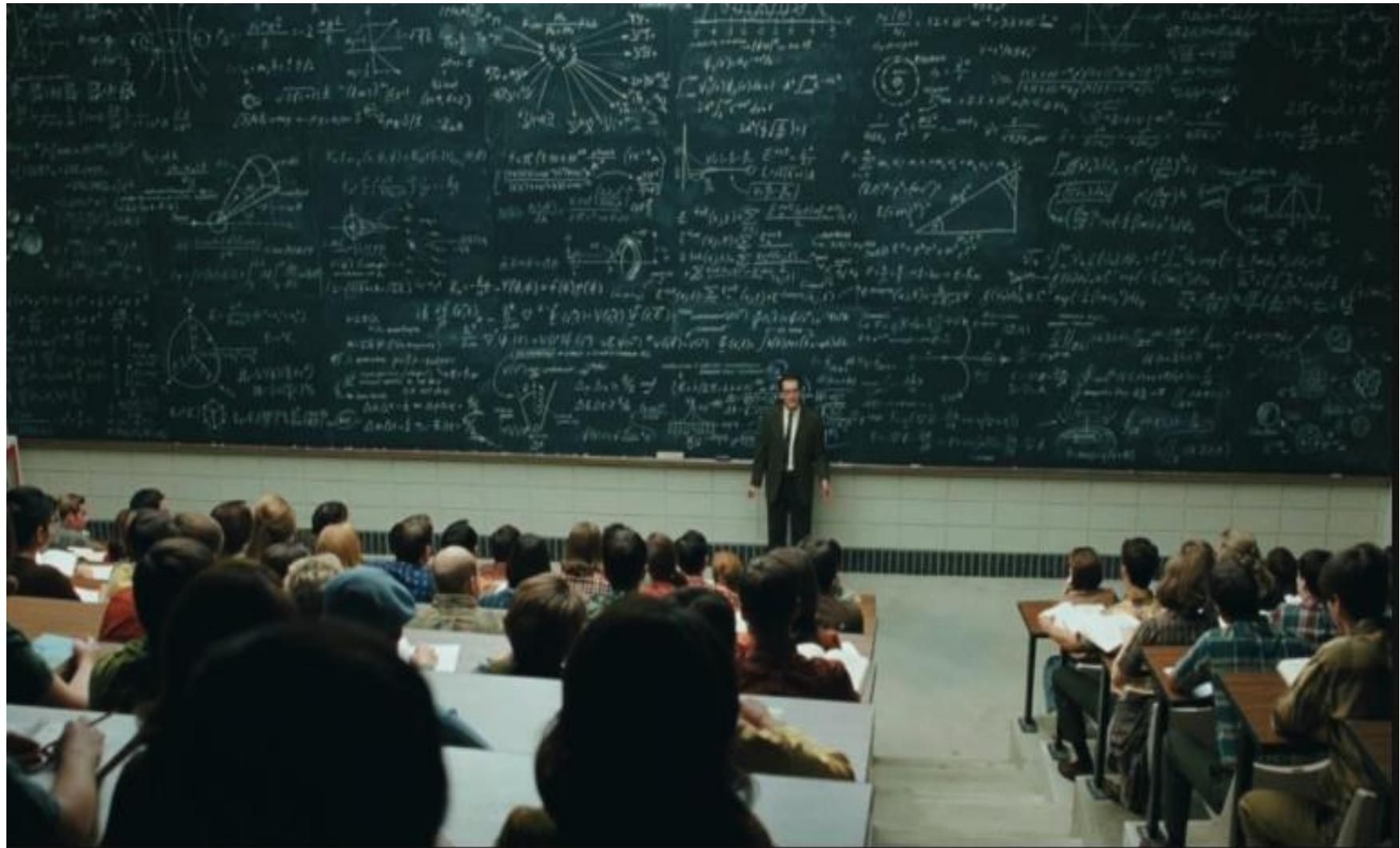
I am thankful for...

Thank You!

Constant feedback from you



Presence in class during the journey



Being active in class



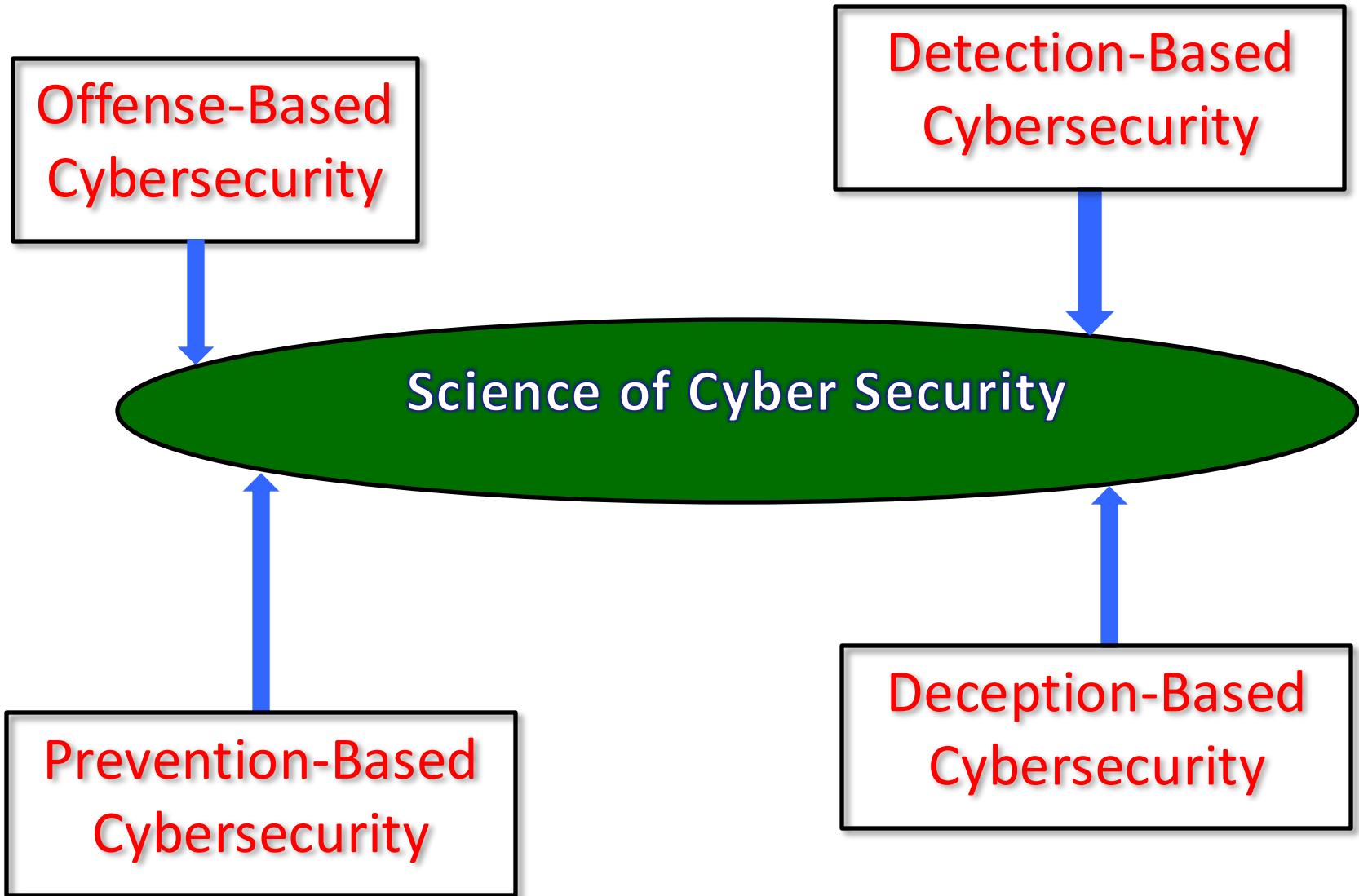
Work hard on the projects



A few things I hope you would understand...



Overview



Voting: Difficulty level

What do you think of the overall difficult level of the class?

- A: Difficult
- B: Easy
- C: About right
- D: Refuse to answer

Voting: What is your most favorite topic?

- A: Offense-based cyber security
- B: Prevention-based cyber security
- C: Detection-based cyber security
- D: Deception-based cyber security

Voting: What is your least favorite topic?

- A: Offense-based cyber security
- B: Prevention-based cyber security
- C: Detection-based cyber security
- D: Deception-based cyber security

Voting: Capture-The-Flag contest

- What is your opinion about the Capture-The-Flag contest project?

- A: I really enjoy it
- B: Honestly I hate it
- C: It's OK
- D: Refuse to comment

Voting: Quizzes

- **What is your opinion about the quiz?**

- A: I really enjoy it
- B: Honestly I hate it
- C: It's OK
- D: Refuse to comment

Second Quiz

- Date: 11/12 (Wednesday)
- Time: 10-10:45AM
- Location: this classroom
- Coverage: all lectures after Quiz 1 (i.e., Lectures 10-20)
- Format: True/False questions

Recruiting... I am trying to get students to help with my projects...

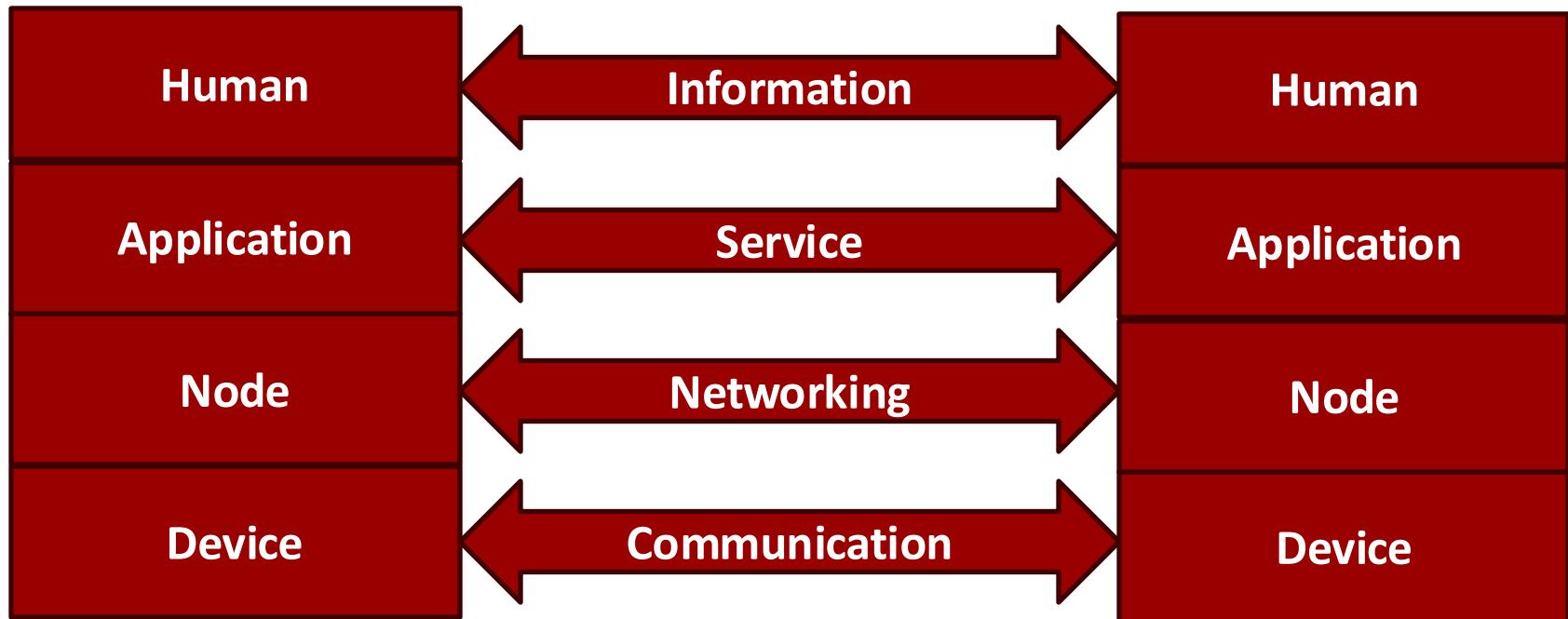


My research focus

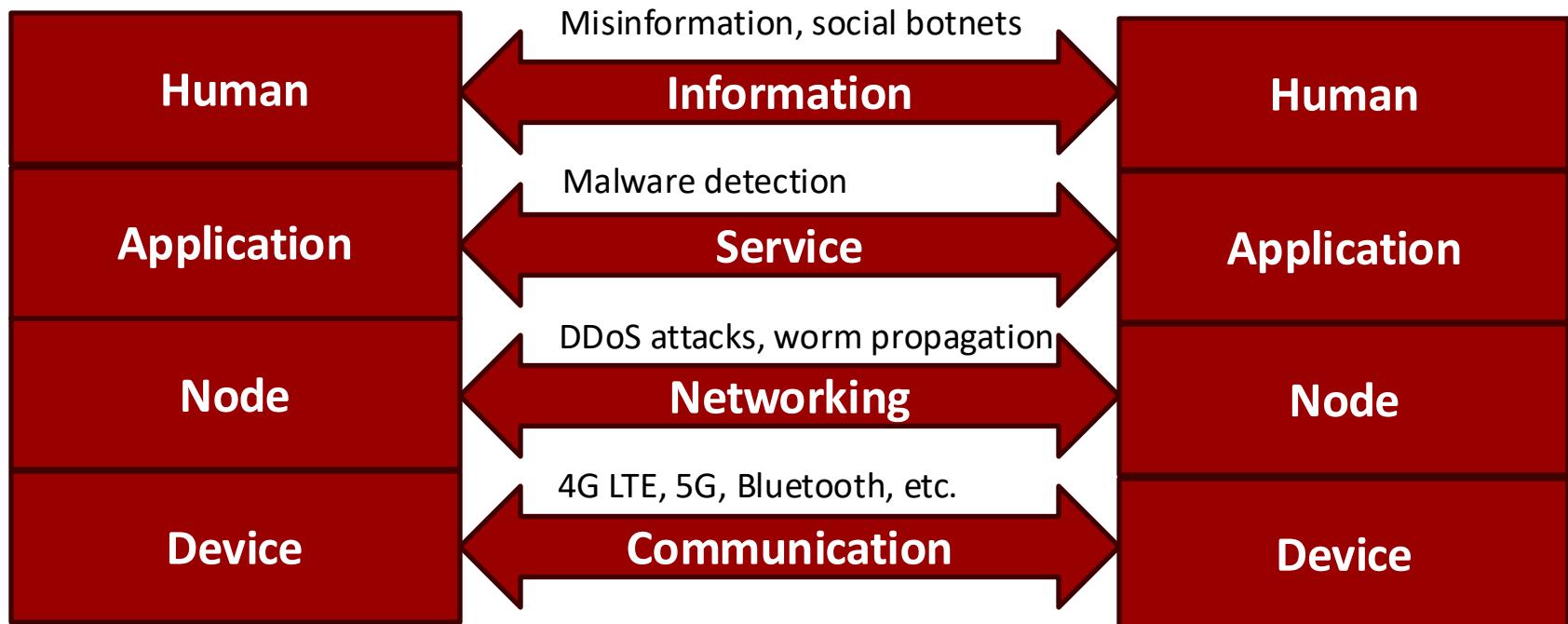


**Cybersecurity for
Distributed and
Networked Systems**

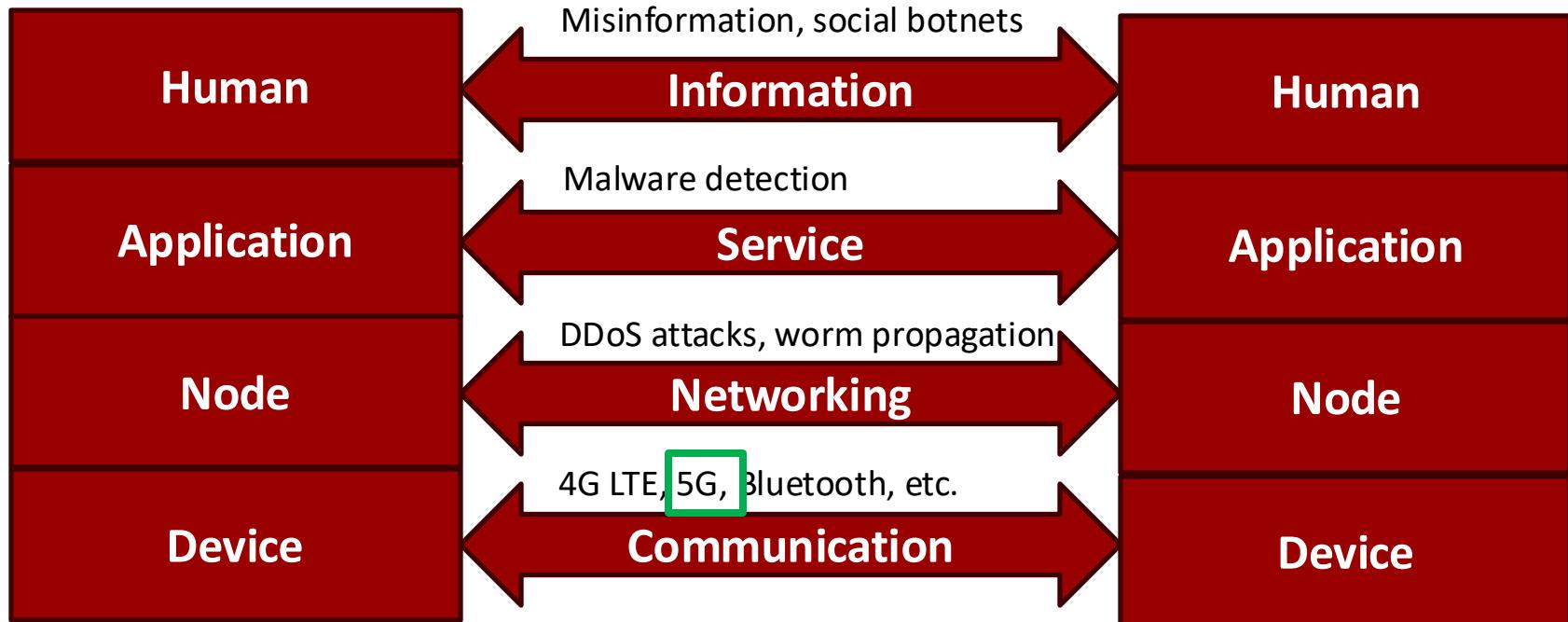
Distributed and networked systems



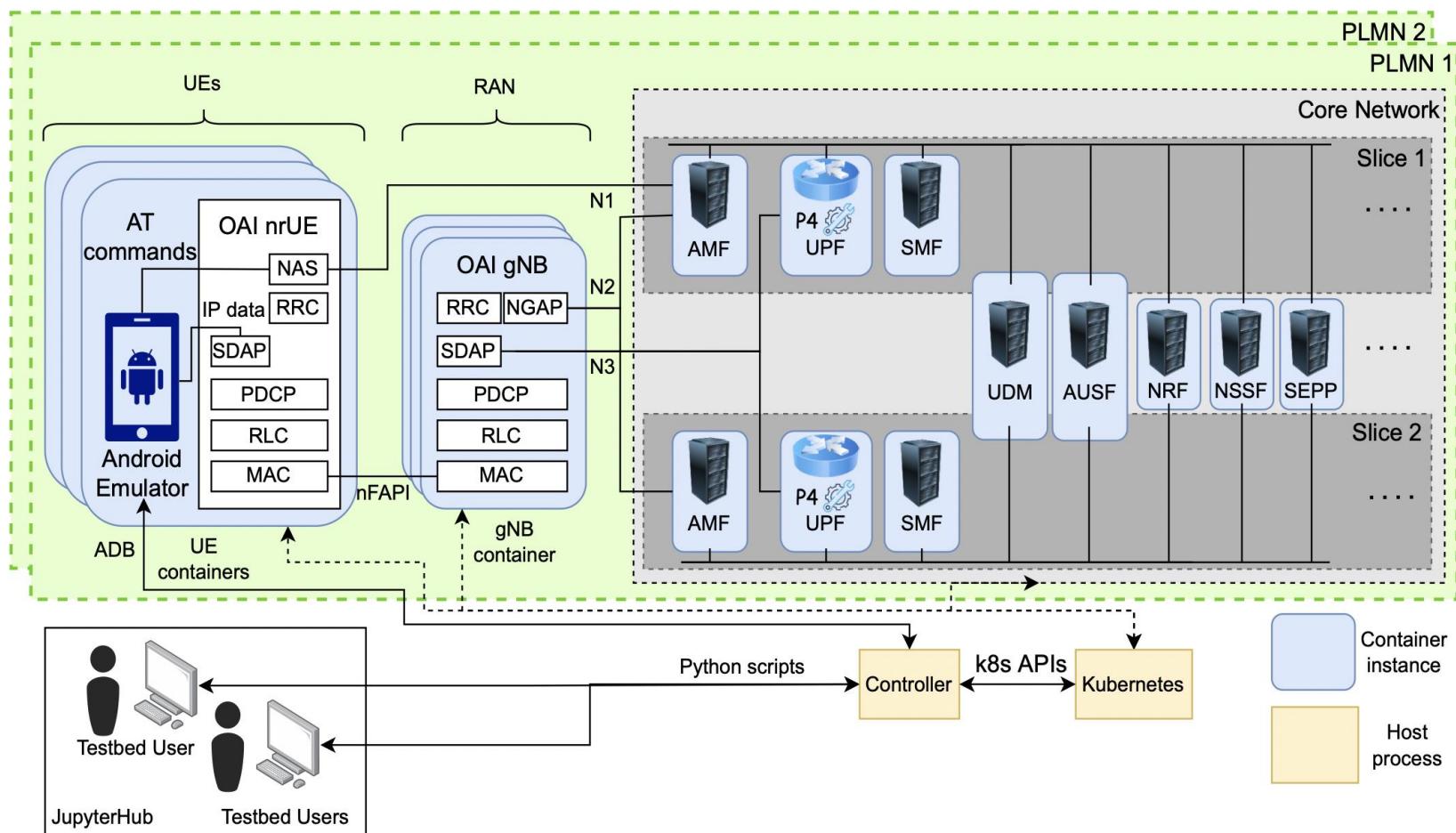
Security of distributed and networked systems



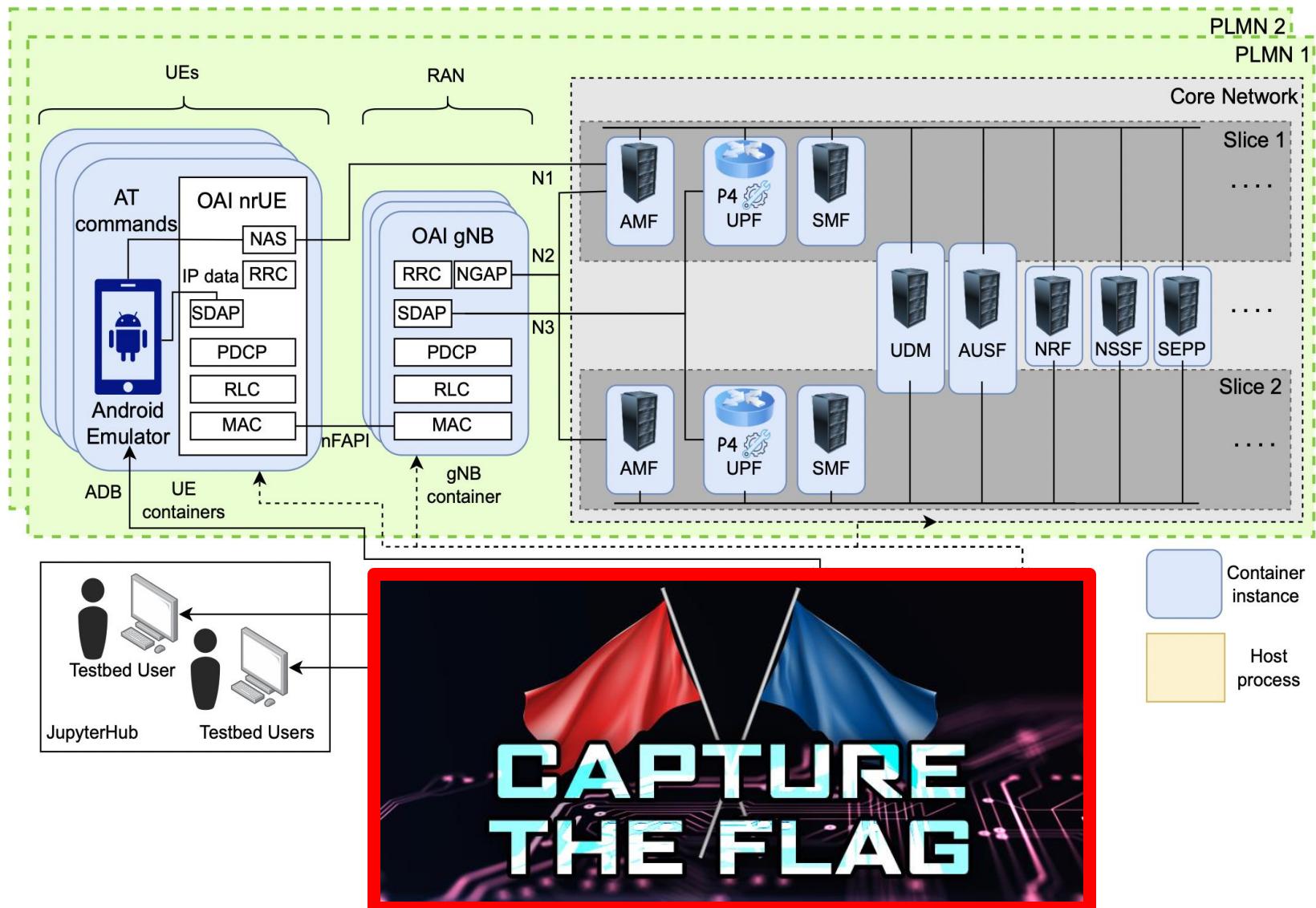
Active project:



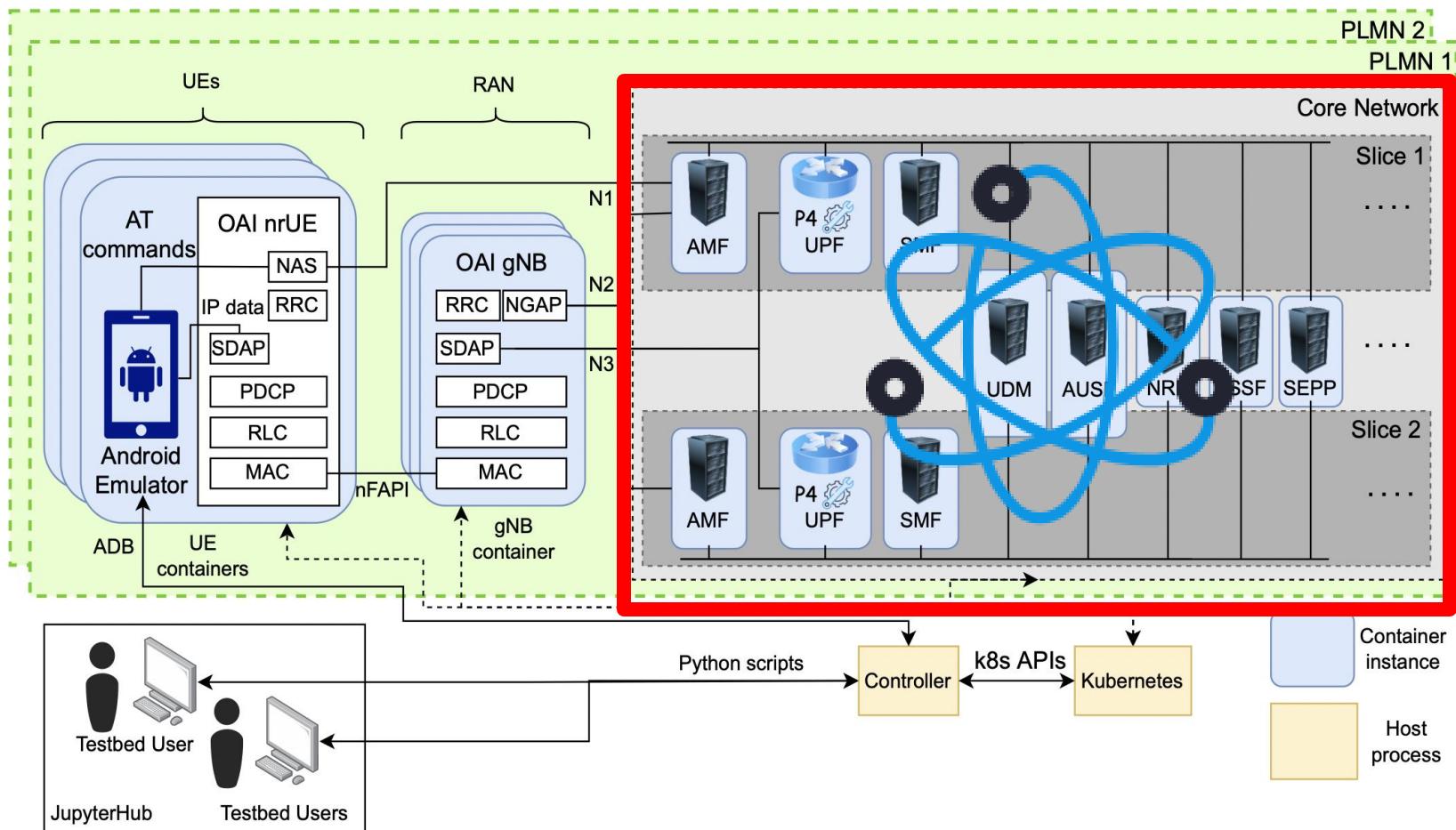
VET5G Testbed



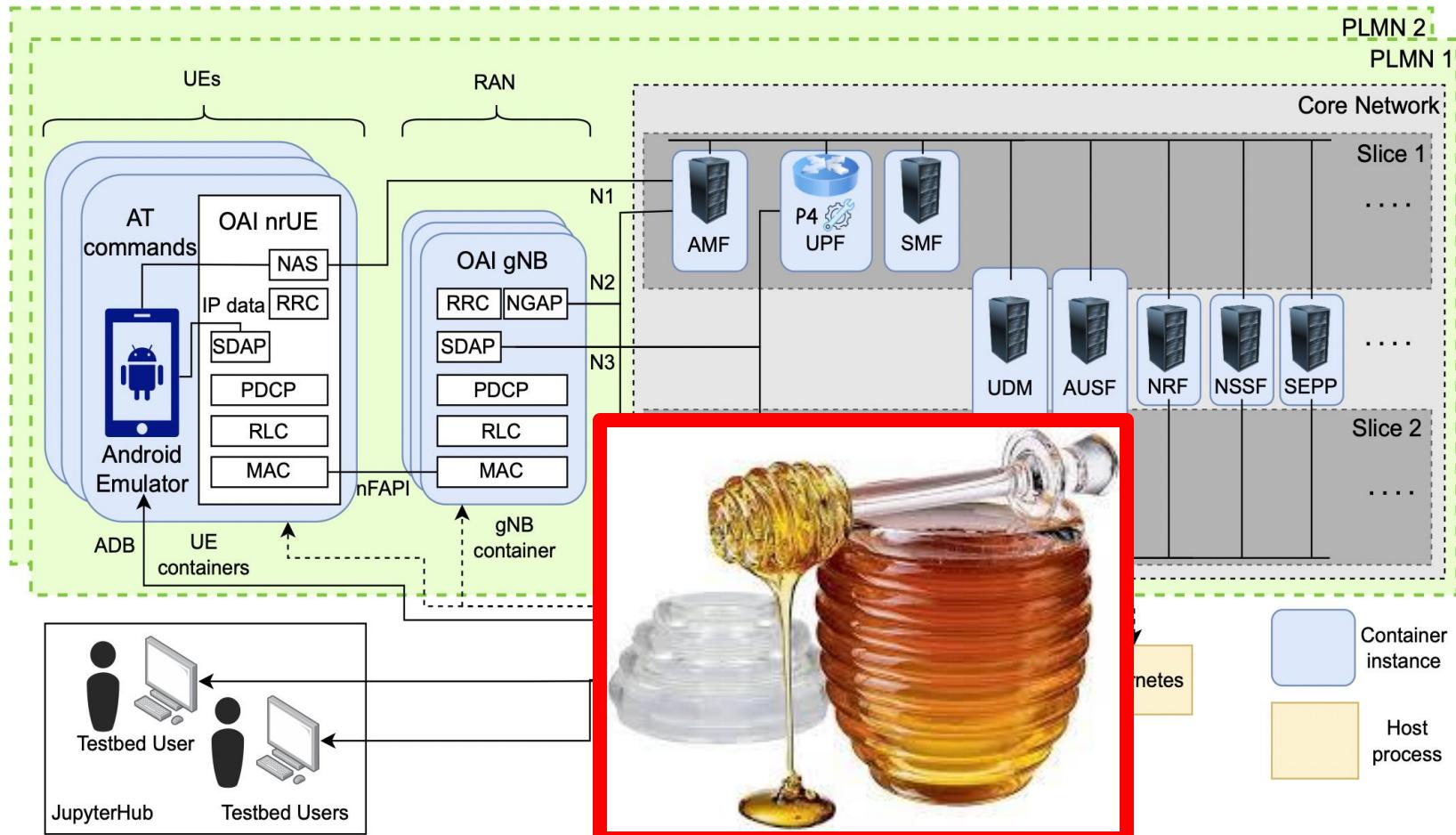
Project 1: Capture-The-Flag Competition



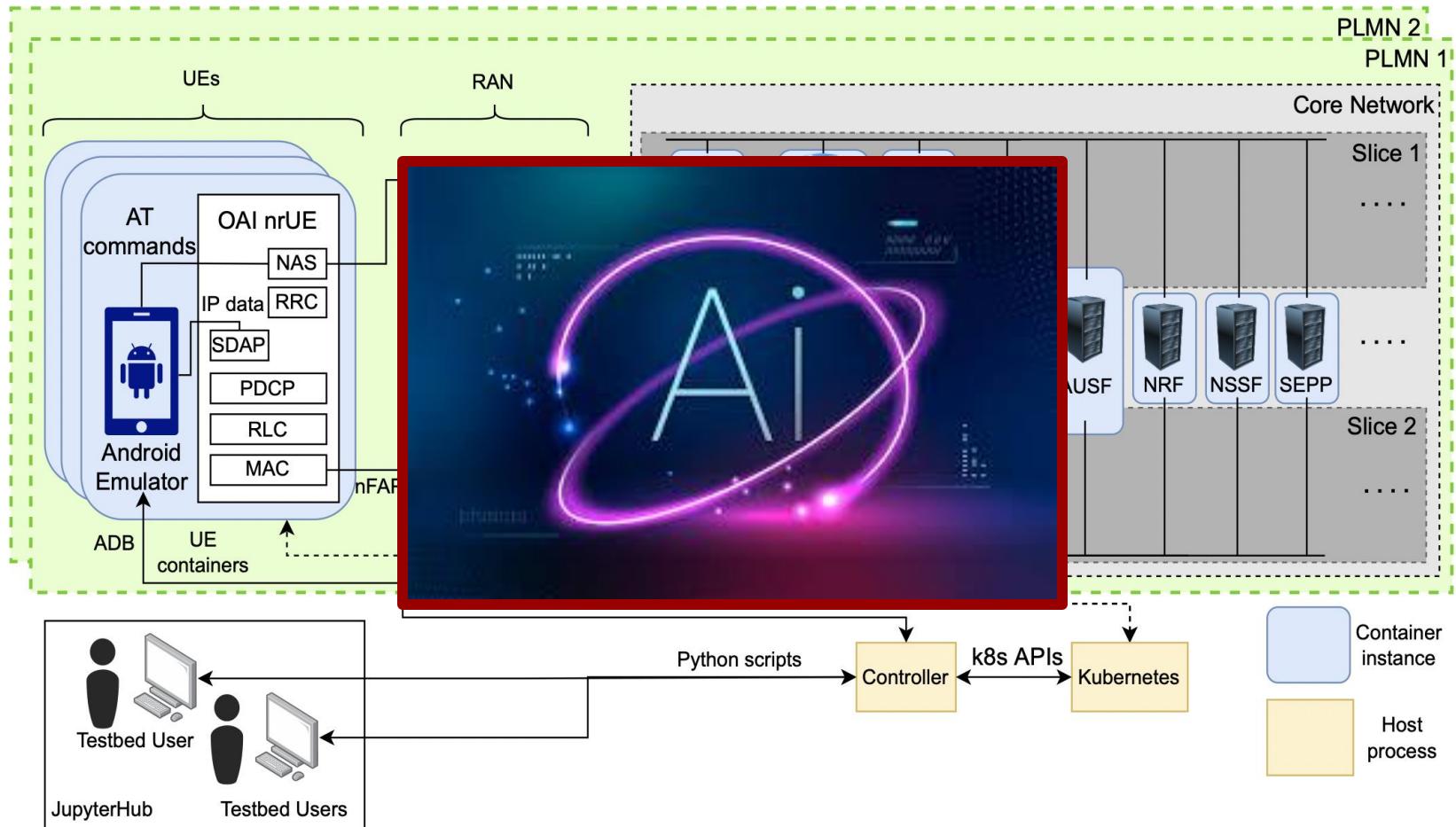
Project 2: Policy Verification



Project 3: Deception for 5G



Project 4: AI for 5G



If you are interested in our research,



Particularly, more challenges to CTF5G!

Reconnaissance	Resource Development	Initial Access	Execution	Persistence	Privilege Escalation	Defense Evasion	Credential Access	Discovery	Lateral Movement	Collection	Command And Control	Exfiltration	Impact	Fraud
2 techniques	4 techniques	7 techniques	5 techniques	5 techniques	2 techniques	17 techniques	9 techniques	17 techniques	7 techniques	17 techniques	6 techniques	4 techniques	18 techniques	5 techniques
Network Service Discovery &	Acquire Infrastructure &	Valid Accounts &	Command and Scripting Interpreter &	Valid Accounts &	Valid Accounts &	Rootkit & Masquerading	Network Sniffing &	Remote System Discovery &	Remote Services &	Network Sniffing &	Exfiltration Over Alternative Protocol &	Automated Exfiltration &	Exploit Public-Facing Application &	Abuse Of Inter-operator Interfaces
Gather Victim Host Information &	Develop Capabilities &	Exploit Public-Facing Application &	Software Deployment Tools &	Traffic Signaling &	Escape to Host &	Brute Force &	Supply Chain Compromise &	Automated Exfiltration &	Software Deployment Tools &	Exploit Public-Facing Application &	Application Layer Protocol &	Exfiltration Over C2 Channel &	Hardware Additions &	Alter Subscribe Profile
Obtain Capabilities &	Supply Chain Compromise &	Trusted Relationship &	Exploitation for Client Execution &	Implant Internal Image &	Pre-OS Boot &	Traffic Signaling &	Credentials from Password Stores &	Remote Services &	Exploitation of Remote Services &	Trusted Relationship &	Proxy &	Exfiltration Over Alternative Protocol &	Exploitation of Remote Services &	Charging Fraud Via NF Contro
Stage Capabilities &	Unauthorized Access To Network Exposure Function (NEF) Via Token Fraud	Registration Of Malicious Network Functions	gNodeB Component Manipulation	Program Wrapper	Implant Internal Image &	Adversary-in-the-Middle &	Network Service Discovery &	Escape to Host &	Unauthorized Access To Network Exposure Function (NEF) Via Token Fraud	Adversary-in-the-Middle &	Traffic Signaling &	Protocol Tunneling &	Network Denial of Service &	Falsify Interconn Invoice
	Exploit Semi-public Facing Application				Pre-OS Boot &	Container Administration Command &	Exploitation of Remote Services &	Container Administration Command &	Radio Control Manipulation Via Rogue xApps	Network-side SMS Collection	Protocol Tunneling &	Exfiltration Over Web Service &	Endpoint Denial of Service &	SIM Cloni
	Radio Control Manipulation Via Rogue xApps				Impair Defenses &	Hide Artifacts &	SIM Cloning	Unauthorized Access To Core Network Function Via Token Abuse	Network Function Service Discovery	Network Flow Manipulation	Telecom Protocol Payload		Data Manipulation &	
					Network Boundary Bridging &	Weaken Encryption &	Force Generation Of Subscriber Keys	Network Flow Manipulation	Radio Control Manipulation Via Rogue xApps	Memory Scraping			Endpoint Denial of Service &	
					Bypass Home Routing	Weaken Integrity		Locate UE	Unauthorized Access To Core Network Function Via Token Abuse	Redirection Of Traffic Via User Plane Network Function			Redirection Of Traffic Via User Plane Network Function	
						Spoof Network Slice Identifier	Malicious VNF Instantiation			Fraudulent AMF Registration For UE In UDM			Device Database Manipulation	
						Manipulate Virtual	Shared Resource Discovery			Locate UE			Vandalism Of Network Infrastructure	
							Charging Data			Malicious VNF Instantiation			Tunnel ID Uniqueness	

<https://fight.mitre.org>

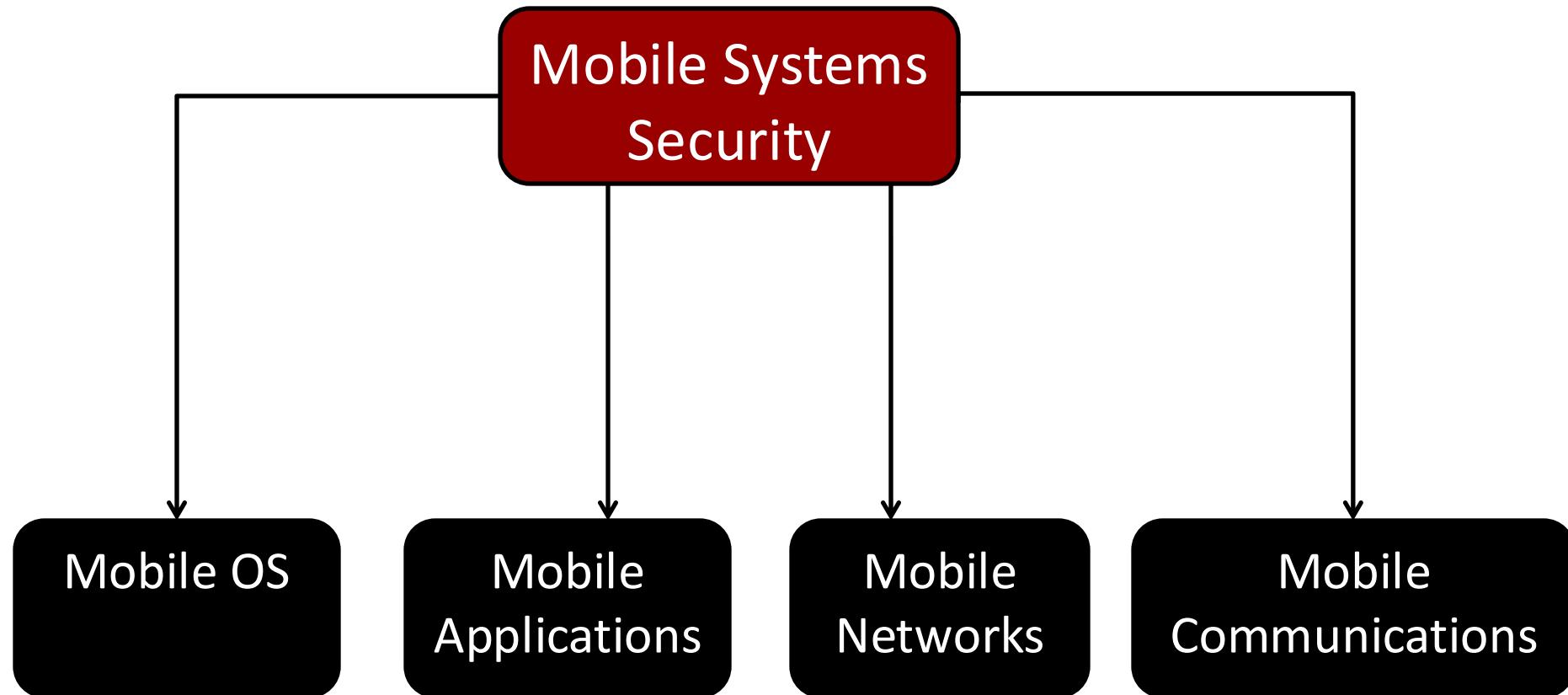
Existing challenges

	FiGHT Tactics	Attack Type
1	Reconnaissance	GTPScan, Newtork Reconnaissance
2	Resource Development	IMSI-catcher*, Fake basestation*
3	Initial Access	Buffer Overflow
4	Execution	Registration Of Malicious Network Functions, NoSQL Injection, SQL Injection
5	Persistence	Program wrapper
6	Privilege Escalation	Heap Overflow, SUID Exploit
7	Defense Evasion	Decoy Recognition, Authorization Bypass
8	Credential Access	Dictionary Attack
9	Discovery	NF discovery through NRF, Parameter Misuse
10	Later Movement	OAuth2.0 scope exploitation
11	Collection	Known Plaintext attack
12	Command and Control	Reverse Proxy using Caddy, TinyShell
13	Exfiltration	DNS tunneling
14	Impact	Rapid Reset, PFCP attack
15	Fraud	SIM cloning

* Still under development.

CS427/527 next semester

■ Mobile systems security (CS427/527)



CS427/527 main topics

- **Introduction: security concepts, syllabus**
- **Mobile OS security: Android OS and security mechanisms**
- **Mobile application security: mobile malware analysis**
- **Mobile communication security: security of communication protocols such as NFC, WiFi, and Bluetooth**
- **Mobile network security: 4G LTE network security, 5G network security**

Course Evaluation and Survey



What is CES?

- The Course Evaluation and Survey (CES) is Binghamton University's new online platform for administering student course evaluations, powered by Watermark.
- Beginning in Fall 2025, CES will replace the previous Student Opinion of Teaching (SOOT) process.

CES survey period

- Evaluations open two weeks before the course ends and close on the last day of the course.



Presentations



Dates: 11/17, 11/19, 11/24, 12/1, 12/3

- **Each student:**

- Presentation time: 5 minutes
 - Setup time: 1 minute

- **12 presentations planned for each day**
- **Presentations will be evaluated by your classmates**
- **Please be professional in evaluation**
- **Please try to use your own machine for presentation**
 - Please send all your slides before the presentation
 - Slides needed for presentation score

CS 459/559: Presentation Evaluation Sheet

Your name: _____ (mark X in the table for your own presentation)

Have you finished CES survey? YES NO

Order	Topic	Score (1-4)
1		
2		
3		
4		
5		
6		
7		
8		
9		
10		
11		
12		

Lottery



Thanks for taking this course



The End