COMP3633 Competitive Programming in Cybersecurity II

Syllabus (2023 Spring)

Course Description

This is the second course out of a series of three special courses that aim to prepare interested students in joining the various cybersecurity competitions. The topics discussed will be practical and related to the cybersecurity competitions.

Prerequisite(s):

COMP2633 and instructor consent

Exclusion(s):

COMP4633

Course Intended Learning Outcomes (CILOs):

Upon completion of the course, students are expected to be able to:

	Course Intended Learning Outcome (CILO)
1	Be able to apply and understand ethical hacking.
2	Be able to analyze various computer systems rigorously and identify potential security flaws in the systems.
3	Be able to understand the current trends in the development of cybersecurity protection measures in the industry.
4	Be able to acquire leadership through team-working in taking part in the cybersecurity contests.
5	Be able to educate less experienced students regarding cybersecurity and provide the leadership in sharing and deepening the understanding of cybersecurity issues among the student community.

Assessments:

A+ to F

Assessment Method	Description	Weighting	CILOs to be addressed
Presentation		50%	1,2,3,4,5
Course participation		15%	1,2,3
International CTF competition participation		35%	4

List of Presentation Topics (subject to change from semester to semester):

Pwn	**Crypto**	**Reverse**	**Web**	**Misc**
Ret2dl_resolve	Lattice-based attack for RSA	RE Automation	NAT slipstream	Cryptocurrency Security
FSOP	Bleichenbacher & Manger attacks	Self written RE tools / project / plugins	Request smuggling	Windows Active Directory / Azure AD Attack
House of Force	Common attack vectors for Elliptic curve cryptology	Reversing a specific modern language (e.g. compiled language features of Rust / Go / Kotlin in JVM / Swift / various mobile frameworks etc)	JavaScript prototype pollution	Memory Forensics / How to find interesting info from memory?
Unsortbin attack + Global_max_fast Hijacking	Study of one major postquantum cryptography type: code-based, lattice-based, hash-	Packing and Unpacking binaries	NoSQL Injections	Container and Cloud Security (e.g. docker / kubernetes internals, AWS / Azure security)

	based, multivariate			
Introduction to Kernel exploitation	Study of implementation flaws of major crypto libraries	Advanced Angr	DNS Rebinding	Advanced OSINT / Threat Intelligence Technique
Sandbox escape		APT malware reverse engineering (eg compiler-level obfuscations) (Links to an external site.)	OAuth	Hardware side channels (Rowhammer, CPU side channels, cache attacks etc)
Windows Pwn			GraphQL	Any techniques / knowledge that you found interesting from MITRE ATT&CK table
House of orange (challenger level)			Java deserialization	Discussion of recent cybersecurity incidents - technical side
			Expression Language Injection	Introduction to fuzzing (eg AFL, honggfuzz, libfuzzer,etc)
			UXSS (should be in pwn?)	Summary of any Brandon Falk 's live streaming gamozolabs
				CodeQL tutorial
				Walkthrough of any Nday exploit chain being used in the wild