CNT5412/CNT4406
Network Security

Course Introduction

Zhenhai Duan

Instructor

- Professor Zhenhai Duan (duan@cs.fsu.edu)
- Office: 162 LOV
- Office hours:
  - 1:00PM to 2:00PM, T/Th
  - Or by appointment
  - Email: duan@cs.fsu.edu
- Class website:
  - Use blackboard http://campus.fsu.edu
  - Discussion board
- Research area
  - Computer networks and network security
  - Homepage: http://www.cs.fsu.edu/~duan

Teaching Assistant

- Shiva Houshmand
  - Office: MCH 106C
  - Office hours
    - 10:00AM – 11:00AM, Wednesday
    - Or by appointment
- Shuaiyuan Zhou
  - Office: MCH 106C
  - Office hours
    - 10:00AM – 11:00AM, Friday
    - Or by appointment

Prerequisites

- **COP4530: Data Structures, Algorithms, and Generic Programming**

- Unofficial requirements
  - Computer Networks
  - CNT 4504 Intro to Computer Networks, or
  - CNT 5505 Data and Computer Networks

  - Programming
  - Comfortable with programming using a high-level programming language such as C/C++ and Java.

Course Material

- **Required Textbook :**
  - **Network Security: Private Communication in a Public World (2nd edition)** by *Kaufman, Perlman, and Speciner*.
  - Publisher: Prentice Hall PTR
- **Recommended Reference Textbook :**
  - **Handbook of Applied Cryptography,** available online
  - **Cryptography and Network Security: Principles and Practice (5th Edition),** by William Stallings.

- Lecture slides posted at the class website

Workload and Grading Policies

1. **Five homework assignments – 40%**
   - 8% for each assignment
   - Including both written and programming assignments
2. **Two exams – 45%**
   - Midterm: 20%
   - Final Exam - 25%
3. **One course project –** 15 **%**
   - Group up to 3 students
   - A group must consist of either all undergraduate students or graduate students.

Final Letter Grades

- Link to final letter grades

Accounts

- Computer Science account (<yourid>@cs.fsu.edu)
  - For doing assignments (linprog1 to linprog4.cs.fsu.edu)
  - http://www.cs.fsu.edu/sysinfo/newstudent.html
- FSU account (<yourid>@fsu.edu)
  - For receiving class announcements
  - For submitting assignments
  - For getting your grades
  - http://www.ucs.fsu.edu/getStarted.html
- Access to blackboard
  - For class materials, discussion board, grades etc.
  - Through your FSU account
  - http://campus.fsu.edu

Academic Integrity

- **Means**
  - **No copying from anywhere**
  - **Don't solve assignments for others**
  - **Don't ask/give solutions.**
  - **Protect your solutions**
  - **Don't distribute assignments/exams to others (in a later semester)**
- **Moss: An automated tool for comparing code will be used.**
- **Please read the policies on course web page**
- **Dishonesty ➔ Not fair to others.**
  - **You may get a grade of F.**
- **Its better to submit an imperfect assignment than to submit a copied one.**
  - Partial points are always possible

Course Policies

- Attendance is **mandatory**
  - Good attendance = missing 3 or fewer lectures
  - Let the Instructor know in advance when possible
- Missed exams:
  - No makeup exams will be given
    - except in emergencies with appropriate document
- Incomplete
  - No incomplete grade “I” will be given
    - Except in emergencies with appropriate document

To ask or not to ask?

- Me and TA are not psychics ☺
- Please let us know if…
  - You are lost
  - You don't understand something
  - You don't have the background
  - Class can be improved in certain ways

- Feel free to give anonymous feedback online
  - Though direct feedback is always welcome!

Course Overview

- Introduction to network security
  - Secure network services
  - Security mechanisms
  - Threats, attacks, countermeasures
- Networking & secure channels
  - Introduction to cryptography and encryption
  - Authentication
  - Cryptographic Protocols
    - Strong authentication, key exchange

Course Overview (Cont'd)

- Analysis of protocols
- Standards
  - SSL/TLS
  - SSH
  - IPSEC, IKE
  - Kerberos, S/Key
- Public Key Infrastructures
  - PKI: X.509
  - PGP

Course Overview (Cont'd)

- Network security systems and applications
  - Packet filtering/firewalls
  - Traffic monitoring and intrusion detection
  - Routing protocols
  - Distributed Denial of Service attacks
  - Network forensics/ vulnerability assessment

Course Overview (if time)

- Privacy
  - Freenet and Tor
- Web security
  - Java, cookies, HTTP/HTTPS
  - Web objects
- DNS security
- Wireless security
- VoIP security
- Worms and botnets
- Smartcards/Biometrics

What is Security?

- Definitions from the Amer. Herit. Dict. :
  - Freedom from risk or danger; safety
  - Measures adopted … to prevent a crime such as burglary or assault.
- Network security measures:
  - Mechanisms to **prevent**, **detect**, and **recover** from network *attacks*, or for **auditing** purposes.
  - Keeping *operations within the network* secure for users of the network

Terminology

- *Network assets & liabilities*
- *Policies*
- *Security breaches*
- *Threats*
  - *Vulnerabilities*
  - *Attacks*
- *Threat intensity*
- *Security attack: a threat*
- *Security services: eg. data confidentiality*
- *Security mechanisms; eg. encryption*

A Secured Network

- A network is “secured” if it has deployed adequate measures for prevention of, detection of, and recovery from attacks.
  - Adequate = commensurate with the value of the network’s assets and liabilities, and the perceived threat intensity.

Security Goals

- Confidentiality
- Integrity
- Availability

Other important security goals include auditability

Security Services

- Data confidentiality
  - Protection from unauthorized disclosure
- Data integrity
  - No modification, insertion, deletion, replay, etc.
- Availability

- Authentication
  - Entity is who it claims to be.
- Nonrepudiation
  - Protection against party to transaction claiming “it wasn’t me”
- Access control
  - Resources that can be used

Security Mechanisms

- Encipherment
- Traffic padding
- Digital signature
- Hashing for data integrity
- Event detection (breaches) & recovery
- Audit trail
- Access control mechanisms

Security operations

- **Prevention** against adversarial or accidental capture and/or modification of information.
- **Audit** of data accesses/modifications, and of privileged operations.
- **Detection** of all improper access to data and system resources.
- **Recovery** from unauthorized access, restoring data values, system integrity, and identifying compromised data/resources.
- Retaliation (legal, PR, info. warfare)

Authentication / Data Integrity

- Authentication mechanisms comprise a substantial portion of this course.
- Used to prevent impersonation and detect unauthorized data modifications.
- Some mechanisms to provide data integrity will not be considered:
  - Enforcement of safe data manipulation methods (file system protection mechanisms, database protection mechanisms).

Availability

- Continuous service, quality of service, resource wastefulness reduction
  - Typical attack: DoS, DDoS
- Prevention by removal of bottlenecks
- **Detection** of attacks
- **Recovery** of service provisionability
- **Audit** of service requests

Concrete Security Measures

- Securing an open network requires adoption of a myriad of measures:
  - Policies, audit and evaluation
  - Personnel training
  - Physical security/ EM emanation shielding
  - Authentication and access control
  - **Communication security:** Cryptography-based techniques
    - *focus of this course*

Reading Assignment

- Chapter 1
- Paper
  - [VK1983]