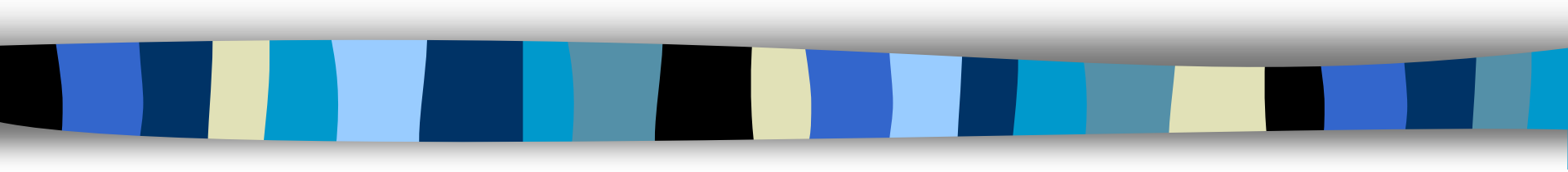
Information Security
CS 526
Topic 1



Overview of the Course

Recent Security News

- Snowden leaks information about various NSA data collection programs
  - Phone call record
  - Supposedly email, instant message, etc.
- National Security Agency
  - http://www.pbs.org/wgbh/pages/frontline/homefront/preemption/nsa.html
- Facebook CEO's page hacked by Palestinian Khalil Shreateh to demonstrate bugs in Facebook

In the News Last Year: Hackers Force Apple, Amazon to Change Security Policy

- What happened?
  - Hackers gained access to Mat Honan (a reporter)'s iCloud account, then (according to Honan)
    - At 5:00 PM, they remote wiped my iPhone
      At 5:01 PM, they remote wiped my iPad
      At 5:05, they remote wiped my MacBook Air.
- How did the attacker get access to iCloud account? Any guess?
- Lessons?
    - Security only as strong as the weakest link.
    - Information sharing across platforms can lead to unexpected vulnerabilities

Stuxnet (2010)

- Stuxnet: Windows-based Worm
  - Worm: self-propagating malicious software (malware)
- Attack Siemens software that control industrial control systems (ICS) and these systems
  - Used in factories, chemical plants, and nuclear power plants
- First reported in June 2010, the general public aware of it only in July 2010
- Seems to be a digital weapon created by a nation-state
  - 60% (more than 62 thousand) of infected computers in Iran
  - Iran confirmed that nuclear program damaged by Stuxnet
  - Sophisticated design, special targets, expensive to develop

Malware That Appear to Be Related to Stuxnet

- Duqu (September 2011)
  - Use stolen certificates, exploits MS Word
- Flame (May 2012)
  - A tool for cyber espionage in Middle East (infecting approx. 1000 machines, mostly in Iran)
  - “Suicide” after being discovered
  - 20 Mbytes, with SQLLite DB to store info, hide its own presence, exploit similar vulnerabilities as StuxNet, adjust its behavior to different Anti-Virus
  - Presents a novel way to produce MD5 hash collision to exploit certificates

See the Course Homepage

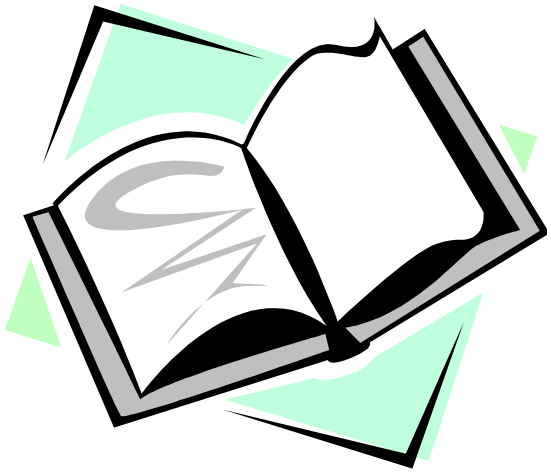
- http://www.cs.purdue.edu/homes/ninghui/courses/526_Fall13/index.html

- Knowledge needed for the course
  - Programming knowledge (for two programming projects)
    - Web (PHP)
    - Low-level (C, knowledge of assembly)
  - Knowledge of computer/networking
  - Appropriate mathematical sophistication

Readings for This Lecture

Required readings:

- Information Security on Wikipedia (Basic principles & Risk management)



Optional Readings:

- Counter Hack Reloaded
  - Chapter 1: Introduction
- Security in Computing: Chapter 1

What is Information (Computer) Security?

- Security = Sustain desirable properties under intelligent adversaries

- Desirable properties
  - Understand what properties are needed.
- Intelligent adversaries
  - Needs to understand/model adversaries
  - Always think about adversaries.

Security Goals/Properties (C, I, A)

- Confidentiality (secrecy, privacy)
  - only those who are authorized to know can know
- Integrity (also authenticity in communication)
  - only modified by authorized parties and in permitted ways
  - do things that are expected
- Availability
  - those authorized to access can get access

Which of C, I, A are violated in ..

- The Stuxnet attack compromises
  - integrity of software systems,
  - availability of some control functionalities,
  - confidentiality of some keys in order to sign malware to be loaded by Windows
- The Apple/Amazon attack
  - Confidentiality of credit card digits
  - Integrity of password
  - Availability of data and devices
- The Facebook attack
  - Integrity
  - Potential availability concern

Computer Security Issues

- Malware (Malicious Software)
  - Computer viruses
  - Trojan horses
  - Computer worms
    - E.g., Morris worm (1988), Melissa worm (1999), Stuxnet (2010), etc.
  - Spywares
  - Malwares on mobile devices
- Computer break-ins
- Email spams
  - E.g., Nigerian scam (419 scam, advanced fee fraud), stock recommendations

More Computer Security Issues

- Identity theft
- Driveby downloads
- Botnets
- Distributed denial of service attacks
- Serious security flaws in many important systems
  - electronic voting machines, ATM systems

Why Do Computer Attacks Occur?

- Who are the attackers?
  - bored teenagers, criminals, organized crime organizations, rogue (or other) states, industrial espionage, angry employees, …
- Why they do it?
  - fun,
  - fame,
  - profit, …
    - computer systems are where the moneys are
  - Political/military objectives

Why These Attacks Can Succeed?

- Software/computer systems are buggy
- Users make mistakes
- Technological factors
  - Von Neumann architecture: stored programs
  - Unsafe program languages
  - Software are complex, dynamic, and increasingly so
  - Making things secure are hard
  - Security may make things harder to use

Why Do These Factors Exist?

- Economical factors
  - Lack of incentives for secure software
  - Security is difficult, expensive and takes time
- Human factors
  - Lack of security training for software engineers
  - Largely uneducated population

Security is Not Absolute

- Is your car secure?
- What does “secure” mean?
- Are you secure when you drive your car?

- Security is relative
  - to the kinds of loss one consider
    - security objectives/properties need to be stated
  - to the threats/adversaries under consideration.
    - security is always under certain assumptions

Security is Secondary

- What protection/security mechanisms one has in the physical world?
- Why the need for security mechanisms arises?
- Security is secondary to the interactions that make security necessary.

> Robert H. Morris : The three golden rules to ensure computer security are: do not own a computer; do not power it on; and do not use it.

Information Security is Interesting

- The most interesting/challenging threats to security are posed by human adversaries
  - Security is harder than reliability
- Information security is a self-sustaining field
  - Can work both from attack perspective and from defense perspective
- Security is about benefit/cost tradeoff
  - Thought often the tradeoff analysis is not explicit
- Security is not all technological
  - Humans are often the weakest link

Information Security is Challenging

- Defense is almost always harder than attack.
- In which ways information security is more difficult than physical security?
  - adversaries can come from anywhere
  - computers enable large-scale automation
  - adversaries can be difficult to identify
  - adversaries can be difficult to punish
  - potential payoff can be much higher
- In which ways information security is easier than physical security?

Tools for Information Security

- Cryptography
- Authentication and Access control
- Hardware/software architecture for separation
- Processes and tools for developing more secure software
- Monitoring and analysis
- Recovery and response

What is This Course About?

- Learn to think about security when doing things
- Learn to understand and apply security principles
- Learn how computers can be attacked, how to prevent attacks and/or limit their consequences.
  - No silver bullet; man-made complex systems will have errors; errors may be exploited
  - Large number of ways to attack
  - Large collection of specific methods for specific purposes

Ethical Use of Security Information

- We discuss vulnerabilities and attacks
  - Most vulnerabilities have been fixed
  - Some attacks may still cause harm
  - Do *not* try these outside the context of this course

Coming Attractions …

- Cryptography: terminology and classic ciphers.
- Readings
  - Cryptography on Wikipedia