Course Description

The class will focus on network security. In order to understand the network security problem, the course will include a review of various forms of network attacks. We will then review basic techniques in applied cryptography, and then secure protocols will be covered including network-layer security and various application-layer secure protocols. We then turn to network-side security management including both passive measures like firewall defense schemes including packet filters and bastion hosts, as well as active intrusion detection and response. Finally, we will cover protocols for protecting privacy and anonymity.

Prerequisites

CS 494 Internetworking Protocols

Course Objectives

On completion of this course students will understand the threats faced by networks and networked applications. They will know how to address each kind of threat at various layers of the TCP/IP protocol stack. Students will have gained hands-on experience with real network protocol attacks and with tools for building secure, resilient protocols that withstand attack. They will be well prepared to follow the latest developments in network security, including from academic sources as well as from the hacker community.

Student Learning Outcomes

1. Explain fundamental notions of information security: Confidentiality, Integrity, and Availability.
2. Program a cryptographic security protocol using authentication and encryption.
3. Analyze tradeoffs between secure network protocols at various network stack layers.
4. Describe the major paradigms in network-based attacks including software exploitation, message spoofing, traffic snooping, denial of service, and common web-based attacks.
5. Explain how firewalls work and how they may be used to improve network security.
6. Demonstrate how a network or bastion host may be monitored in order to improve network security.
7. Explain common pitfalls in the most common approaches for network intrusion detection.

Course Outline

1. Vulnerabilities in classical TCP/IP networks and protocols  (1 week)
2. Basics of applied cryptography  (2 weeks)
3. Protocols for authentication and security  (2 weeks)
4. Firewalls and network perimeter defense (1 week)
5. Network security management and intrusion detection (1 week)
6. Security of core Internet infrastructure (DNS and BGP) (1 week)
7. HTTP and web security (1 week)
8. Privacy and anonymity (1 week)

Course Requirements

There will be two lectures each week and regular reading assignments. Students will be assigned a set of hands-on programming exercises approximately every week, and some amount of class time will be made available for work on programming problems. There will be two exams: a midterm and a final.

Compared to the undergraduate network security course (CS 496), students in the graduate section (CS 596) will perform additional, more in-depth analysis on each set of homework problems. Some homework assignments and both exams will include a few advanced questions for only the graduate section. Additionally, each graduate student will be required to present a recent research paper in class.

Recommended Texts


Method of Evaluation

Letter grades will be determined according to the following formula:

<table>
<thead>
<tr>
<th></th>
<th>496</th>
<th>596</th>
</tr>
</thead>
<tbody>
<tr>
<td>Programming Assignments</td>
<td>50%</td>
<td>40%</td>
</tr>
<tr>
<td>Presentation</td>
<td>n/a</td>
<td>10%</td>
</tr>
<tr>
<td>Weekly Quizzes</td>
<td>25%</td>
<td>25%</td>
</tr>
<tr>
<td>Final Exam</td>
<td>25%</td>
<td>25%</td>
</tr>
</tbody>
</table>

Academic Honesty

All submissions must represent the work of the submitting team or individual. It is permissible to discuss the assignment with other students, but you must develop the solution yourselves. Do not, under any circumstances, copy another person's program and submit it as your own. Writing any material (whether it be code, English text, or other) for use by another or using another's work as your own, in any form (even with their permission), will be considered cheating. Cheating on an assignment or exam, including attempts to subvert the course infrastructure, will result in an **automatic zero grade** for that piece of work, and the initiation of disciplinary action at the University level.

Ethics

Some of the technical material studied in this course might be useful for doing things that violate university regulations, laws, or common standards of ethical behavior. Any such behavior that comes to the instructor's attention will be reported to appropriate authorities. In particular, note that use of university computing resources is governed by the Office of Information Technology's Acceptable Use Policy, which may be found at http://oit.pdx.edu/aup/.
Access and Inclusion for Students with Disabilities

PSU values diversity and inclusion; we are committed to fostering mutual respect and full participation for all students. My goal is to create a learning environment that is equitable, useable, inclusive, and welcoming. If any aspects of instruction or course design result in barriers to your inclusion or learning, please notify me. The Disability Resource Center (DRC) provides reasonable accommodations for students who encounter barriers in the learning environment.

If you have, or think you may have, a disability that may affect your work in this class and feel you need accommodations, contact the Disability Resource Center to schedule an appointment and initiate a conversation about reasonable accommodations. The DRC is located in 116 Smith Memorial Student Union, 503-725-4150, drc@pdx.edu, https://www.pdx.edu/drc.

Reporting Obligations

As an instructor, one of my responsibilities is to help create a safe learning environment for my students and for the campus as a whole. Please be aware that as a faculty member, I have the responsibility to report any instances of sexual harassment, sexual violence and/or other forms of prohibited discrimination. If you would rather share information about sexual harassment, sexual violence or discrimination to a confidential employee who does not have this reporting responsibility, you can find a list of those individuals. For more information about Title IX please complete the required student module Creating a Safe Campus in your D2L.