Lecture 1: Introduction

CS 436/636/736
Spring 2012

Nitesh Saxena
Today’s informative/fun bit -- CAPTCHA
Outline

• Administrative Stuff
• Introductory Technical Stuff
Some Important Pointers

- Instructor: Nitesh Saxena
  - Office: CH 133
  - Email: saxena@cis.uab.edu (best way to reach me!)
  - Phone No: 205-975-3432
  - Office Hours: Thursdays 3-4pm (or by appointment)
- Course Web Page (also accessible through my web-page)
  http://www.cis.uab.edu/saxena/teaching/csx36-s12/
- TA/Grader
  - TBA
- Blackboard: https://cms.blazernet.uab.edu/cgi-bin/bb9login
About the Instructor

• PhD graduate from UC Irvine
• Previously an Assistant Professor at the Polytechnic Institute of New York University
• Research in computer and network security, and applied cryptography
• Web page: http://cis.uab.edu/saxena
Prerequisites

• The official prerequisites for the undergraduate (436) students are:
  – Algorithms and Data Structures (CS 303 or equivalent)
  – Computer Organization and Assembly Language Programming (CS 330 or equivalent)
• A minimum grade of C is required in the prerequisite courses
• At a higher level, the course requires the students to have good mathematical background, programming knowledge, and familiarity with algorithms and data structures
What to expect

- The course would be quite involved
  - Lot of math
  - Some programming
  - Reasonable workload
- The grading will 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 😊)
- 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
- This class is not
  - Going to be be an easy substitute for something (believe me it will not be!)
  - About “hacking”
What I expect of you

- Please do attend lectures
- Review lecture slides after each lecture
- Solve textbook exercises as you read through the chapters
- Ask questions in the class
- Ask questions over email
- Attend office hours
- Try to start early on homework assignments
  - Don’t wait until the very last minute!
- Follow the instructions and submit assignments on time
Course References

- No mandatory textbook
  - Lecture slides are your primary reference

- Recommended text:

- Wikipedia can be a good reference at times
- Other references to be provided as we proceed
Grading

• 50% - Homework Assignments (some may involve programming)
• 25% - 1 Midterm Exam
• 25% - 1 Final Exam
Policies Against Cheating or Misconduct

- You are not allowed to collaborate with any other student, in any form, while doing your homeworks, unless stated otherwise; perpetrators will at least fail the course or disciplinary action may be taken.
- No collaboration of any form is allowed on exams.
- You can definitely refer to online materials and other textbooks; but whenever you do, you should cite so in your homeworks. This is a rule of thumb.
- Also check: http://main.uab.edu/Sites/undergraduate-programs/general-studies/academic-success/67537/
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**

- Cryptography: first several lectures
- Some Network Security: Protocol Design
- Privacy and Anonymity
- Security Design Principles
- Threat Modeling
- Software Vulnerabilities (Buffer Overflows)
- Usable Security
Scheduled Travel

• Jan 26-28
  – Giving an invited colloquium seminar in the Computer Science Department at Brown University
  – **No class on Jan 26 (Thursday)**
  – However, this will not affect our overall course schedule and topic coverage.

• Information about any further travel will be provided as it becomes available
Instructions

- HW submissions
  - Name your files “Lastname_Firstname_HW#”
  - Submit it on Blackboard
    - Please make sure that you have correctly submitted/uploaded the files
      (simply “saving” them may not be sufficient)
  - PDF format only
- Check the course web-site regularly
  - I am posting lecture slides and homeworks there
- Check your UAB email regularly
  - I am sending out announcements there
    - e.g., when I post homeworks
- Only use your UAB email to communicate with me and the TA/grader
- **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
  - Weak threat model and under-estimation of 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, delaying, denial of service, malware, 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
Computer Security – Evolving Definitions

• **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.
Computer Security – Informal Definitions

- Cheswick 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 and anonymity
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.
UAB Data Protection and Security Policy

• http://www.uab.edu/handbook/f-policies-procedures/f-data-protection
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
Operational Issues in Security

- Risk Analysis or Assessment
- Cost-Benefit Analysis
- Laws and Regulations
- Human Issues: usability
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?
- You do not make your age public on Facebook. An attacker can however infer your age from the ages of your friends. What has been violated?
- 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 “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