CS 495 Reverse Software Engineering

Time: Fri. 2:00 – 5:00 PM

Venue: Visual Art Building 1033, the Center for Cybersecurity Education and Research

Instructor: Cong Wang

https://www.lions.odu.edu/~c1wang/

Course Description:

The object of Software Reverse Engineering is to provide students with the understanding and practice to perform analysis on malware, deduce their and determine how malware works, and to aid the analysis via disassembly. Students will be able to use tools (IDAPro, Ollydbg) to safely perform static and dynamic analysis of malware, including encoded, packed, obfuscated ones. In particular, the course will have extensive hands-on labs/assignments on each knowledge unit.

Goals:

- Understand the mechanisms of malicious programs such as virus, worms, trojans, backdoors and rootkits
- Use reverse software engineering tools and methodologies to explore executable machine code
- Understand vulnerabilities that malware can exploit to compromise system
- Learn techniques to identify malware and how they evade detection
- Learn countermeasures that detect malware and understand the tricks malware can do to disable such countermeasures
- Understand ethical responsibilities and obligations associated with developing, acquiring and operating software system

Core Knowledge Units of the Course:

- Static Analysis of Binaries, Disassemblers (IDAPro)
- Dynamic Analysis (OllyDbg)
- Virtualization-based sandbox environments (VMware)
- Process and file activity monitors (ProcMon)
- Network activity monitors (Wireshark, tcpdump)

Gradings:

Attendance & In class homework	30%
Homeworks	40%
Final project	30%

Tentative Course timeline:

Week #	Topics Covered
Week 1 Sept. 1	Introduction Motivation Chapter 1. Basic Static Techniques
Week 2 Sept. 8	Chapter 2: Malware Analysis in VMs Chapter 3: Basic Dynamic Analysis
Week 3 Sept. 15	Advanced Static Analysis Chapter 4: x86 Assembly Chapter 5: IDA Pro
Week 4 Sept. 22	Chapter 6: C code in Assembly Chapter 7: Malicious Windows Programs
Week 5 Sept. 29	Advanced Dynamic analysis Chapter 8: Debugging Chapter 9: OllyDbg
Week 6 Oct. 6	Chapter 11: Malware Behavior
Week 7 Oct. 13	Chapter 12: Covert Launching Chapter 13: Data Encoding

Week 8 Oct. 20	Chapter 14: Network Signatures Chapter 15: Anti-Disassembly
Week 9 Oct. 27	Chapter 16: Anti-Debugging Chapter 17: Anti-VM Techniques
Week 10 Nov. 3	Chapter 18: Packers and Unpacking Chapter 19: Shellcode Analysis
Week 11 Nov. 10	Chapter 20: C++ Analysis Chapter 21: 64-bit Malware
Week 12 Nov. 17	Networking Attacks Network Traffic Analysis
Week 13 Dec. 1	Anomaly Detection Analysis
Week 14 Dec. 8	Adv. Static Analysis: Machine Learning/Deep Learning

Textbook:

Practical Malware Analysis – Michael Sikorski et. al.

Supplemental Textbooks:

Reversing Secrets of Reverse Engineering, Eldad Eilam et. al.

The IDAPro Book, Chris Eagle

Practical Reverse Engineering, Bruce Dang et.al