

## Lecture 1: Computer Security, Cryptography and Privacy

ECE1776  
David Lie

1

## Overview

- What is this course about?
  - Computer System Security: vulnerabilities and defenses
    - What constitutes a vulnerability
    - How vulnerabilities are exploited
    - How to identify and prevent vulnerabilities
    - How to (build) secure systems
    - Theoretical Security Models
    - Cryptography and protection of information
  - A focus on how to systems are exploited, and from that, how to build secure systems



2

## Overview

- Who should take this course:
  - Primarily intended for Graduate Students
  - People interested in building secure systems
  - Students should have a good understanding of operating systems (ECE344 or equivalent)
- Class format
  - Each class begins with a short discussion of current events
  - Students will do their presentations of papers assigned the previous week
  - I will give a lecture for this week that gives background for this week's readings
  - The lectures indicate the current "best practice", while the papers give an idea of what the "cutting edge" in research and industry is



3

## Grading

- Assignments:
  - Presentation of papers (20%)
  - Assignments (20%)
  - Class Participation (10%)
  - Final Project (50%)



4

## Presentation

- 2-3 Papers are covered per lesson
- Students will make a short 30 minute presentation at the beginning of the next class
  - 2-3 minute explanation of the problem the paper is trying to address
  - 1-2 minute overview of the solution presented in the paper
  - 3-4 minute detailed explanation of the solution
  - 2-3 minute explanation of the evaluation methods used and results
  - 2-3 minute conclusion on what you LEARNED from reading the paper, and what the important results of the paper are
- They will then lead a 10-15 minute discussion on the papers



5

## Assignment and Project

- Assignment
  - Programming: Writing and identifying exploits in code
    - Should have some familiarity with Linux, use of a debugger, and assembler
  - Written Assignment: Solve some security related problems
- Final Project
  - A final project will be assigned
  - Students have the option of creating their own project
- You will need access to an Intel based Linux Machine for this
  - There are several on the eecg system that you can use
  - If you don't have access, please let me know



6

## A Bit About Me

- David Lie:
  - More information at [www.eecg.toronto.edu/~lie](http://www.eecg.toronto.edu/~lie)
  - Interests in Computer Security, Operating Systems and Computer Architecture
- Educational background:
  - Graduated Bachelor's in Engineering Science, U of T
  - Master's and Ph.D at Stanford University



7

## The History of Computing

- For a long time security was largely ignored in the community
  - The computer industry was in "survival mode", struggling to overcome technological and economic hurdles
  - As a result, a lot of corners were cut and many compromises made: e.g. Intel, Microsoft
    - Companies that tried to always design perfect systems often failed
  - There was lots of theory, and even examples of systems built with very good security, but they were largely ignored or unsuccessful:
    - As a programming language ADA had many features which would have increased program security and reliability, however, C became the language of choice for the systems community due to its power and ease of use



8

## Computing Today is very Different

- Computers today are far from "survival mode"
  - Performance is abundant and the cost is very cheap
  - As a result, computers find their way into every application, every facet of society
    - Governments
    - Hospitals
    - Appliances...
- The introduction of the Internet is the other big factor
  - Computers are all connected and interdependent
  - This codependency magnifies the effects of any failures or mishaps



9

## Biological Analogy

- Computing today is very homogeneous. A single architecture and a handful of operating systems (read 2) dominates the population
- In biology, homogeneous populations are in danger – a single disease or virus can wipe them out over night because they all share the same weaknesses. The disease needs only a vector to travel from one host to another.
- While the computers are like the animals, the Internet provides the vector. It's like having only one kind of cow in the world, and having them drink from one single pool of water!
  - The conclusion is that there is an explosive situation brewing here.



10

## The Warhol Worm

- Andy Warhol claimed that: "In the future everyone will have 15 minutes of fame"
- In Usenix Security 2002, Stuart Staniford, Vern Paxson and Nicholas Weaver published a paper called "[How to Own the Internet in your Spare Time](#)".
  - Show that a properly designed worm can infect every vulnerable host on the internet within 15 minutes
    - Exploit many vectors such as P2P file sharing, intelligent scanning, use of hitlists, etc...
  - In 2003, Slammer became the fastest worm ever infecting 90% of vulnerable hosts in 10 minutes



11

## Computer Security as a Field

- Computer Security is broader than just defending against intrusions and hackers.
- In general Computer Security is the study of protecting computer systems and digital data. This can include:
  - Protecting Electronic Privacy
  - Tamper Resistance for software and hardware
  - Protection intellectual property (digital rights management)
  - Increasing the reliability of infrastructure against failure and attacks



12

## Who Needs Security?

- Used to be only Governments and Banks were interested in security
  - Governments had very important secrets that other governments had great incentives to attain
    - Military pass codes
    - Caesar used a simple substitution cipher
    - The Enigma machine in WWII
  - Large businesses such as Banks, Credit Cards
    - Have to protect the data of millions of customers
    - Often have sensitive information about strategies, patents, etc.



13

## The Internet has Changed all That

- Everyone Needs security
  - All businesses risk getting their data and IP stolen
    - Valve's Leak of the Half-life 2 source code
    - Yahoo and EBay's Denial of Service Attacks cost \$\$\$
    - Credit card numbers stolen from CDNow
    - Microsoft's Versign Certificate compromised
    - Sobig Virus reportedly contributed to the Black-out of 2003
  - Even the average user
    - Personal information, bank accounts, passwords, etc...
    - But their machine can be stolen to launch other attacks
    - DDOS, Connection Laundering, FTP Server



14

## Security Problems

- Systems must be error-free:
  - Even if a vulnerability is obscure or infrequent, adversaries will exploit it
  - Developers constantly release patches, but people are slow to apply them
- Security is very hard to configure:
  - Systems are only secure if configured correctly
  - Often default installations are NOT secure
  - Patching systems is complicated, causing downtime to reboot or causing compatibility problems
- Security should be transparent for the user:
  - SSH vs. PGP
  - If system is complicated, people won't use it



15

## Resources for this Course

- The course will use the following textbook as a reference:
  - [Security in Computing](#) by Pfleeger and Pfleeger
- The following textbooks are also recommended as reference:
  - [Applied Cryptography, 2nd. ed](#) by Bruce Schneier
  - [Handbook of Applied Cryptography](#) by Menezes et al.
- Web Page
  - <http://www.eecg.toronto.edu/~lie/ECE1776>
- Lots of other stuff on the web:
  - Phrack, TESO, Bugtraq ...



16

## Some Reading

- [Reflections on Trusting Trust](#), Ken Thompson.



17