

CTF Workshop

Mustakimur Rahman Khandaker
09/01/2021 @ 4:00 - 5:30 PM



CAPTURE THE FLAG

Institute of Cybersecurity & Privacy

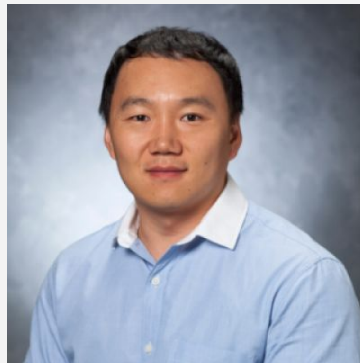
[Team disekt: DARPA's Cyber Grand Challenge](#)



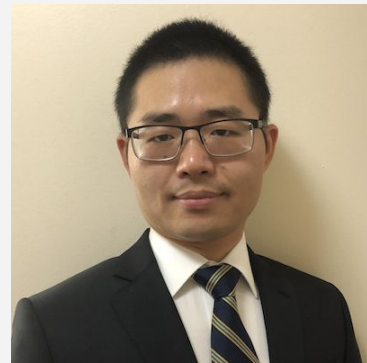
Roberto Perdisci
Director & Professor
Network Security



Kyu Hyung Lee
Associate Director & Associate
Professor
Computer Forensics



Jaewoo Lee
Assistant Professor
Privacy



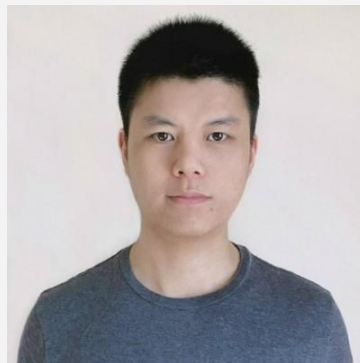
Wenwen Wang
Assistant Professor
System and Software Security



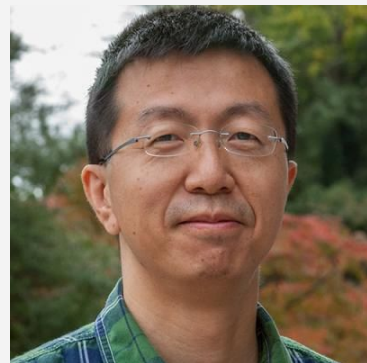
Le Guan
Assistant Professor
System Security



Mustakimur Khandaker
Assistant Professor
System and Software Security



Chenglin Miao
Assistant Professor
IoT Security



Kang Li
Adjunct Professor
System Security

Capture The Flag

Capture the Flag (CTF) is a special kind of information security competitions.

- Players use real hacking tools to break into the system, detect vulnerabilities, and exploit them to capture an encoded string.
 - This string is known as a **flag** i.e. is evidence that a player has discovered the weakness in the systems.

There are three common types of CTFs:

- Jeopardy
- Attack-Defence
- Mixed

Why should you consider playing CTF?

- Learning new skills is one of the most essential things to get ahead in your career.
 - Especially if you are working in a field such as Cybersecurity, where new challenges keep arising on a regular basis.
- Also, it is fun to break systems, develop team spirit, and boost your confidence.
- But, foremost, secure a well-paid job in information security.

Types of CTFs

Jeopardy:

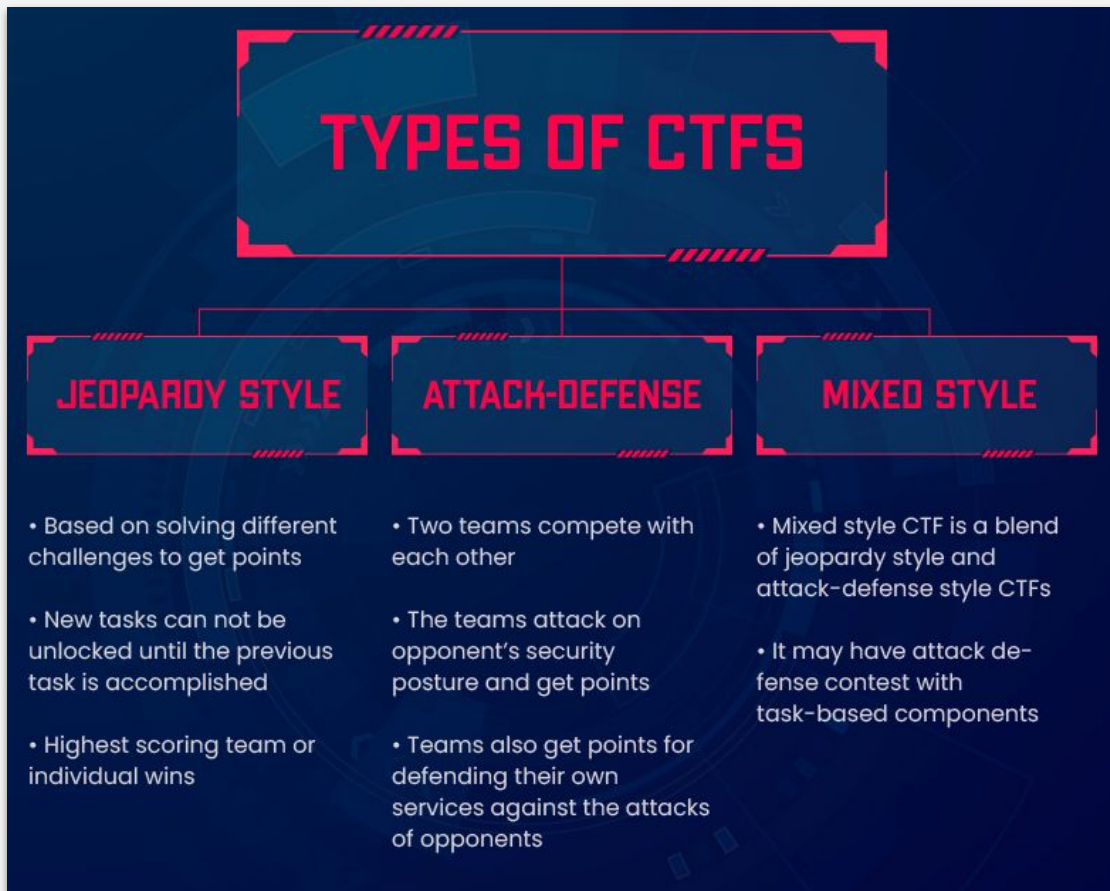
- Cryptography.
- Binary Exploitation.
- Web Exploitation.
- Forensics.
- Reverse Engineering.
- Pwn.
- Packet Analysis.
- Miscellaneous.

Attack-Defense (wargame):

- Finding out vulnerabilities.
 - Generate exploit.
 - Patch the vulnerabilities.

Mixed:

- Wargame with special time for task-based elements.



Online Resources

Jeopardy Practice:

- [Pwnable.kr](https://pwnable.kr)
- [OtterCTF](https://otterctf.com)
- pwnable.tw
- [OOO archive](https://ooo.ctf) | [DEF CON CTF](https://defconctf.com)
- [Reversing.Kr](https://reversing.kr)
- [picoCTF](https://picoctf.com)
- [The Cryptopals Crypto Challenges](https://thecryptopals.com)
- [pwn.college!](https://pwn.college)
- [PortSwiggerportswigger.net](https://portswigger.net)
- [CTFlearn](https://ctflearn.com)
- [Google CTF](https://google.ctf)

Attack-defense Practice:

- <https://ctf365.com/>
- <http://smashthestack.org/>
- <https://legitbs.net/>

Check for upcoming CTF competition:

- <https://ctftime.org/>

CTF Events						
All Upcoming Archive Format Location Restrictions 2021						
Name	Date	Format	Location	Weight	Notes	
DEF CON CTF Qualifier 2021	01 May, 00:00 UTC — 03 May 2021, 00:00 UTC	Jeopardy	On-line	80.92	136 teams will participate	
ImaginaryCTF	01 May, 16:00 UTC — 31 May 2021, 16:00 UTC	Jeopardy	On-line	0	8 teams will participate	
DawgCTF 2021	07 May, 22:00 UTC — 08 May 2021, 22:00 UTC	Jeopardy	On-line	23.29	10 teams will participate	
San Diego CTF 2021	08 May, 00:00 UTC — 10 May 2021, 00:00 UTC	Jeopardy	On-line	0.00	15 teams will participate	
PwnTillDawn Online Battlefield - Goodwill Edition 2021	08 May, 05:00 UTC — 09 May 2021, 05:00 UTC	Hack quest	On-line	0.00	2 teams will participate	
saarCTF 2021	08 May, 13:00 UTC — 08 May 2021, 22:00 UTC	Attack-Defense	On-line	24.42	19 teams will participate	
m0leCon CTF 2021 Teaser	14 May, 17:00 UTC — 15 May 2021, 17:00 UTC	Jeopardy	On-line	24.55	9 teams will participate	
FarEastCTF - 2021	15 May, 10:30 UTC — 15 May 2021, 18:00 UTC	Jeopardy	Russia, Khabarovsk	23.40	1 teams will participate	
3kCTF-2021	15 May, 11:00 UTC — 16 May 2021, 17:00 UTC	Jeopardy	On-line	24.14	7 teams will participate	
NorzhCTF 2021	21 May, 18:00 UTC — 23 May 2021, 18:00 UTC	Hack quest	On-line	0.00	4 teams will participate	

Hacking Capture-The-Flag



Workshop Purpose

Introduce students (undergraduate and graduate) to CTF competition.

Regular sessions on problem solving of different categories.

- Starting with ICSP faculty members and gradually transferring the presentation to the experienced students.
- ICSP faculty members will be always there for advising.

Assigning students CTF problems to solve and discuss the problems in next workshop session.

- A website will be maintained to help students on track and observing their progress.
- ICSP will also invite external CTF expertise for specialized talk (e.g. tutoring about their invented tool).

Ultimate goal is to build 2-3 strong teams from the department students.

- ICSP will organize online CTF competition to help students find out their teams.
- ICSP will sponsor top student teams to participate in flagship CTF competitions (e.g. Defcon CTF).

ICSP will invite federal agencies and industries who will be interested to see the activities.

- CTF workshop participants will be able to engage that will benefit them on job hunting.

Fall 2021 Workshop Schedule

Date	Category	Presentation	Exercise
09/01/2021	Intro, Misc	Intro, letter, pdfcrack, recurse	re , Experience
09/08/2021	Bin Exploit	bof, Passcode.	
09/15/2021	Crypto	ocr_is_cool, crypto_60, crypto_70	crypto_file, factored
09/29/2021	Packet Analysis	Birdman's Data, Otter Leak	
10/06/2021	Bin Exploit		
10/20/2021	Web Exploit		
10/27/2021	Rev Eng		
11/03/2021	Forensics		
11/10/2021	Rev Eng		
11/17/2021	Advanced		

Spring 2022 Plan

Invite at least 2 external presenters to give talks.

- Someone experienced with CTF competition and invented tools well-known in the arena.

By mid semester, arrange a local CTF competition for the UGA students.

- It will be a good time to build teams to participate in flagship CTF competition.

Selecting top UGA team/s to sponsor in participating in flagship CTF competition.

- Specially, DefCon 2022 (probably will held on May).

Invite representative from federal agencies and industries to tour our activities and meet with students.

- Hopefully, collaborate with UGA Career Center.

Miscellaneous

Letter [Google CTF 2018]

<https://gctf-2018.appspot.com/#beginners/misc-letter>

LETTER

misc

Garbo-can

You really went dumpster diving? Amazing. After many hours, SUCCESS! Between what looks like a three week old casserole and a copy of "Relative-Time Magazine", you found this important looking letter about the victims PC. However the credentials aren't readable - can you still obtain them?

[Attachment]

CTF(...)

Submit flag

Fake Name
Fake Address
Fake City

A couple of days ago

IOT Credentials

Dear Customer,

Thanks for buying our super special awesome product, the Foobarnizer 9000!
Your credentials to the web interface are:

- Username: [REDACTED]
- Password: [REDACTED]

Note: For security reasons we cannot change your password. Please store them safely.

PDFuck! [OtterCTF]

<https://otterctf.com/challenges#PDFuck!>

Challenge 48 Solves X

PDFuck!
300

I found some interesting PDF and file on my otter PC. take a look and see if you can get the secret message.

zip password: otter

Unlock Hint for 150 points

PDFuck.txt history.zip

Flag Submit

A Book containing 485 pages

The Philosophy of History Georg Wilhelm Friedrich Hegel

With Prefaces by Charles Hegel
and the Translator, J. Sibree, M.A.

*"The History of the World is not intelligible apart from a
Government of the World." — W. V. Humboldt*

451, 896
2, 1302
208, 45
426, 943
377, 503
133, 44
268, 1994
462, 1442
448, 2425
190, 1129
334, 471
455, 1473
407, 271
203, 98
307, 465
126, 258
188, 1341
132, 1593
258, 44
473, 1951
404, 2184
447, 1416
186, 1591
15, 1758
340, 1512
231, 1965
168, 1769
137, 819
244, 711
33, 43
335, 2264

ReCurse [OtterCTF]

<https://otterctf.com/challenges#ReCurse>

Challenge

134 Solves


X

ReCurse
150

Found this nested zip in Morty's PC. what is it that he is hiding?

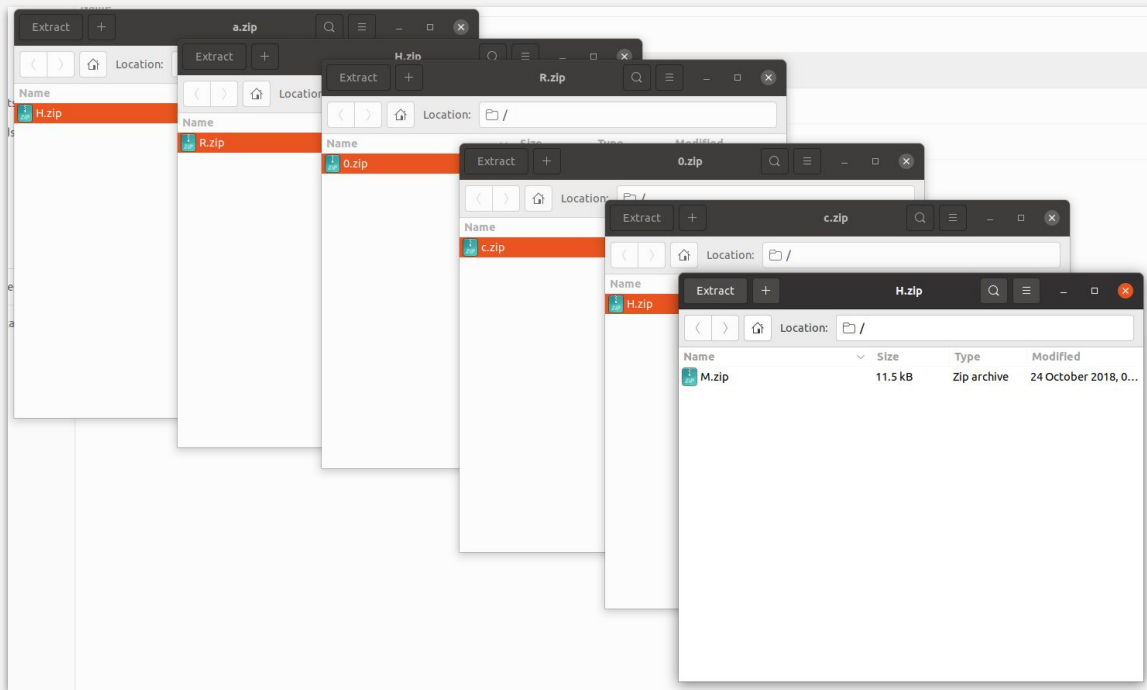
Unlock Hint for 30 points

Unlock Hint for 50 points

 a.zip

Flag

Submit



Exercise

<http://ctf.cs.uga.edu:8000/challenges>

UGA-ICSP-CTF

[Users](#)

[Scoreboard](#)

[Challenges](#)

[Admin Panel](#)

[Notifications](#)

[Profile](#)

[Settings](#)



Challenges

Misc

re|lllll

5

Experience

10

Slides:

<https://www.mustakim.info/teaching/ctf-workshop-2021/session-1-introduction-miscellaneous/>

Slack Workspace:

https://join.slack.com/t/slack-jsh6294/shared_invite/zt-v611vt1v-p0pdAF2WDOu5PwmsenZPbA

See you on 09/08/2021
@ 4:00 – 5:30 PM
@ Boyd – 201

