Lecture 1: Introduction*

CS 392/6813 2009

Nitesh Saxena

*Adopted from Previous Lectures by Nasir Memon

Outline

- Administrative Stuff
- Introductory Technical Stuff

9/10/2009 Lecture 1 - Introduction
Some Important Pointers

- Instructor: Nitesh Saxena
  - Office: LC 228
  - Email: nsaxena@poly.edu (best way to reach me!)
  - Phone No: 718-260-3116
  - Office Hours: **Wednesdays 3-4pm** (or by appointment)
- Course Web Page (also accessible through my webpage)
  http://isis.poly.edu/courses/cs392-f2009
- TA:
  - Yasemin Avcular: yavcul01@students.poly.edu
  - PhD student, research in networking and security
- MyPoly Web Page: http://my.poly.edu/

About the Instructor

- A fairly recent PhD graduate from UC Irvine
- Research in computer and network security, and applied cryptography
- Web page: http://cis.poly.edu/~nsaxena
Prerequisites

1. Solid background in Mathematics
2. Good programming skills
3. Knowledge in Algorithms/Data Structures
4. [Others]
   1. Operating Systems
   2. Networks

- If you don’t satisfy the prerequisites
  - Talk to me

What to expect

- The course would be quite tough
  - Lot of math and programming
  - Hectic schedule; heavy workload
- The grading might not be curved
  - I would love to give A's but I won't mind giving F's when deserved
- I might/will make mistakes
  - Please point them out
  - Talk to me if you have any complaints (or send me an anonymous email 😊)

**But, I guarantee that**

- I will encourage you to do your best
- you'll have fun
- I'll help you learn as much as I can – don't hesitate to ask for help whenever needed
- although you won't become experts, you will learn enough to move on!
- you'll hopefully get motivated to pursue research in this area, ultimately

- You should not take this course if
  - you are not serious
  - you think it would be an easy substitute
  - you think you will learn "hacking"
  - you think he's a new(ish) instructor, so he'll keep the course easy and give away grades
Other Security Courses at Poly

- Network Security: offered in spring
- Cryptography: offered in spring
- Other specialized courses

Course References

- Introduction to Computer Security -- Matt Bishop
- Handbook of Applied Cryptography – Alfred Menezes, Paul van Oorschot, Scott Vanstone
  - Free online copy http://www.cacr.math.uwaterloo.ca/hac/
- Wikipedia can be a good reference at times
- Other references to be provided as we proceed
Grading

- 50% - Weekly Homeworks and Programming assignments
- 50% - 1 Midterm and 1 Final

Collaboration and Cheating Policy

- You are not allowed to collaborate with one another, in any form, while doing your homeworks and exams, unless stated otherwise; perpetrators will at least fail the course
- You can definitely refer to online materials and other textbooks; but when you do, you should cite so in your homeworks.
- No reference to previous years’ homework solutions is allowed – this also constitutes cheating – violators will at least fail the course
Late Homework Policy

- None – no late homeworks are allowed
- Either you submit on time and your homework will be graded OR you submit late and the homework is NOT graded
- You should stick to deadlines
- Exception will be made ONLY under genuine circumstances

Tentative Course Schedule

- Basic Cryptography
- Some Network Security: Protocol Design
- Access Control
- Privacy and Anonymity
- Security Design Principles
- Threat Modeling
- Software Vulnerabilities (Buffer Overflows)
- Usable Security
Good News: HW#1 is assigned

- See course web page
- **Due next Thursday (mid-night: 11:59pm) on 09/17/09**
- Be honest in your answers - this will give me an idea as to where you stand and help me mold my lectures accordingly

Instructions

- HW submissions
  - Name your files "Lastname_Firstname_HW#"
  - Submit it on MyPoly
  - PDF format only
- Check the course web-site regularly
  - I am posting lectures/homeworks there
- Check your **poly email** regularly
  - I am sending out announcements there
    - e.g., when I post homeworks
- **NO EXCUSES** for not following instructions
Computer Security: Why it is important?

- The numbers speak for themselves.
  - CERT Statistics
- Our computer systems are quite vulnerable
  - Poor design or after the fact design
  - Lack of awareness and education
  - Under-estimation of threat model and attacker capabilities
  - Buggy software

Primary motivation for the course!

Threats, Vulnerabilities and Attacks

- A threat to a system is any potential occurrence, malicious or otherwise, that can have an adverse effect on the assets and resources associated with the system.
- A vulnerability of a system is some characteristic that makes it possible for a threat to occur.
- An attack on a system is some action that involves exploitation of some vulnerability in order to cause an existing threat to occur.
Types of Threats

- Can be classified into four broad categories
  - Disclosure - unauthorized access to information
  - Deception - acceptance of false data
  - Disruption - interruption or prevention of correct operation
  - Usurpation - unauthorized control of some part of a system
- Examples include – snooping, sniffing, spoofing, delay, denial of service, theft of computational resources...

Primary Issues

- **Confidentiality**: prevention of unauthorized disclosure of information
- **Integrity**: prevention of unauthorized modification of information
- **Availability**: ability to withstand unauthorized withholding of information or resources

- **Security** – freedom from risk and danger.
- In early days of computers security meant physical security and confidentiality.
- Integrity and access control then became important with multi-tasking computers.
- In recent years availability is a big issue.
- Now security is hard to define!!

Computer Security Definitions.

- Security is the ability of a system to protect information and system resources with respect to confidentiality, integrity, and availability.
- Computer Security deals with the prevention and detection of unauthorized actions by users of a computer system.
- Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.

- Cheswik and Bellovin – “keeping anyone from doing things you do not want them to do, with, on, or from your computers or any peripheral devices.”

- Garfinkel and Spafford - “A computer is secure if you can depend on it and its software to behave as you expect ... This concept is often called trust; you trust the system to preserve and protect your data.”

Computer Security – other issues

- There are other issues that arise in the design of secure systems besides confidentiality, availability and integrity:
  - Accountability
  - Reliability
  - Access Control
  - Authentication
  - Non-repudiation
  - Privacy
Policy and Mechanism

- A security policy is a statement of what is, and is not, allowed.
  - Expressed mathematically. Axiomatic.
  - List of allowed and disallowed actions
- A security mechanism is a procedure, tool, or method of enforcing security policy.

Security Policy

- A security policy is a set of rules stating which actions are permitted and which are not.
- Can be informal or highly mathematical.
- If we consider a computer system to be a finite state automaton with state transitions then
  - A security policy is a statement that partitions the states of a system into a set of authorized or secure states and a set of unauthorized or non-secure states.
  - A secure system is a system that starts in an authorized state and cannot enter an unauthorized state.
  - A breach of security occurs when a system enters an unauthorized state.
- We expect a trusted system to enforce the required security policies.
Elements of a Security Policy

- A security policy considers all relevant aspects of confidentiality, integrity and availability.
  - Confidentiality policy: Identifies information leakage and controls information flow.
  - Integrity Policy: Identifies authorized ways in which information may be altered. Enforces separation of duties.
  - Availability policy: Describes what services must be provided: example – a browser may download pages but no Java applets.

CS Department Security Policy

- [http://cis.poly.edu/security-policy.html](http://cis.poly.edu/security-policy.html)
Security Mechanism

- A security mechanism is a procedure that enforces some part of a security policy.
- We will learn many cryptographic and non-cryptographic mechanisms.

Goals of Security Mechanism

- Given a policy that specifies what is “secure” and what is “non-secure” goal of security is to put in place mechanisms that provide:
  - Prevention
    - Involves implementing mechanisms that users cannot override and are trusted to be implemented in correct and unalterable ways.
  - Detection
    - Goal is to determine that an attack is underway, or has occurred and report it.
  - Recovery
    - Resuming correct operation either after an attack or even while an attack is underway.
Types of Security Mechanisms/controls

- Cryptography and cryptographic protocols.
- Software controls.
- Hardware controls.
- Physical controls.

Trust

- Security policies and mechanisms are based on assumptions and one trusts that these assumptions hold.
- Aspirin from drugstore is considered trustworthy. The basis of this trust is:
  - Testing and certification by FDA.
  - Manufacturing standard of company and regulatory mechanisms that ensure it.
  - Safety seal on the bottle.
- Similarly, for a secure system to achieve trust, specific steps need to be taken.
Trust

- Trusting the mechanism requires us to assume:
  - Each mechanism designed to implement part of policy
  - Union of mechanisms implement all aspects of policy
  - Implemented correctly
  - Installed and administered correctly

Specification, Design and Implementation

- A specification is a statement of the desired functioning of the system.
- Design of a system translates the specifications into components that will implement the specifications.
- Given a design, an implementation creates a system that satisfies the design.
Operational Issues in Security

- Risk Analysis or Assessment
- Cost-Benefit Analysis
- Laws and Regulations
- Human Issues: usability

Security Life Cycle

- Threats
- Policy
- Specification
- Design
- Implementation
- Operation and Maintenance
Some Questions

- I access internet via your wireless access point: this is an example of ------?
- Alice knows that Bob bought a herpes drug today: what’s violated?
- I use an open smtp server to send an email using your email address: I -----ed you?
- My photos are residing on facebook’s server: what do I trust?
- Microsoft keeps issuing security patches for their softwares: what stages in security life cycles are involved?

Some Questions

- University policy disallows cheating – copying another students homework assignment. Student A has her homework file world readable. Student B copies it. Has B violated the policy?
- Eve jams the wireless signal in the CS: what does she achieve?
- INS officials identify immigrants using their fingerprints: what is the primary assumption in play?
- US law allows sharing copyright movies using for example BitTorrent: true or false?
- Alice is dead. Could Alice’s mother get access to her late daughter’s emails residing on yahoo’s server? See: http://www.cnn.com/2009/TECH/05/18/death.online/index.html
Further Reading

- Must read chapter 1 of text
- Must read “What is There to Worry About? An Introduction to the Computer Security Problem” by Brinkley and Schell
- Optional read “Concepts and Terminology for Computer Security” by Brinkley and Schell