

≡ Network Security

CSE 571S: Network Security, Fall 2018

Instructor: Ning Zhang, zhang.ning@wustl.edu

Meeting: TuThu 10:00 pm – 11:30 pm

Classroom: Lopata 202

Course Description



This course covers principles and techniques in securing computer networks. Real world examples will be used to illustrate the rationales behind various security designs. There are three main components in the course, preliminary cryptography, network protocol security and network application security. Topics include IPSec, SSL/TLS, HTTPS, network fingerprinting, network malware, anonymous communication, and blockchain. The class project allows students to take a deep dive into a topic of choice in network security.

Textbook



There is no textbook for the class. We will use research papers for some of the topics. However, the following references can be helpful.

- *Network Security: Private Communication in a Public World (2nd Edition)* by Charlie Kaufman, Radia Perlman, and Mike Speciner
- *Computer Security: A Hands-on Approach* by Wenliang Du

≡ Network Security

- *A Graduate Course in Applied Cryptography* by Dan Boneh and Victor Shoup

Grading

There is no exam in this class, evaluation will be based on class participation, lab reports and final projects.

Labs	55% (14 + 14 + 14 + 13)
Projects	40%
Class Participation	5%

Schedule

Slides, Lab Assignments and QA are in the WUSTL backboard system.

Date	Topics	Reading	HW/Lab Assignment
8/28/2018	Course Overview, Security Fundamentals	<u>Reflections on Trusting Trust</u>	
8/30/2018	Network Protocol Attacks – Packet/IP/TCP	<u>A Look Back at “Security Problems in the TCP/IP Protocol Suite”</u> <u>IP spoofing demystified</u>	TCP/IP Attack Lab (1 week)

≡ Network Security

9/11/2018	Block Cipher, Modes of Operations	Kaufman Ch 4	Blockcipher lab (1 weeks)
9/13/2018	Key Exchange, DH	Kaufman Ch 6, 7	
9/18/2018	Assymmetric Crypto	Kaufman Ch 6, 7	
9/20/2018	Hash Functions, MAC	Kaufman Ch 5	MD5 - Collision Lab (1 week)
9/25/2018	Authentication	Kaufman Ch 9	
9/27/2018	PKI, CA	Kaufman Ch 15	
10/2/2018	IPSec	Kaufman Ch 17,18	
10/4/2018	TLS	Kaufman Ch 19	PKI Lab (1 week)
10/9/2018	HTTPS		
10/11/2018	Web Security		
10/16/2018	Fall Break - No class		
10/18/2018	DNS, DDoS		Term Project Topic Selection
10/23/2018	Firewall / Intrusion Detection	Kauffman Ch 23	
10/25/2018	Network Scan and Fingerprinting		
10/30/2018	Project lightning talk		Term Project Status Report
11/1/2018	Blockchain	<u>bitcoin</u>	
11/6/2018	Blockchain Attack and Defense		
11/8/2018	Limitation of Blockchain		

≡ Network Security

11/15/2018	Attack and Defense	
11/20/2018	Limitation of Smart Contract	Term Project Project Status Report
11/22/2018	Thanksgiving Break – No class	
11/27/2018	IoT Security	
11/29/2018	IoT Security	
12/4/2018	IoT Security / Final Project Presentation	
12/6/2018	Final Project Presentation	
12/19/2018	Project Report Due	

Labs

- Lab1 – focus on replay attack, TCP/IP session hijacking, and more
- Lab2 – focus on experiencing frequency attack and cipher mode
- Lab3 – focus on exploring hash function collision
- Lab4 – focus on deploying PKI and how it stops man-in-the-middle attack

Projects

≡ Network Security

pages). The class project can also be improvement on an existing security tool. The development should be source controlled using tools, such as git. Students are expected to spend at least six to eight hours on the class labs and projects every week. Some of the ideas for projects are listed below

- Build an IoT device locator in the Internet using tools from Zmap project
- Automatic vulnerability discovery using protocol specification
- Automatic context recovery of network services in operating system
- Adversarial learning on network systems
- Security Measurement on services on the Internet
- Build a covert channel over the network using various services
- Building physical communication covert channel by misusing IoT devices
- Automatic context recovery of network services in operating system
- Build specialized finger printing mechanisms to for a type of device
- Analyze security of a real world product, it can be cyber-physical systems like car or IoT devices like smart coffee machine.
- **YOUR IDEA**

Ethics



With greater power, comes greater responsibility. In this course, we will be learning about and exploring some vulnerabilities that could be used to attack systems. Students are expected to behave responsibly and ethically. You may not attack any system prior approval of the site owners, and may not use anything you learn in this class to disrupt services or harm others. If you have any doubts about whether or not something you want to do is ethical and legal, you should check with the course instructor.



Network Security