Master Course Description for EE-468 (ABET sheet)

Title: Software and Embedded Systems Security
Credits: 4
Coordinator: Radha Poovendran, Professor, Electrical and Computer Engineering

Goal: This course in general is about exploiting the basic building blocks of security bugs—assembler, source code, the stack, the heap, and so on and help the students to explore, and understand the systems they are running and how to better protect them. This course covers the critical topic of discovering, exploiting, and preventing system security flaws by integrating and applying the techniques and methodologies; also discusses the strengths and weaknesses of these techniques and methodologies, and when each should be used. In particular, the course will teach binary reverse engineering, vulnerability analysis, exploit development, patching vulnerabilities, bug hunting, etc. through ten-weeks of hands-on labs with examples. During this course students will learn how to use GDB debugger which demonstrates what is going in a program while it executes or what another program was doing at the moment it crashed.

Learning Objectives: At the end of this course, students will be able to:

1. Using GDB debugger to analyze binary codes
2. Writing shell codes and exploit the vulnerabilities in the shell environment
3. Investigating the basic building blocks of security bugs—assembler, source code, the stack, the heap
4. How to exploit the vulnerabilities of system using binary codes and analyzing defenses proposed to address these vulnerabilities
5. Plan and execute a cyber penetration test, and utilize various vulnerability vectors that can be used to achieve an attacker’s goals.

Prerequisites:

- either E E 241, or CSE 163

Recommended Preparation:

- E E 469, E E 472

Textbooks:

1. Chris Anley et al., The Shellcoder's Handbook: Discovering and Exploiting Security Holes, 2nd Edition 2nd Edition

References:

1. Wenliang Du, Computer & Internet Security: A Hands-on Approach, Second Edition
2. Peter Kim, *The Hacker Playbook 3: Practical Guide to Penetration Testing*, McGraw-Hill, 2018.
3. Matt Monte, *Network Attacks and Exploitation: A Framework* (1st edition), 2015.

Topics:

1. Intro to reverse engineering (e.g., Binary analysis, Exploit writing, Patching vulnerabilities) *[Week 1]*
2. Environment variable and attack *[Week 2]*
3. Writing shellcode, shellcode tricks, shellshock attack *[Week 3]*
4. Frame-pointer attack and buffer overflow attack *[Week 4]*
5. Return to libc and ROP attack *[Week 5]*
6. Format string vulnerability *[Week 6]*
7. ShadowStack, CFI, and other defenses *[Week 7]*
8. Meltdown attack and Spectre attack *[Week 8]*
9. Hardware Trojans and techniques for hardware Trojan threat mitigation *[Week 9]*

Grading: 20% Homework, 40% projects, 10% midterm, 20% final exam, 5% in-class activity, 5% completion of evaluation forms.

Religious Accommodation Policy "Washington state law requires that UW develop a policy for accommodation of student absences or significant hardship due to reasons of faith or conscience, or for organized religious activities. The UW's policy, including more information about how to request an accommodation, is available at Religious Accommodations Policy (https://registrar.washington.edu/staffandfaculty/religious-accommodations-policy/). Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form (https://registrar.washington.edu/students/religious-accommodations-request/)."

ABET Student Outcome Coverage: This course addresses the following outcomes:

H = high relevance, M = medium relevance, L = low relevance to course.

(1) *An ability to identify, formulate, and solve complex engineering problems by applying principles of engineering, science, and mathematics.* **(H)** The course uses binary debugger tools e.g. GDB. Students must implement the security attacks and defenses. Engineering judgment is developed through understanding the vulnerability of systems security defenses. Throughout the course we emphasize the need to learn how to write customized tools to protect your systems, not just how to use ready-made ones. Towards this direction, security defenses designed to address the flaws are discussed. Assignments require students to analyze other defenses with weaknesses. The homework involves solving engineering problems identified by the assignments and exemplified by class discussion. The students develop the state-of-the-art system security attacks and their defenses.

(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.* **(M)** The project challenges the students to develop, design and implement different system security attacks.

(3) *An ability to communicate effectively with a range of audiences.* **(M)** Students are required to write up their simulations in an engineering format. The ability to communicate effectively in writing is a portion of the grade received on homework and projects. Students are required to give a short presentation on their projects defined on system security attacks and defenses.

(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.* **(H)** The course covers system security vulnerabilities and their defense implications, enabling the students to recognize the vulnerabilities of softwares and systems. Impact of good system security and the need to learn how to write customized tools to protect your systems is emphasized. We discuss the impact of design of insecure systems and the way they can be exploited. Focus here will be to show how to design systems that are resilient to common security threats such as buffer overflow attacks.

(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.* **(H)** The course project is conducted in teams of up to three to four members and constitutes 15% of their grade.

(7) *An ability to acquire and apply new knowledge as needed, using appropriate learning strategies.* **(H)** The course emphasizes the need for evolving current secure system designs as new threats emerge and security assumptions are weakened.

Further, pointers to security websites and articles are provided in order to enhance personal knowledge in this developing area.