Master Course Description for EE-465 (ABET sheet)

Title: Network and web security
Credits: 4
Coordinator: Radha Poovendran, Professor, Electrical and Computer Engineering

Goals: To develop an understanding of the fundamental principles of network and communication security. This course is an introduction to the basic theory and practice of network security. This course will serve as an introduction to the vulnerabilities and defenses in network and communication systems. We will introduce state-of-the-art network and web security attacks along with hand-on activities to provide better understanding of the security vulnerabilities. The objective of this course is to enable students to understand the main challenges in designing security mechanisms and protocols for thwarting attacks on existing and emerging computer networks including network's communication protocols, domain name systems, wireless networks, web security.

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

1. *Study, implement and analyze* some fundamental protocol security attacks and defenses including TCP session attack, man-in-the-middle, heartbleed bug and attack
2. *Study, implement and analyze* representative fundamental web security attacks and defenses including DNS spoofing, denial of service
3. *Study, implement and analyze* some fundamental domain name attacks and defenses including site request forgery, site scripting attacks and SQL injection
4. *Study, and analyze* some of fundamental wireless security protocols and security vulnerabilities and defenses

Textbooks:

1. Wenliang Du, Computer & Internet Security: A Hands-on Approach, Second Edition

References:

1. Mike Speciner et al., Network Security: Private Communications in a Public World 2nd Edition, (also available in Kindle format)
2.

Prerequisites:

- either CSE 163, or E E 241; E E 418

Recommended Preparation:

- EE EE 419 Introduction to Computer-Communication Networks

Topics:

Network Security [Week 1-4]:

1. Network background and attacks on TCP, DNS, DHCP, Packet sniffing and spoofing attack *[week 1]*
2. *SYN flooding attack [week 2]*
3. *TCP Session Hijack attack [week 2]*
4. Intro to network's attacks' types (Phishing, Botnet, DoS (Denial of Service), Routing Hijacking, HoneyNets, Privilege Escalation, Man-in-the-middle, etc), Network Mapping tools, Vulnerability Scanners *[week 3]*
5. Malice-in-the-middle attack *[week 3]*
6. Heartblead bug and Attack *[week 4]*
7. Blended Attacks *[week 4]*

DNS [Week 5-6]:

1. Review of DNS (DNS Domain Hierarchical, Zone,query process, etc) *[week 5]*
2. DNS Spoofing and defense *[week 5-6]*
3. DNS Rebinding Attack and Defense *[week 6]*

Web security in practice [Week 7-8]:

1. Firewalls and Firewall Rules, Virtual Private Network (VPN, TLS/SSL), how to setup VPN to bypass firewalls *[week 7]*
2. Cross-site request forgery *[week 7]*
3. Cross-site scripting attacks *[week 8]*
4. SQL injection attack *[week 8]*

Wireless network security [Week 9]:

1. System security in wireless network (Trusted platforms, Trust principles, technologies and methodologies for trusted platforms, trusted platform in practice (TPM))
2. Physical layer security (Shannon's Perfect secrecy, Wyner's wiretap channel, Wiretap code for achievable Secrecy using linear codes)

Grading: 35% Homework, 20% midterm, 15% Project, 25% final exam, 5% in-class quiz participation activity.

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 networks tools. Students must implement the security attacks and defenses. Engineering judgment is developed through understanding the vulnerability of network protocols and advantages of security defenses. Throughout the course we emphasize the need to use sound design principles instead of relying on ad-hoc heuristics only. Towards this direction, network security protocols with design flaws are discussed. Assignments require students to analyze other network protocols with weaknesses. The homework involves solving engineering problems identified by the assignments and exemplified by class discussion. The exams and projects challenge the students to identify other network security issues and their solutions.

(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 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 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 security vulnerabilities in systems and their defense implications, enabling the students to analyze and identify the vulnerabilities of network protocols. Impact of good network security protocols is emphasized. We discuss the impact of design and implementation of insecure protocols and the way they can be exploited.

Case studies of designing protocols that are resilient to common security threats such as man-in-the-middle and denial of service attacks will be discussed.

(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 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 will be provided in order to enhance knowledge in this emerging area.