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

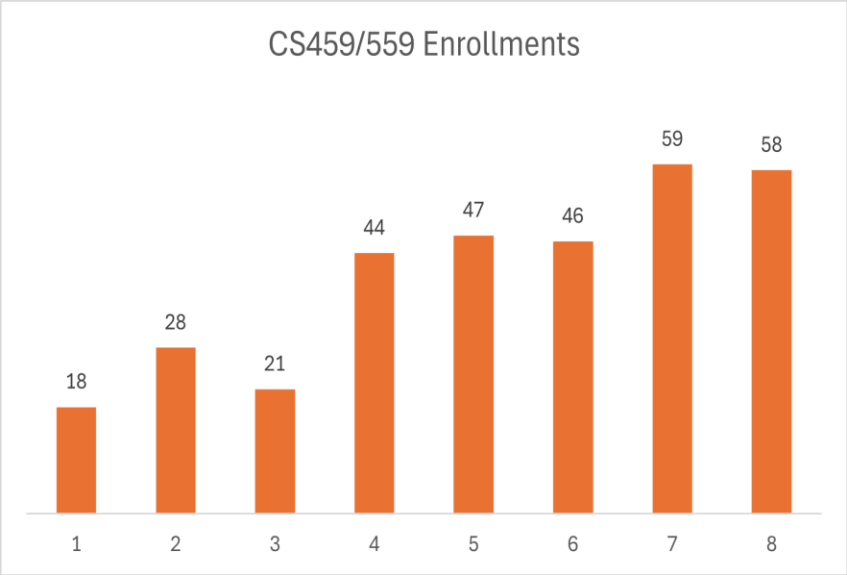
What we have learned so far…

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: …

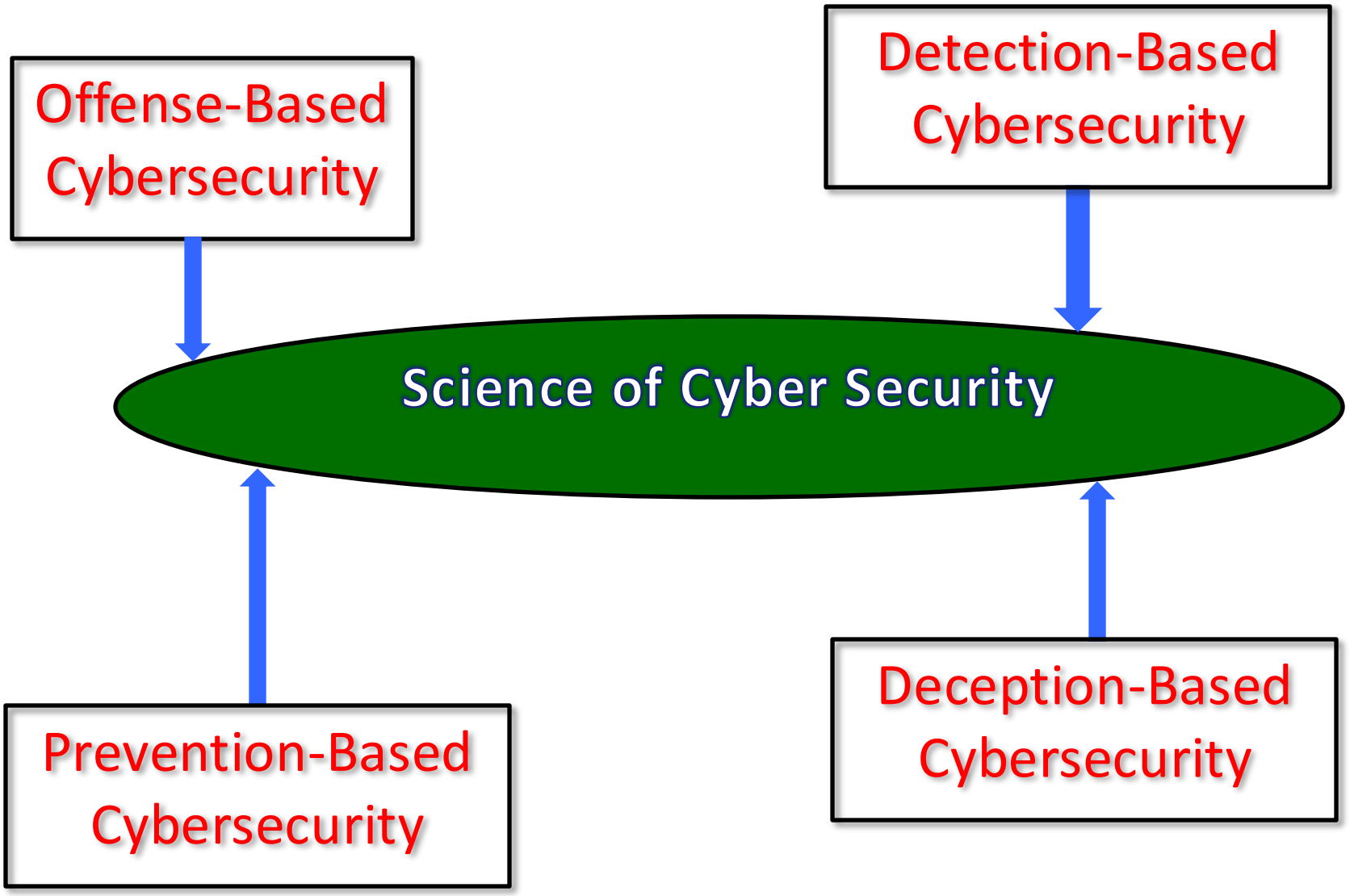


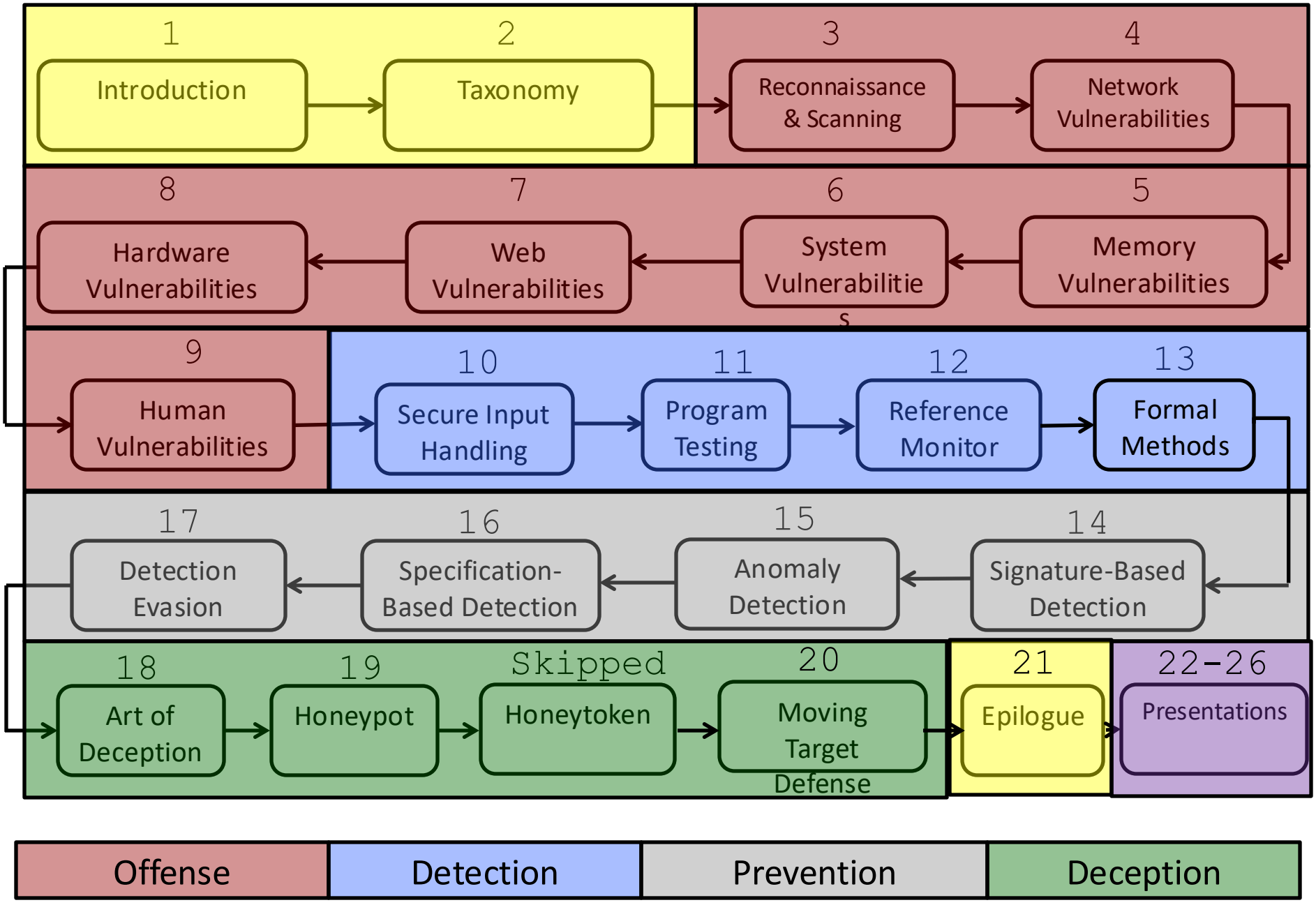
We have done or will do:

- 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


Offense-Based Cybersecurity
Detection-Based Cybersecurity
Science of Cyber Security
Prevention-Based Cybersecurity
Deception-Based Cybersecurity


1
Introduction
2
Taxonomy
3
Reconnaissance & Scanning
4
Network Vulnerabilities
8
Hardware Vulnerabilities
7
Web Vulnerabilities
6
System Vulnerabilities
5
Memory Vulnerabilities
9
Human Vulnerabilities
10
Secure Input Handling
11
Program Testing
12
Reference Monitor
13
Formal Methods
17
Detection Evasion
16
Specification-Based Detection
15
Anomaly Detection
14
Signature-Based Detection
18
Art of Deception
19
Honeypot
Skipped
Honeytoken
20
Moving Target Defense
21
Epilogue
22-26
Presentations
Offense
Detection
Prevention
Deception

At this point, you should feel proud of yourself

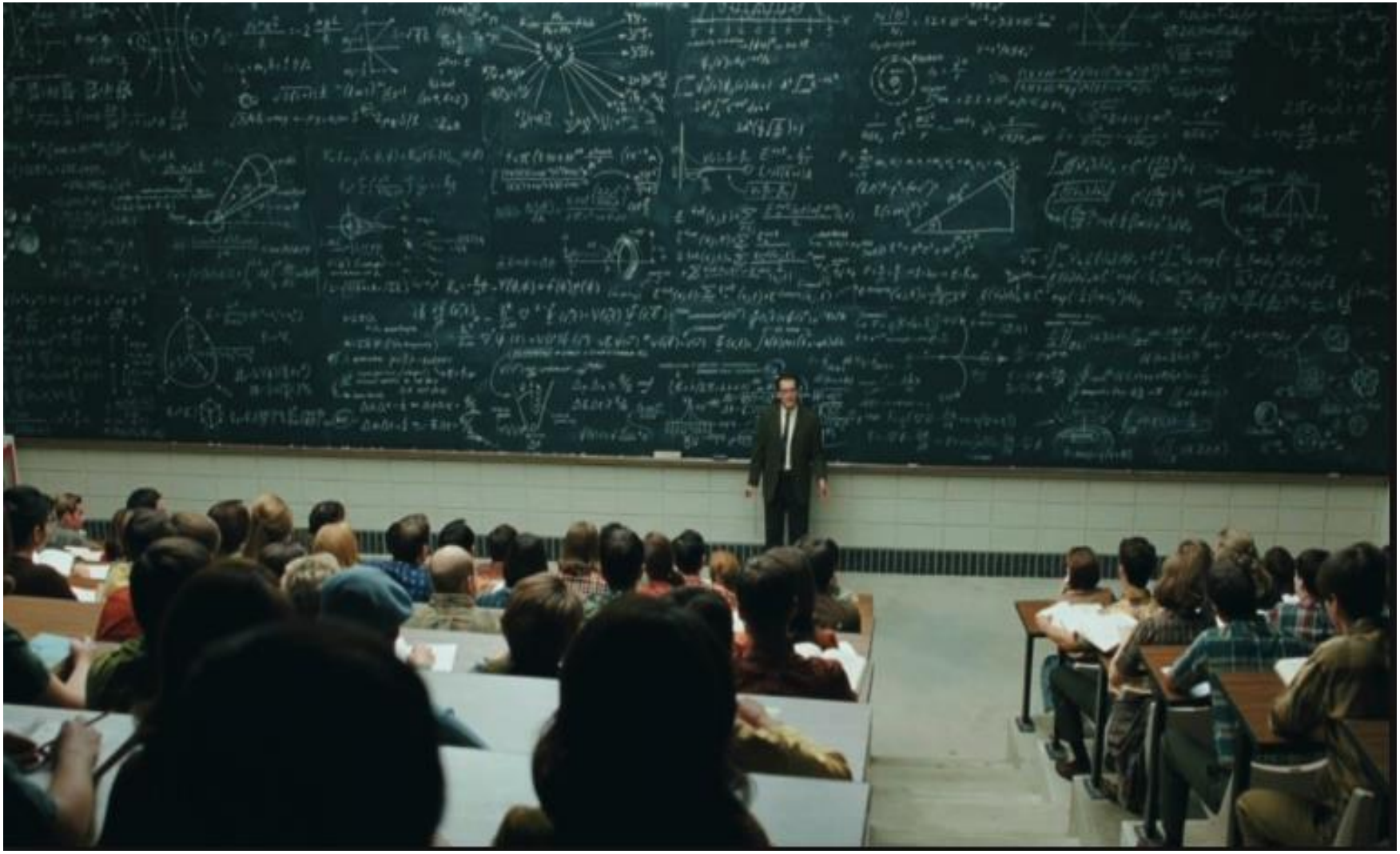
- We have covered major methodologies used for cybersecurity (except cryptography)

- If you do well on this course, hopefully you can land a decent cyber security job

I am thankful for…

Constant feedback from you

Presence in class during the journey

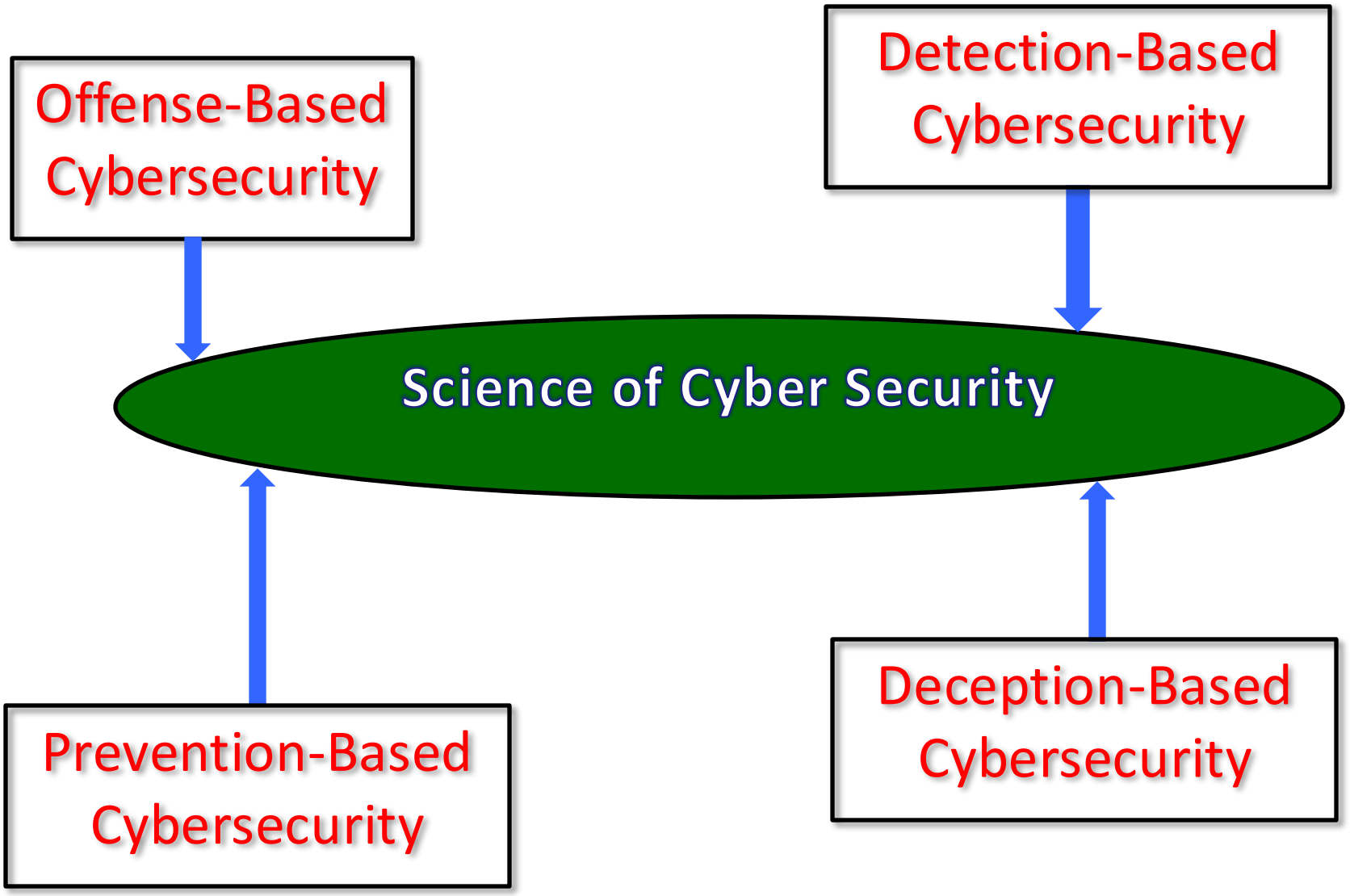


Being active in class

Work hard on the projects

A few things I hope you would understand…

Overview


Offense-Based Cybersecurity
Detection-Based Cybersecurity
Science of Cyber Security
Prevention-Based Cybersecurity
Deception-Based Cybersecurity

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

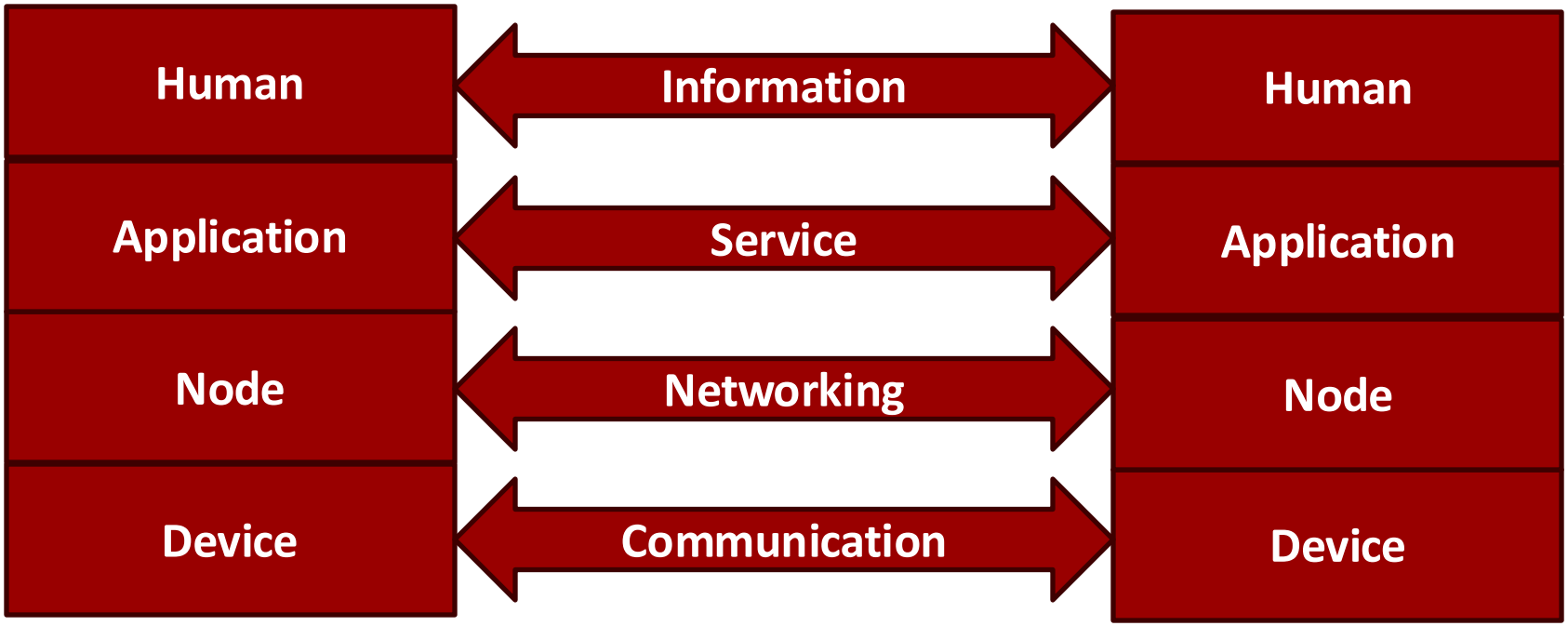
- Date: 11/12 (Wednesday)
- Time: 10-10:45AM
- Location: this classroom
- Coverage: all lectures after Quiz 1 (i.e., Lectures 10-20)
- Format: True/False questions

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

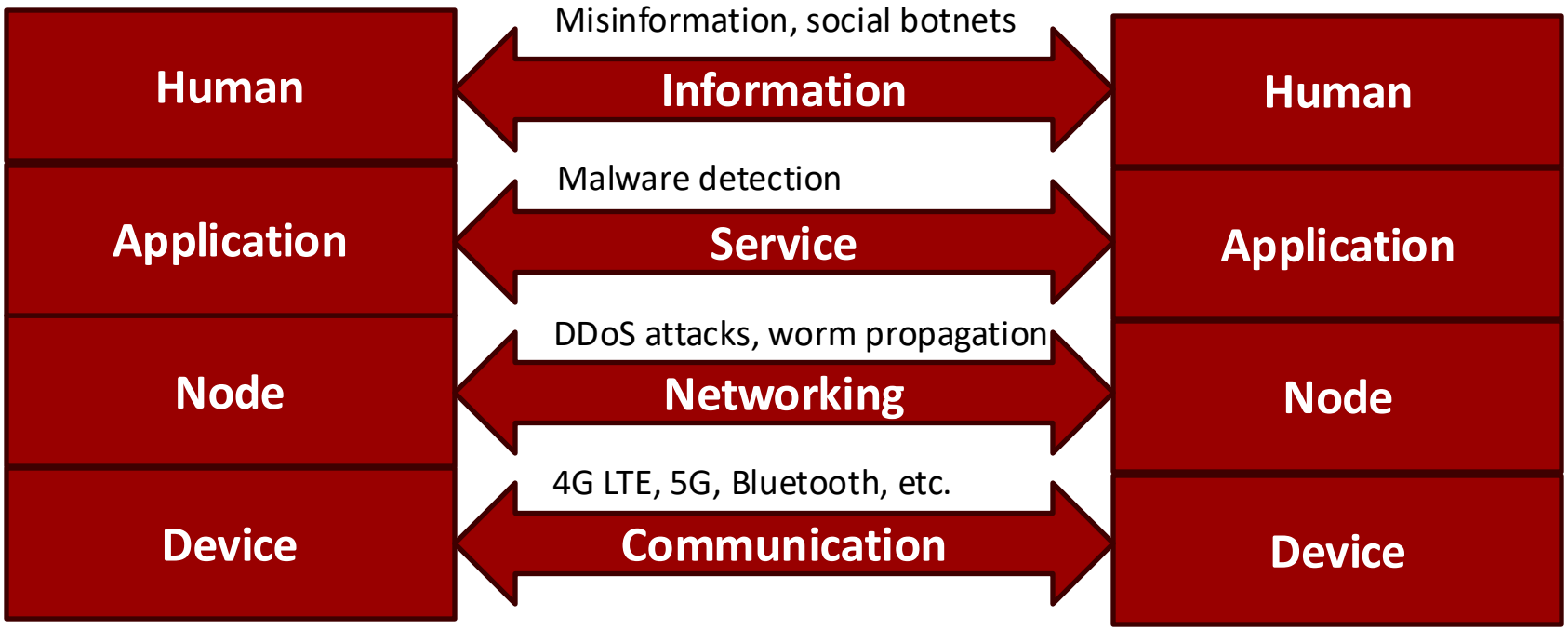
My research focus

Cybersecurity for Distributed and Networked Systems

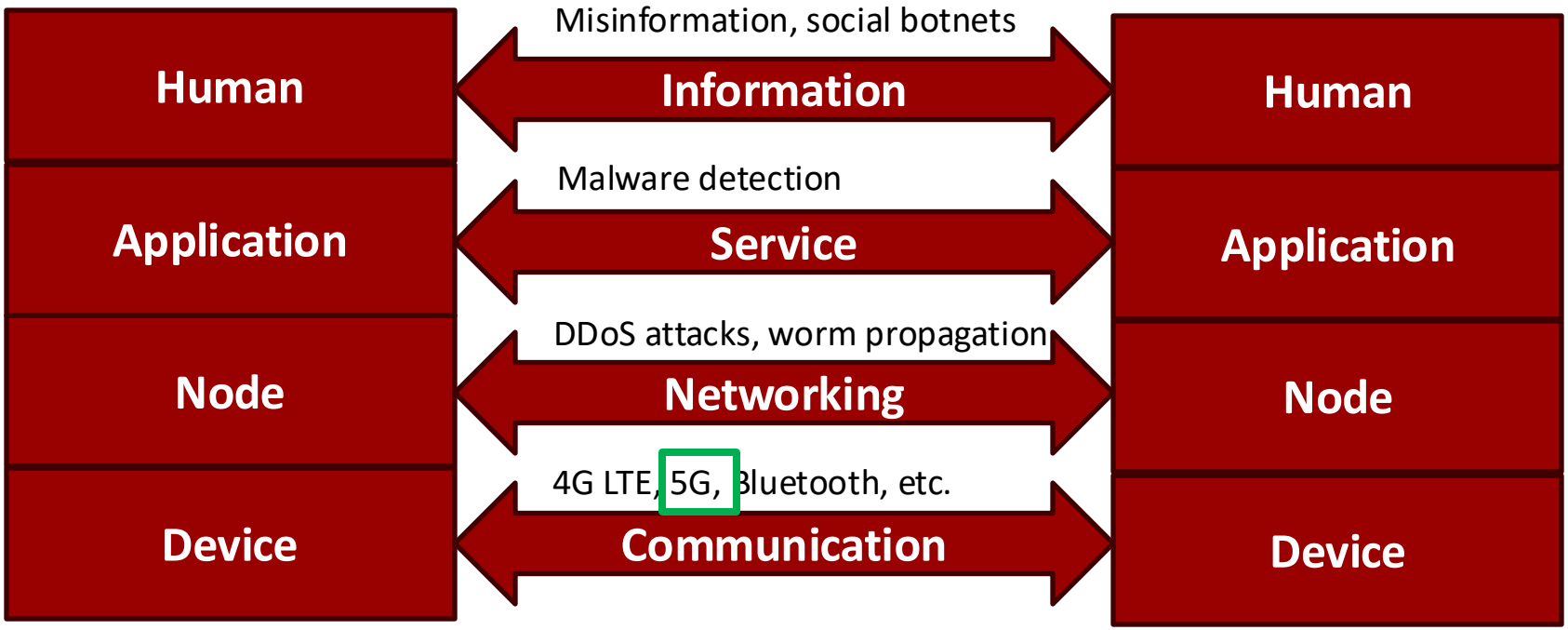
Distributed and networked systems



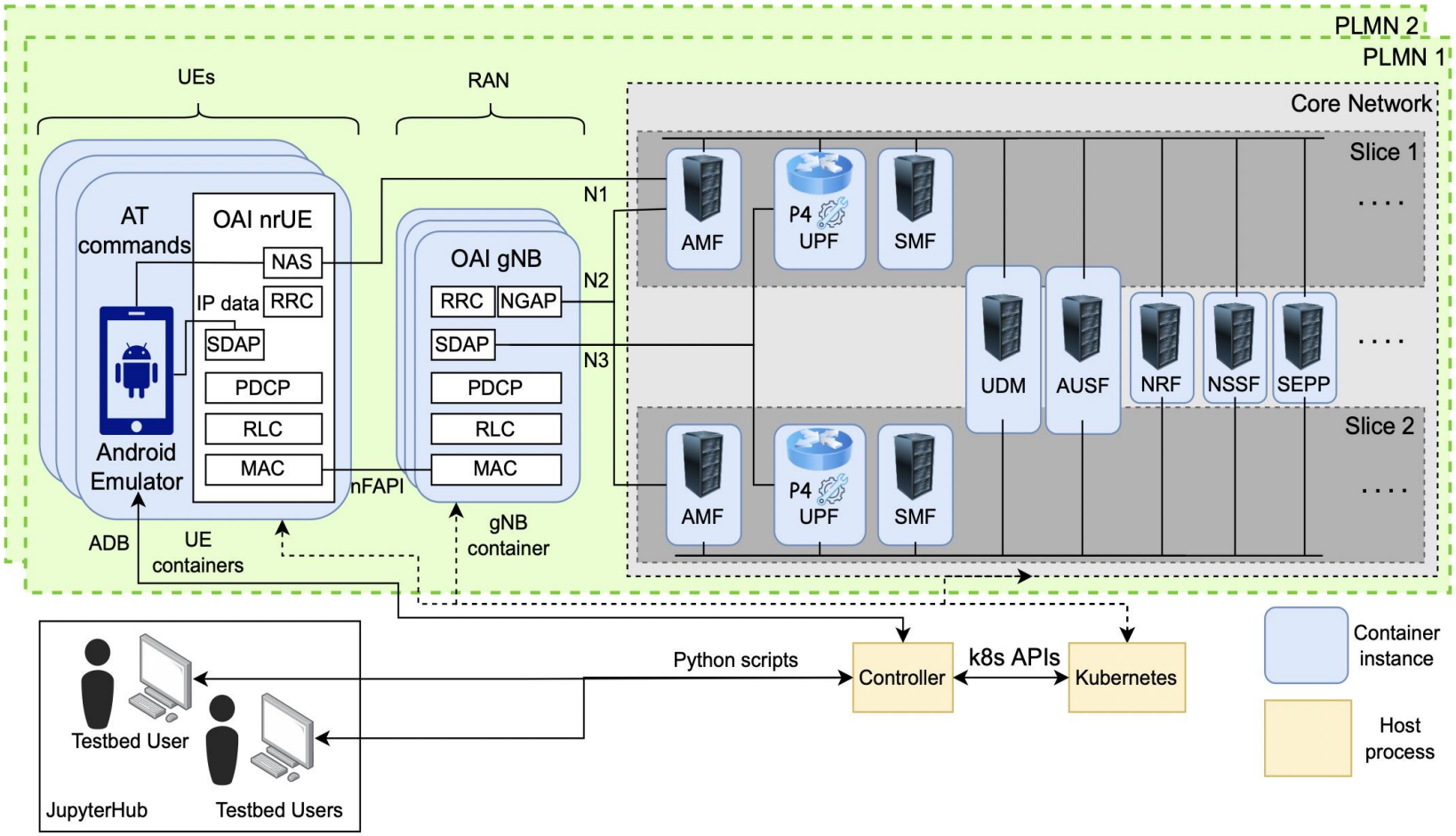
Security of distributed and networked systems



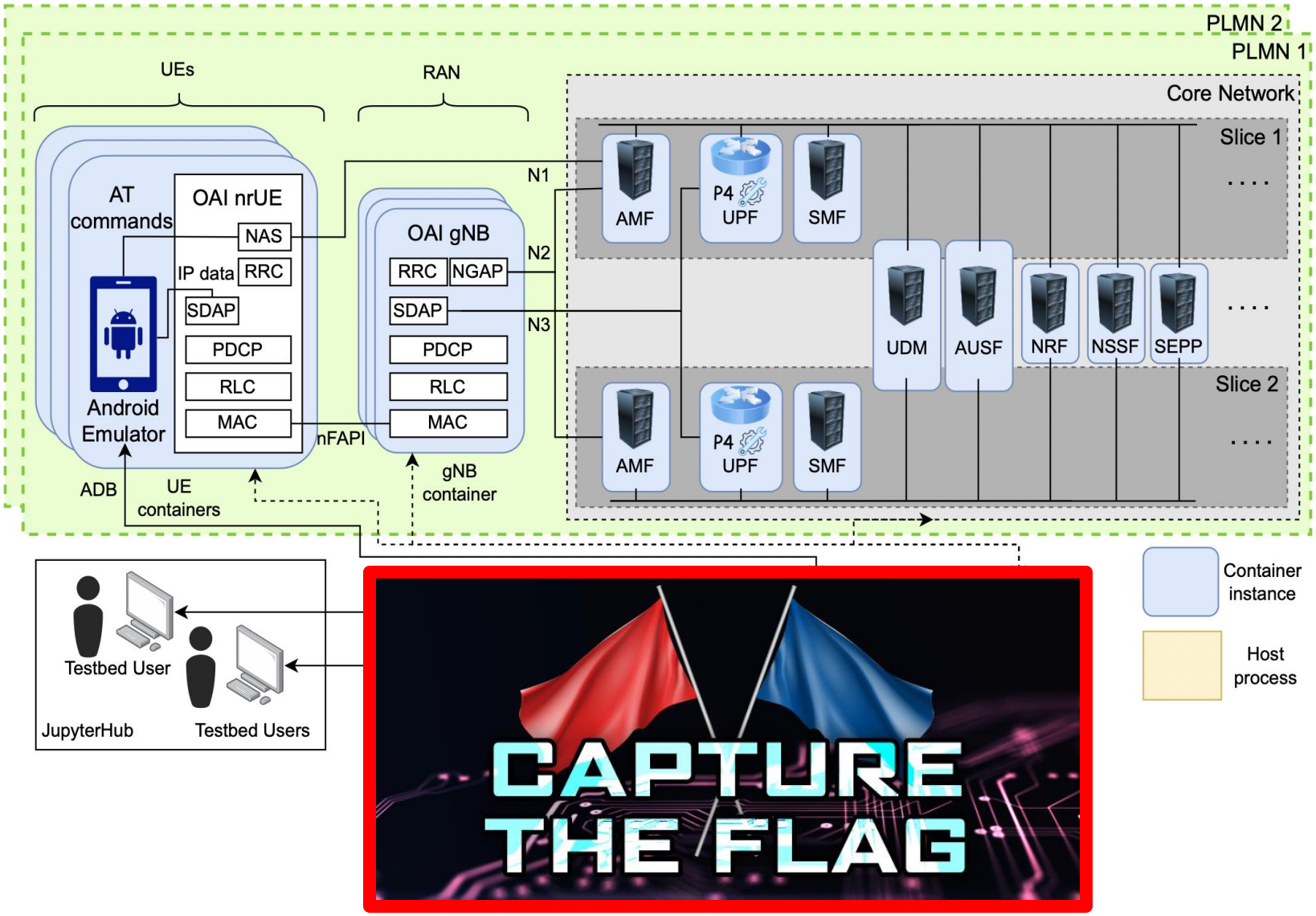
Active project:



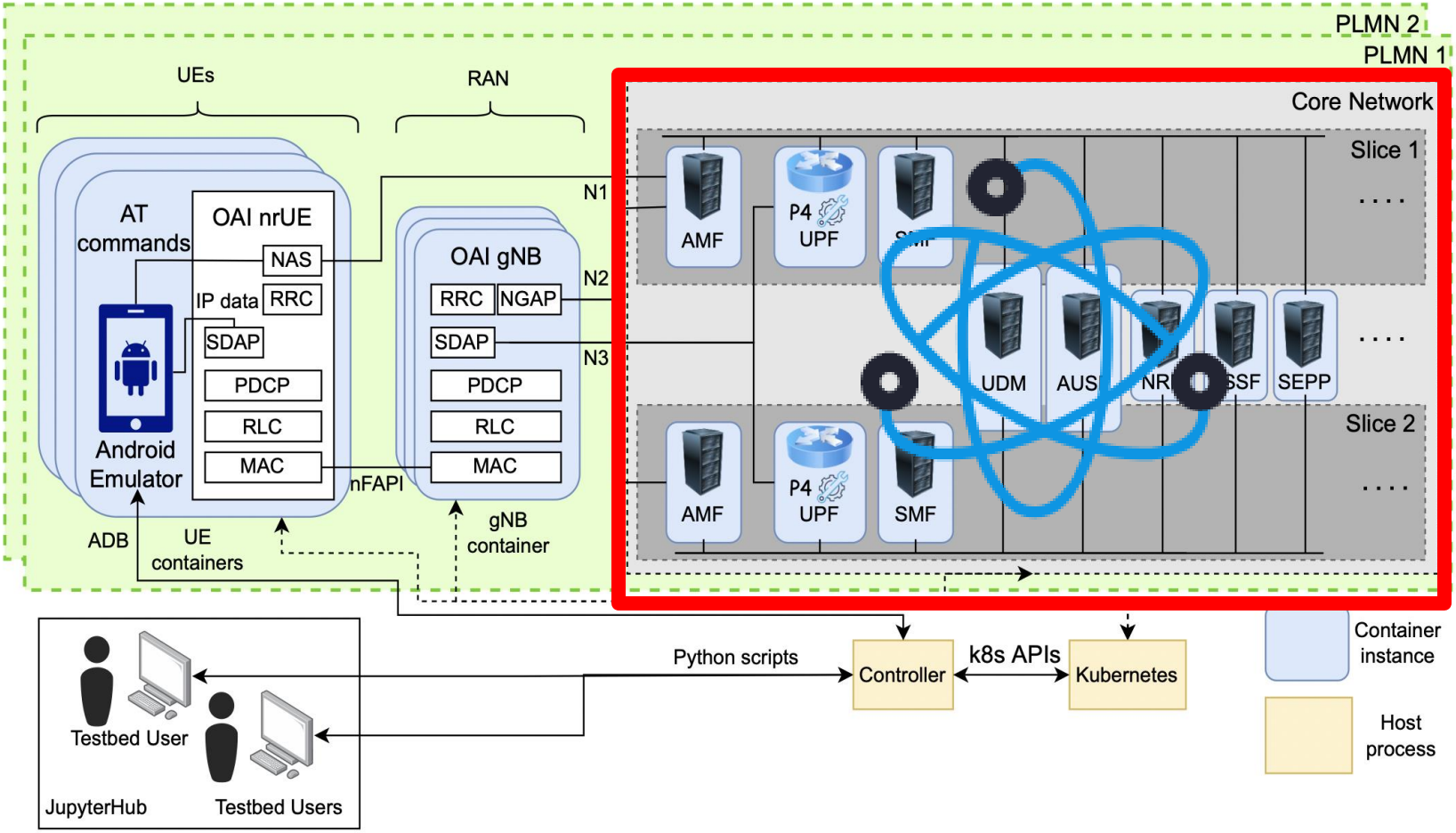
VET5G Testbed



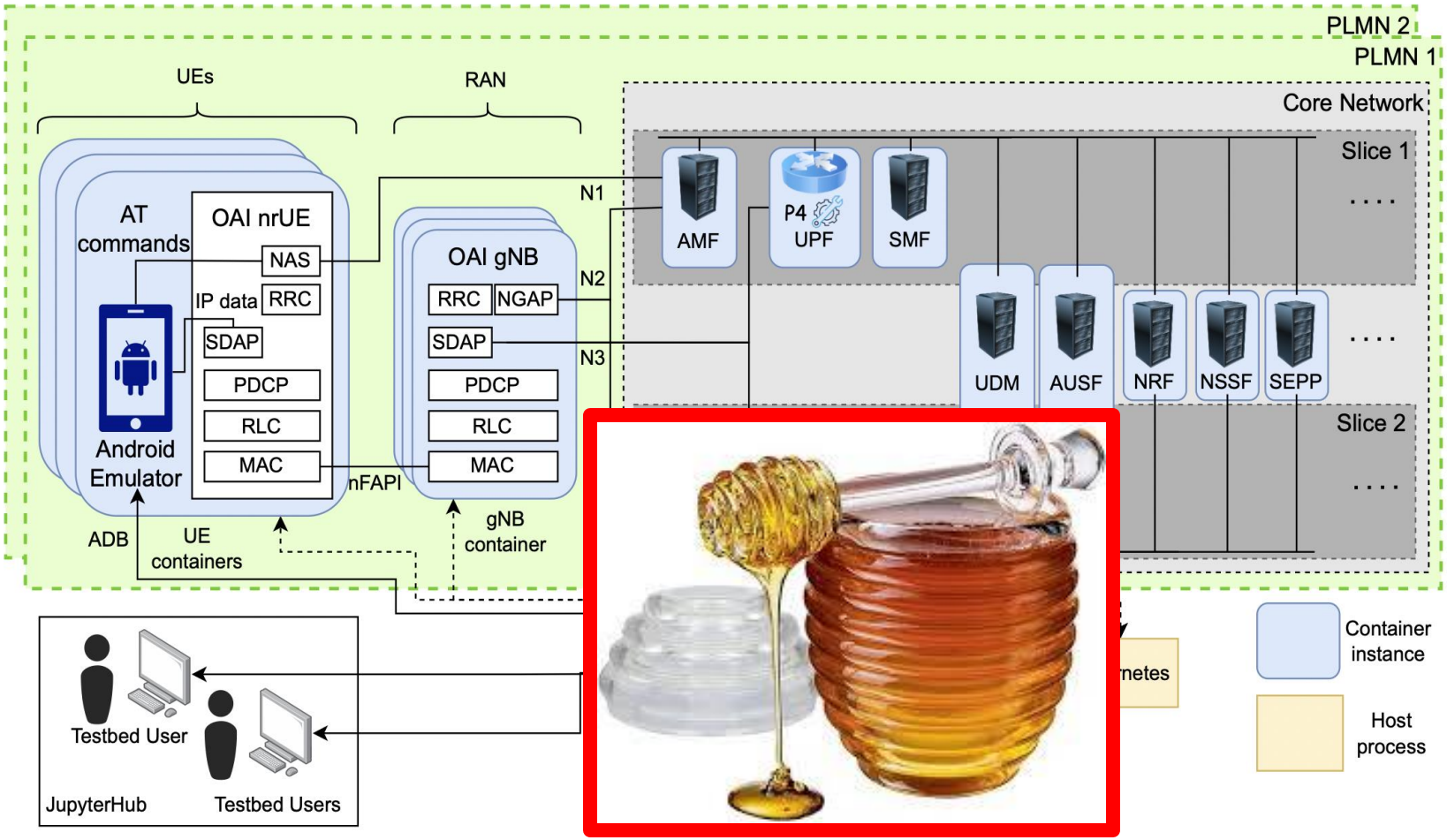
Project 1: Capture-The-Flag Competition



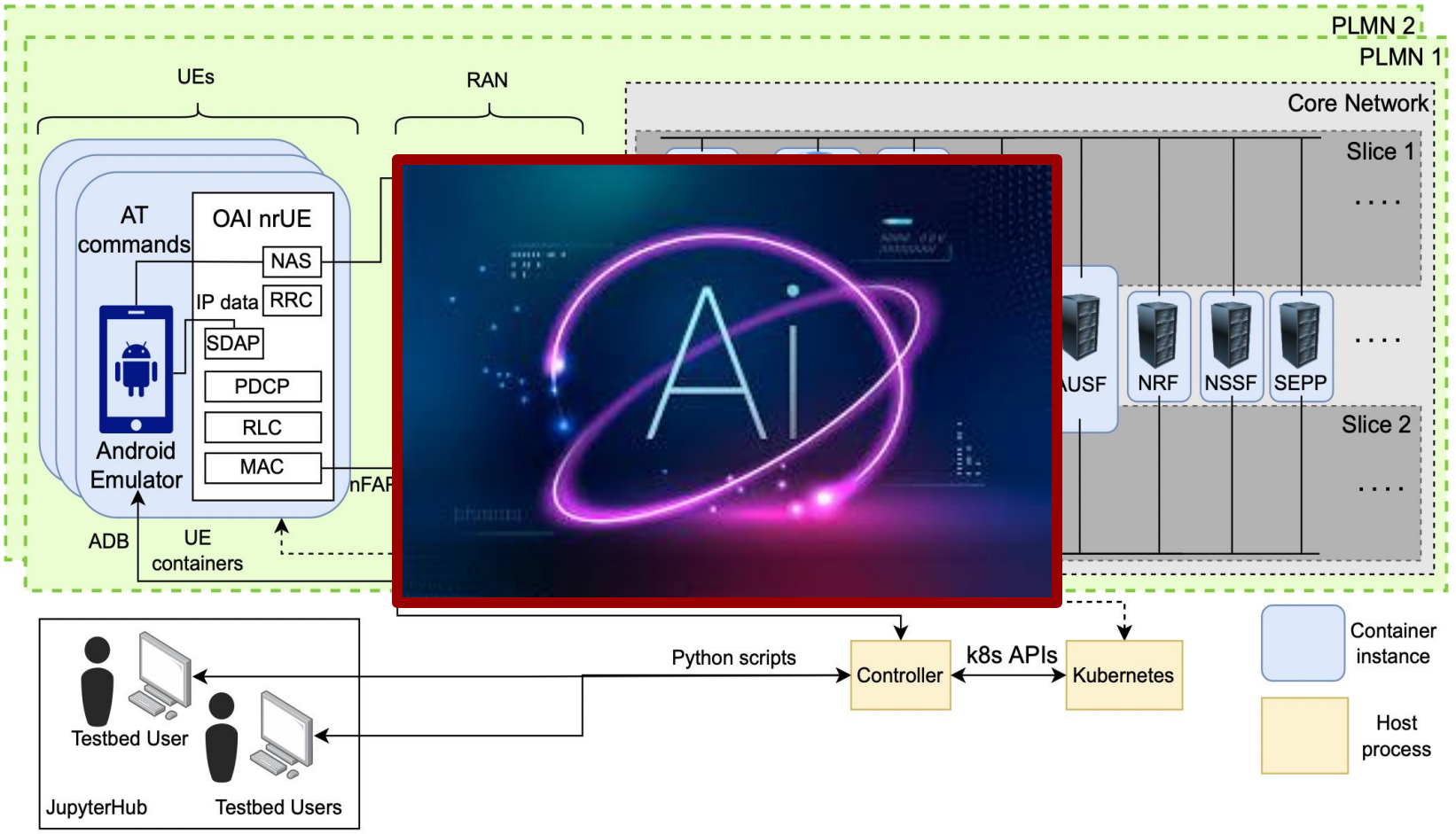
Project 2: Policy Verification



Project 3: Deception for 5G

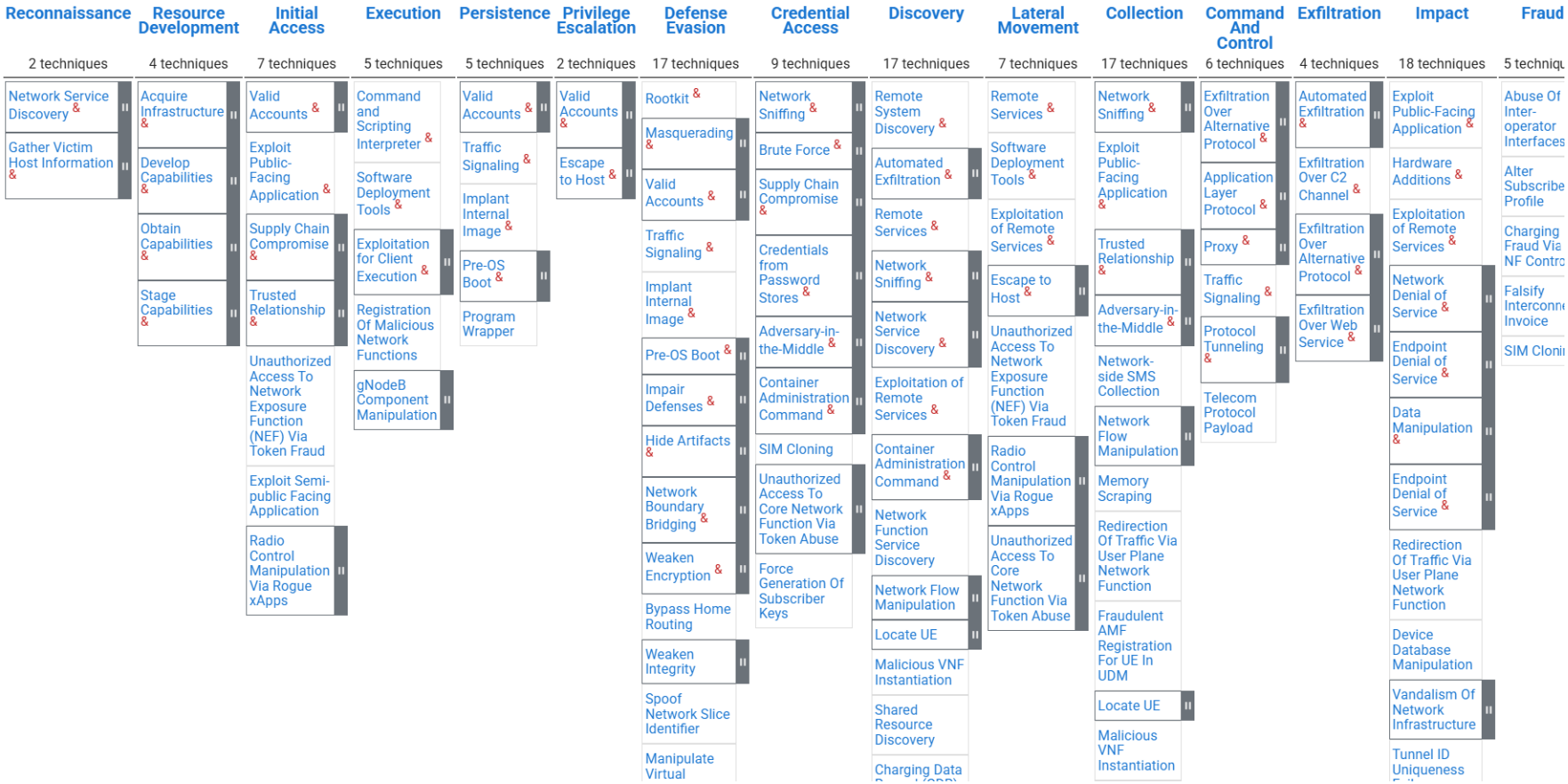


Project 4: AI for 5G



If you are interested in our research,

Particularly, more challenges to CTF5G!



https://fight.mitre.org

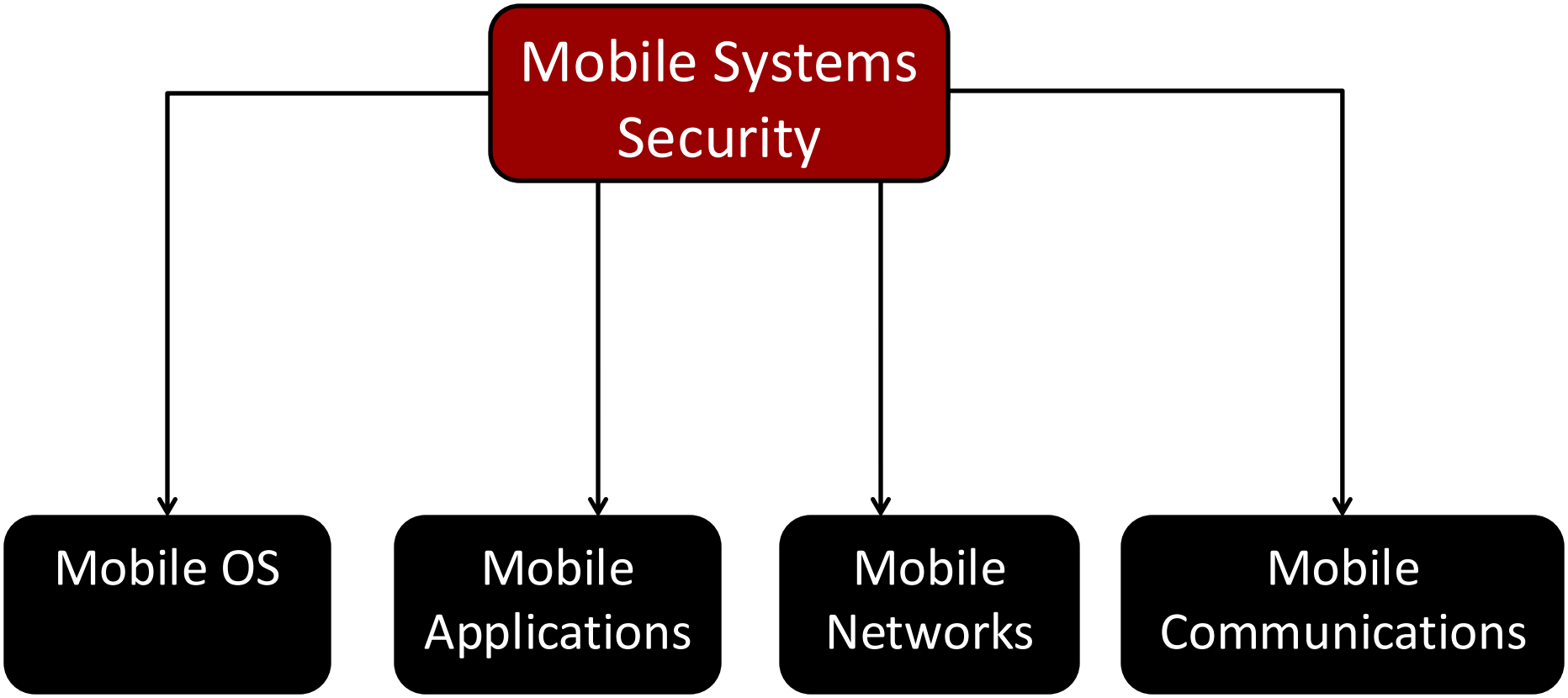
Existing challenges

	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

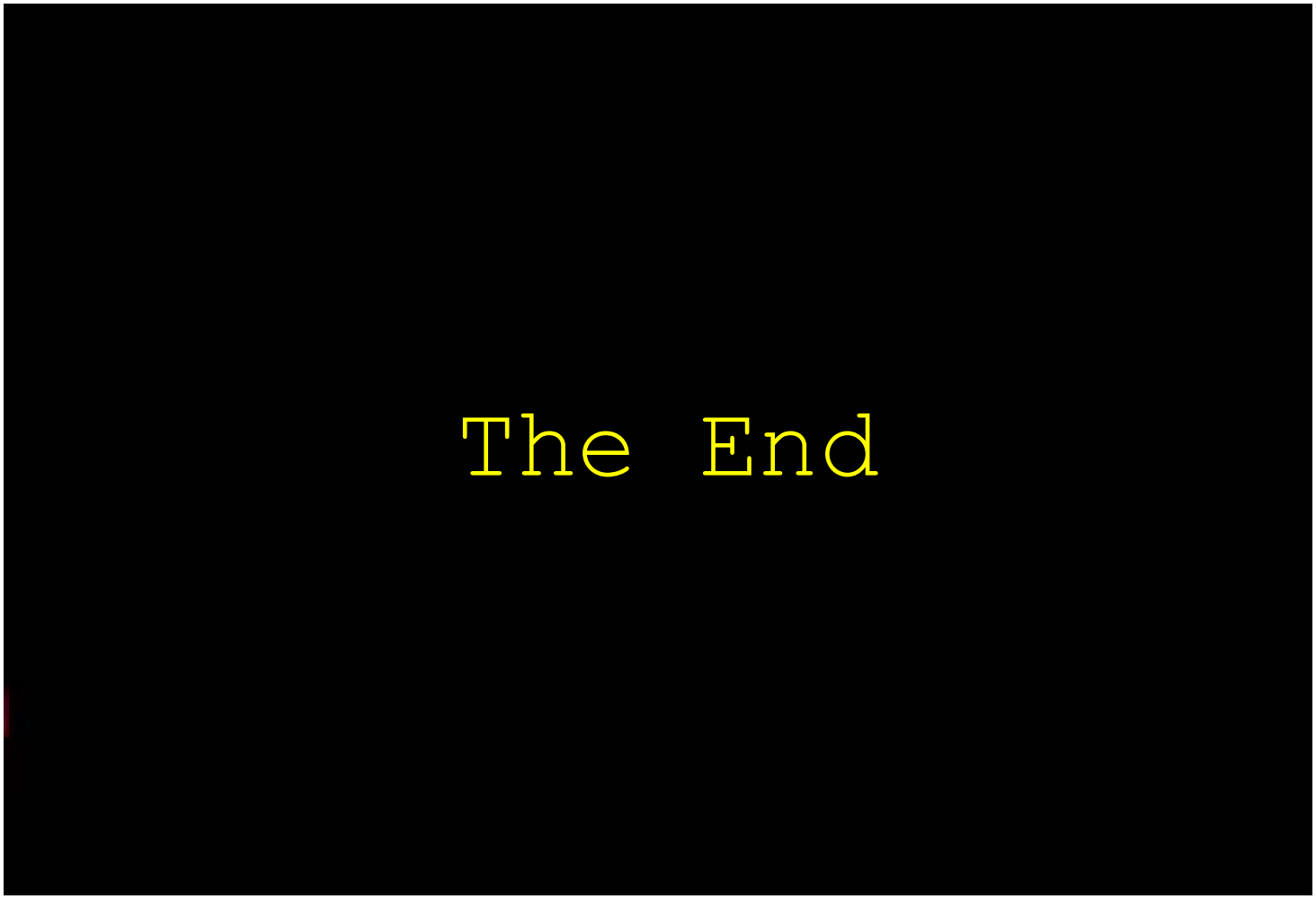
Your name: _____ (mark X in the table for your own presentation)

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