Network and Communication Security

DRAFT SYLLABUS

Course Goals

This course is an introduction to the theory and practice of network and communication security and will cover the vulnerabilities and defenses in network and communication systems. It 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 the fundamental wireless security protocols and security vulnerabilities and defenses.

Textbooks

Wenliang Du, Computer & Internet Security: A Hands-on Approach, 2nd Edition

References

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

Prerequisites

Proficiency in Python programming. Understanding of the fundamentals of network security and cryptography and computer- communication networks is recommended.

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

Homework: 45% (three at 15% each)

Project: 55%

- Proposal: 5%
- Checkpoint report: 10%
- Final presentation: 15%
- Final report: 25%

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. Accommodations must be requested within the first two weeks of this course using the Religious Accommodations Request form.