https://brown-csci1660.github.io

CS1660: Intro to Computer Systems Security
Spring 2026

Final Review

Instructor: **Nikos Triandopoulos**

April 28, 2026

BROWN

Lecture 14

- Operating system (OS) security
  - 14.1 SQL injection, database security
    - CIA for DBMS
    - Indirect information disclosure
    - SQL-injection attacks (how, why, effect)
  - 14.2 Buffer overflows
    - Buffer-overflow attacks (how, why, effect)
      - Three main required steps (see Shellcode example)
      - Role of memory stack

Lecture 15

- OS security
  - 15.1 Access control, 15.2 OS access control
    - Main concepts/principles
      - Authentication Vs. authorization, reference monitor
      - ACE, ACL
      - DAC Vs. MAC
      - Closed Vs. open

Lecture 17

- OS security
  - 17.1 File-system access control, 17.2 setuid/setgid vulnerabilities
    - Basics on Linux permissions
    - Role of
      - setuid/setgid programs
      - /tmp directory
      - symlinks
      - Root
    - Focus on security examples

Lecture 18

- OS security
  - 18.1 More on race conditions, 18.2 isolation
    - Race conditions, Time to Check Vs. Time to Use (see examples)
    - Principle of Least Privilege, isolation mechanisms
  - 18.3 Malware
    - Main types: virus, worm, trojans, rootkits, ransomware
    - Main ideas on transmission, propagation, activation

Lecture 19

- Network security
  - 19.1 More on malware, 19.2 malware detection
    - Main ideas on countermeasures
    - Detection limitations
  - 19.3 Cloud security
    - Computing and security advantages, security concerns (e.g., CIA)
  - 14.4 email security
    - Conceptual understanding of SMTP, SPF, DKIM, DMARK protocols
  - 19.5, 20.0 APTs
    - What they involve, what do we learn (or not) through discussed examples?

Lecture 20

- Network security
  - 20.1 PillarBox, SIEM, security analytics
    - What is the problem studied in PillarBox?
    - What is the importance of security analytics?
    - What is the role of APTs in this new defense setting?

Lecture 21

- Network security
  - 21.1 Networking and security, 21.2 protocol layers and encapsulation
    - High-level understanding of how the Internet works
  - 21.3, 21.4 The physical, link and network (+ 22.3 transport) layers
    - High-level understanding of these core layers
    - Link/frames/MACs, Network/packets/IP addresses (+ Transport/sessions/ports/TCP,UDP)
  - 21.5 LAN attacks
    - ARP spoofing/poisoning, MAC-learning attack, ARP and DOS

Lecture 22

- Network security
  - 22.1 DHCP, NAT, 22.2 routing
    - DHCP poisoning, routing vulnerabilities
  - 22.3 The transport layer
    - General concepts as they relate to security topics, TCP Vs. UDP
  - 22.4 DNS security
    - How DNS operates, how CIA relates to DNS, how DNSSEC and NSEC work, what new vulnerabilities were introduced, what motivated NSEC3, …
  - 22.5 DDoS attacks
    - The Dyn DDOS attack, the general DDOS-attack format
    - Examples: Ping flood, Smurth attack, echo-chargen, SYN flood