Introduction and overview

- What is computer/network security?
- Course philosophy and goals
- High-level overview of topics
- Course organization and information

“Security”

- Most of computer science is concerned with achieving desired behavior
- In some sense, security is concerned with preventing undesired behavior
  - Different way of thinking!
  - An enemy/opponent/hacker/adversary may be actively and maliciously trying to circumvent any protective measures you put in place

Broader impacts of security

- Explosive growth of interest in security
- Impact on/interest from most areas of CS
  - Theory (especially cryptography)
  - Databases
  - Operating systems
  - AI/learning theory
  - Networking
  - Computer architecture/hardware
  - Programming languages/compilers
  - HCI
Philosophy
- We are not going to be able to cover everything
- Main goals
  - Exposure to different aspects of security; meant mainly to “pique” your interest
  - The “mindset” of security: a new way of thinking...
  - Become familiar with basic crypto, acronyms (RSA, SSL, PGP, etc.), and “buzzwords”

Student participation (I hope!)
- Ask questions
- Read the textbook chapters, course notes and papers listed on course webpage
- Monitor the media
  - Email me relevant/interesting stories

High-level overview
- Introduction...
  - What do we mean by security?
  - Is security achievable...?
- Cryptography
  - Cryptography is not the (whole) solution
  - ...but is is an important part of the solution
  - Along the way, we will see why cryptography can’t solve all security problems

High-level overview II
- System security
- General principles
- Security policies
- Access control; confidentiality/integrity
- OS security
High-level overview III
- Network security
- Identity
- Authentication and key exchange protocols
- Some real-world protocols

High-level overview IV
- Application-level security
- Web-based security
- Buffer overflows
- Viruses, worms, and malicious code

Course Organization

Staff
- Me
- TA
- Contact information, office hours, listed on course webpage
Course webpage

- [http://www.cc.gatech.edu/~aboldyre/teaching/Sp06cs4803/](http://www.cc.gatech.edu/~aboldyre/teaching/Sp06cs4803/)
- Contains course organization, updated syllabus, various links, etc.
  - Also links to papers
  - Slides posted for convenience, but no substitute for attending lecture
  - Homeworks distributed from the course webpage
  - Check often for announcements

Textbooks

- I will primarily use two textbooks:
  - “Security in Computing” by Pfleeger and Pfleeger
  - “Network Security...” by Kaufman, Perlman, and Speciner
  - Both will make it easier to follow the course (but only the first one is required)
  - For the crypto part I will use the online lecture notes of Bellare and Rogaway (links are on the course web page)

Other readings

- Will be linked from the course webpage
- Please suggest other readings or relevant news articles!

Course requirements

- Homeworks and project
  - About 4-5 HWs throughout the semester
  - Some parts (usually the programming portion) may be done with a partner
  - 2 exams
  - TAs will help with using programming
  - Details about project to come...
Security is Harder than it Seems*

*And it already seems quite hard!

Some terminology
- Confidentiality, privacy
- Integrity, authenticity
- Availability
- Often, these are conflicting goals...

“We are all Security Customers”
- Security is always a trade-off
- The goal should never be “to make the system as secure as possible”...
- ...but instead, “to make the system as secure as possible within certain constraints” (cost, usability, convenience)

Cost-benefit analysis
- Important to evaluate what level of security is necessary/appropriate
- Cost of mounting a particular attack vs. value of attack to an adversary
- Cost of damages from an attack vs. cost of defending against the attack
- Likelihood of a particular attack
“More” security not always better
• “No point in putting a higher post in the ground when the enemy can go around it”
• Need to identify the weakest link
• Security of a system is only as good as the security at its weakest point...
• Security is not a “magic bullet”
• Security is a process, not a product

Human factors
• E.g., passwords...
• Outsider vs. insider attacks
• Software misconfiguration
• Not applying security patches
• Social engineering
• Physical security

Importance of precise specification
• Security policy
  • Statement of what is and is not allowed
• Security mechanism
  • Method for enforcing a security policy
• One is meaningless without the other...

Prevention not the only concern
• Detection and response
  • How do you know when you are being attacked?
  • How quickly can you stop the attack?
  • Can you prevent the attack from recurring?
• Recovery
  • Can be much more important than prevention
• Legal issues?
“Managed security monitoring”

- Is the state of network security this bad?
- Network monitoring; risk management
  - Attacks are going to occur; impossible to have complete protection
- Security as a process, not a product...

“Trusting trust”

- Whom do you trust?
- Does one really need to be this paranoid??
  - Probably not
  - Sometimes, yes
- Shows that security is complex...and essentially impossible
- Comes back to risk/benefit trade-off

Nevertheless...

- In this course, we will focus on security in isolation
- But important to keep in the back of your mind the previous discussion...
  - ...and if you decide to enter the security field, learn more about it!