网络安全原理与实践

林峰

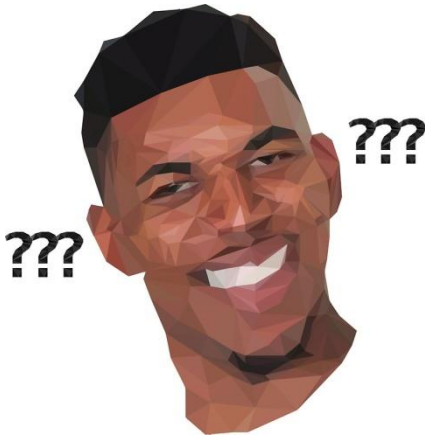
2024年春季学期

Network Security Theory and Practice

Thank You

wish you health & safety

Network Security?



Network ?

Network of computers

Network of computers

share resources

Network of computers

share resources via

communication

Network of computers

share resources via

communication

(data transmission)

Network of computers

communication:

wired

wireless

what channel?

Network of computers

communication:

single-hop

multi-hop

how far?

Network of computers

communication:

single-path

multi-path

how many routes?

Network of computers

communication:

unicast

multicast

broadcast

who to reach?

Network of computers

communication:

data transmission

what data?

Network of computers

communication:

services

what data?

Network of computers

communication:

services

search

Network of computers

communication:

services

streaming

Network of computers

communication:

services

messaging

Network of computers

communication:

services

email

Network of computers

communication:

services

storage

Network of computers

communication:

services

payment


WARNING

Network of computers

communication:

services

messaging



what if overheard?

Network of computers

communication:

services

storage

what if leaked?

Network of computers

communication:

services

payment

what if stolen?

Network Security

protect

communication

Network Security

protect

communication:

confidentiality

integrity

availability

The CIA Triad

Network Security

Theory and Practice?

Network Security
Theory

Reference

- Courses

Course	Instructor	University
Computer and Network Security	R. Rivest Y. Kalai	MIT
Network Security	V. Sekar	CMU
Computer Systems Security	N. Zeldovich	MIT
Computer Security	R. A. Popa	UC Berkeley

- Book

  Security Engineering, Ross Anderson

Agenda

- Secure Routing
- DDoS
- Anonymous Communication
- Web Security
- Traffic Analysis
- PKI/Email Security
- Traceback
- Network Protection

welcome to explore network security together

Website

http://list.zju.edu.cn/kaibu/netsec2022/

Network Security Theory and Practice

College of Computer Science and Technology, Zhejiang University, Spring 2022
Monday 15:55 – 17:30, Tuesday 15:55 – 17:30, Room CW-104
Tuesday 14:05 – 15:40, Room CW-503

Wish You Health and Safety

Instructor

Kai Bu Email: kaibu@zju.edu.cn
Office: Room 503 Zetong Building. Office hour: By appointment

Thank you for studying Network Security with me.

Teaching Assistant

Jiongrui Huang Email: jiongrui_huang@zju.edu.cn
Office: Room 503 Zetong Building. Office hour: By appointment

Course Objective

This course aims to help students understand and practice network attack and defense strategies. As the saying from security research community goes, if you want to secure a system, hack it first. Such a principle drives the development of course content. Each defense strategy is well motivated by example attacks that might take place if it were not enforced. Topics to be covered include DDoS, secure routing, anonymous communication, Web security, Email security, intrusion detection, traceback, and various commonly adopted network protection strategies. Well-crafted lab tasks are also required to help students practice these security techniques. Through integrating both theory and practice, students are expected to grasp the essence of network security as well as train their security mindset.

Prerequisites

Networking, Security, Programming

network security

exciting yet challenging

exciting yet challenging
for me as well…

Instructor

Feng Lin 林峰

百人计划研究员，博导

Ph.D. from Tennessee Tech U, 2015

Research Interests: IoT security, network security (wire/wireless), AI security

research interns wanted

https://flin.group

Teaching Components

- Lecture
- Lab or Project
- Assignment & Exam

Tentative Schedule

Week	Dates	Topics
Week 01	2024.02.27/2024.02.29	Lecture 01-1: Course Introduction Lecture 01-2: Secure Routing
Week 02	2024.03.05/2024.03.07	Lecture 02: DDoS
Week 03	2024.03.12/2024.03.14	Lecture 03: Anonymous Communication
Week 04	2024.03.19/2024.03.21	Lecture 04: Web Security
Week 05	2024.03.26/2024.03.28	Lecture 05: Traffic Analysis
Week 06	2024.04.02/2024.04.04	Lecture 06: PKI/Email Security
Week 07	2024.04.09/2024.04.11	Lecture 07: Traceback
Week 08	2024.04.16/2024.04.18	Lecture 08-1: Network Protection Lecture 08-2: Course Overview

Final Exam: April 20, 2024

Network Security
Practice

Lab

- 3 lab assignments with tutorials
- Practice oriented
- E.g., port scanning, spoofing attack

Lab

- Lab 01: Penetration Testing
- Lab 02: Spoofing Attack
- Lab 03: Web Security

Project

- One semester-long project
- Individual or Group of 2
- Research oriented

Practice & Goal

- **Proposal**
  reading, thinking, creating
- **Prototype**
  coding, design, development
- **Presentation**
  speaking, communication skills
- **Report**
  academic writing, communication skills

Requirement

https://list.zju.edu.cn/kaibu/netsec2022/project.html

Network Security Theory and Practice

College of Computer Science and Technology, Zhejiang University, Spring 2022
Monday 15:55 - 17:30, Tuesday 15:55 - 17:30, Room CW-104
Tuesday 14:05 - 15:40, Room CW-503

Requirements

1. Proposal
   - Browse the programs of recent S&P/SEC/CCS/NDSS/OSDI/SOSP/SIGCOMM/ISCA/MICRO/HPCA/ASPLOS conferences in the area of (network) security;
   - Find a research topic on (network) security you are interested in;
   - Read state-of-the-art papers as well as recent related papers in the preceding conferences;
   - Discover their common limitations;
   - Propose a feasible solution; [optional for proposal, encouraged for mid-term, must for wrapup]
2. Report
   - What is the research problem?
   - Why is it important?
   - How does the state of the art address it?
   - Any limitations?
   - What would you do? Learn from Research Patterns by Prof. Nick Feamster.
3. Prototype
4. Presentation

WOW THE CLASS!

Reference Project Themes

A Method of Detecting Sensor Attacks Against Robotic Vehicles
Persistent Client-Side Cross-Site Scripting
PhantomCache: Obfuscating Cache Conflicts with Localized Randomization
Blind Certificate Authority
Universal Zero-Knowledge Proof Protocol
Body Sensor Network Security
Off-Path TCP Exploit
Vale: Generating Verifiably Cryptographic Assembly Code
SQLIA detection using Fingerprints method
Atomos: Constant-Size Path Validation Proof
SSD bug hunting: new model prepare for analysis
A New Cryptography Algorithm to Protect Cloud-based Healthcare Services
Automatically Identifying and Understanding Dark Jargons
Web Crawler
CRLite
SUNFLOWER: A Trust Execution Environment on RISC-V Based on Tagged Memory
Honeywords
Automated Website Fingerprinting with Machine Learning
Atlas: Ecient Multipath Validation
Differential Privacy
Detecting Browser Extensions
Preventing Malicious Calls with Machine Learning
Attempts to Make Two Initial Improvements to Tor
Brain Password
Deep Website Fingerprinting
Web Enclave

2019

2020

Deep Website Fingerprinting
Honeywords: Password Hashing Competition
Detecting DNS Covert Tunnel Based on Machine Learning
Spectre Attack and How to Defend: Data Side and Instruction Side
Password Retention Problem in Android
Multi-Cloud Oblivious Storage
Blind Certificate Authorities
ZBAFuzzer: A Fuzzing Tool for BLE Programs in Zephyr Firmware
Backdoor Attack By One-pixel Trigger
How to End Password Reuse on the Web
An Informal Survey on Randomized Smoothing
On the Decentralization of the Consensus Protocol of Bitcoin
Hitchhiker: Accelerating ORAM with Dynamic Scheduling
Adversial Example Defense
PrivKVD
Database Recovery with Query Distribution
Crowd-sensing

Why do you care?

40% of Grade
lab alternative

More than that?

Learn to
learn things differently

Know not only how but also why

What’s more?

cultivate research experience

aim at publication

gain leverage for graduate/job application

Grade?

Grading

10%	Assignment
40%	Lab or Project Lab 01:10% Lab 02: 10% Lab 03: 20%
50%	Final Exam closed-book + memo

Teaching Plan

- Keep it simple
- Focus on the core concepts
- Try to help you more easily understand

How will you contribute?

Thanks In Advance

- Be initiative
- Be active
- Be devoted
- …
- **AT LEAST**

  submit assignments & lab reports

  show up to final exam

Office Hour

- By appointment
- Teaching Assistant: Fanli Jin

Reading

- The Security Mindset by Bruce Schneier [video] [text1] [text2]
- The Internet: Cybersecurity & Crime by Parisa Tabriz and Jenny Martin