ECE 5567.02 (Approved): Reverse Engineering and Malware Analysis

Course Description

This course will give students an overview of cutting edge reverse engineering techniques as well as software
security and defense practices. Programming experience in C required.

Transcript Abbreviation: ReverseEng
Grading Plan: Letter Grade
Course Deliveries: Classroom, 100% at a distance
Course Levels: Undergrad, Graduate
Student Ranks: Junior, Senior, Masters, Doctoral, Professional
Course Offerings: Spring
Flex Scheduled Course: Never
Course Frequency: Every Year
Course Length: 14 Week
Credits: 3.0
Repeatable: No
Time Distribution: 2.0 hr Lec, 2.0 hr Lab
Expected out-of-class hours per week: 5.0
Graded Component: Lecture
Credit by Examination: No
Admission Condition: No
Off Campus: Sometimes
Campus Locations: Columbus
Prerequisites and Co-requisites: Prereq: CSE 2431, 5431 or graduate standing. Prereq or concur: ECE 5561 or CSE 5471.
Exclusions: Not open to students with credit for CSE 5477.02
Cross-Listings: Cross-listed with CSE 5477.02

Course Rationale: Provide students an opportunity to understand malware and techniques to analysis them.

The course is required for this unit's degrees, majors, and/or minors: No
The course is a GEC: No
The course is an elective (for this or other units) or is a service course for other units: Yes

Subject/CIP Code: 14.0101
Subsidy Level: Doctoral Course

Programs

Abbreviation	Description
CpE	Computer Engineering
EE	Electrical Engineering

Course Goals

Master Reverse Engineering tools and techniques
Be familiar with taxonomy of malware
Be competent in common reverse engineering techniques
Be competent in common anti-reverse engineering techniques such as obfuscation

Be exposed to advance techniques like machine learning (ML) security and artifact intelligence (AI) assisted reverse engineering

Course Topics

Topic	Lec	Rec	Lab	Cli	IS	Sem	FE	Wor
Reverse engineering tools (e.g., disassemblers, decompilers, debugging, emulation, virtual machine monitor)	1.0		2.0					
Taxonomy of malware	3.0							
Static analysis techniques: control-flow analysis and data-dependency analysis	2.0		1.0					
Static analysis techniques: value-set analysis and backward slicing	2.0		1.0					
Dynamic analysis techniques: tainting	2.0		1.0					
Dynamic analysis techniques: fuzzing	2.0		1.0					
Dynamic analysis techniques: symbolic execution and concolic execution	2.0		1.0					
Introduction to anti-static analysis techniques (e.g., obfuscation, shell, polymorphic)	4.0		2.0					
Introduction to anti-dynamic analysis techniques (e.g., anti-debugger, detecting virtual machines, detecting analysis tools)	4.0		2.0					
Advance topics: Machine Learning security	3.0							
Advance topics: Video Game Security	3.0							
Advance topics: AI for malware analysis (e.g., classification)	3.0							

Representative Assignments

Intro to Reverse Engineering lab (get familiar with tools such as gdb, ollydbg, angr.)
Static analysis lab
Dynamic analysis lab
Anti-reverse engineering lab

Grades

Aspect	Percent
Lab	40%
Course projects	20%
Final exam	20%
Midterm exam	15%
Class participation	5%

ABET-EAC Criterion 3 Outcomes

Course Contribution		College Outcome
*	a	An ability to apply knowledge of mathematics, science, and engineering.
***	b	An ability to design and conduct experiments, as well as to analyze and interpret data.
***	c	An ability to design a system, component, or process to meet desired needs.
	d	An ability to function on multi-disciplinary teams.
**	e	An ability to identify, formulate, and solve engineering problems.

Course Contribution		College Outcome
*	f	An understanding of professional and ethical responsibility.
**	g	An ability to communicate effectively.
*	h	The broad education necessary to understand the impact of engineering solutions in a global and societal context.
**	i	A recognition of the need for, and an ability to engage in life-long learning.
*	j	A knowledge of contemporary issues.
***	k	An ability to use the techniques, skills, and modern engineering tools necessary for engineering practice.

CpE ABET-EAC Criterion 9 Program Criteria Outcomes

Course Contribution		Program Outcome
***	1	an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
**	2	an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
*	3	an ability to communicate effectively with a range of audiences
**	4	an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
**	5	an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives
***	6	an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
***	7	an ability to acquire and apply new knowledge as needed, using appropriate learning strategies

EE ABET-EAC Criterion 9 Program Criteria Outcomes

Course Contribution		Program Outcome
***	1	an ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics
**	2	an ability to apply engineering design to produce solutions that meet specified needs with consideration of public health, safety, and welfare, as well as global, cultural, social, environmental, and economic factors
*	3	an ability to communicate effectively with a range of audiences
**	4	an ability to recognize ethical and professional responsibilities in engineering situations and make informed judgments, which must consider the impact of engineering solutions in global, economic, environmental, and societal contexts
**	5	an ability to function effectively on a team whose members together provide leadership, create a collaborative and inclusive environment, establish goals, plan tasks, and meet objectives
***	6	an ability to develop and conduct appropriate experimentation, analyze and interpret data, and use engineering judgment to draw conclusions
***	7	an ability to acquire and apply new knowledge as needed, using appropriate learning strategies

Additional Notes or Comments

changed title and added crosslisting with CSE 11/11/2020 BLA

Streamlined with CSE Content EE

```
Added CSE 5477.02 as exclusion
```

Prepared by: Eylem Ekici