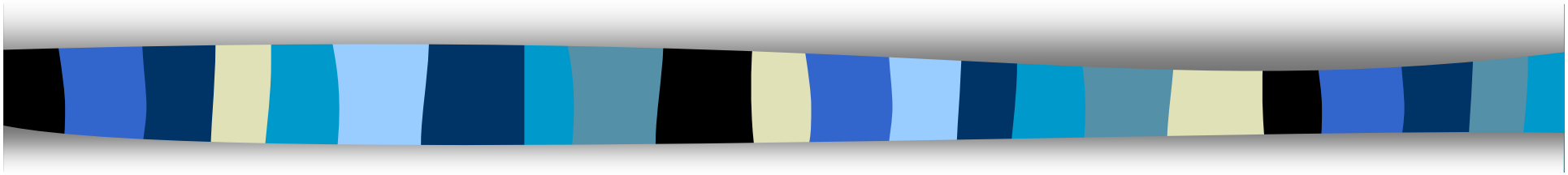
# Computer Security
# CS 426
## Lecture 1



## Overview of the Course

# In Recent (Last Week)'s News

- **Intel buys McAfee for $7.7B in push beyond PCs**
- **HP to Buy Vulnerability Specialist Fortify Software**

The market for computer security knowledge will grow.

# More In the News

- Malware Call to Arms: Threat at All-Time High and Rising
- Beware the Facebook "Dislike" Button Scam
- Facebook Warns of Clickjacking Scam
- Android Game Is a Spy App in Disguise
- Cameron Diaz hot bait for online traps
- Virus Fools People Into Uninstalling Their Antivirus Software

What are some common themes of the attacks?

# Why Do Computer Attacks Occur?

- Who are the attackers?
  - bored teenagers, criminals, organized crime organizations, rogue states, industrial espionage, angry employees, …
- Why they do it?
  - fun,
  - fame,
  - profit, …
    - computer systems are where the moneys are

# Computer Security Issues

- Computer viruses
- Trojan horses
- Computer worms
  - E.g., Morris worm (1988), Melissa worm (1999), etc.
- Distributed denial of service attacks
- Computer break-ins
- Email spams
  - E.g., Nigerian scam, stock recommendations

# More Computer Security Issues

- Identity theft
- Zero-day attacks
- Botnets
- Serious security flaws in many important systems
  - electronic voting machines, ATM systems
- Spywares
- Driveby downloads
- Social engineering attacks

# Why do these attacks happen?

- 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 does this happen?

- 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 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.

# 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

# 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-sustained field
- 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?

# What is This Course About?

- Learn 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
- Learn to think about security when doing things
- Learn to understand and apply security principles

# See the Course Homepage

- http://www.cs.purdue.edu/homes/ninghui/courses/426_Fall10/index.html

# Course Outline

- Introduction/review of cryptography
- Operating system security
- Software security
- Access control models
- Network security
- Web security

# 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 at home

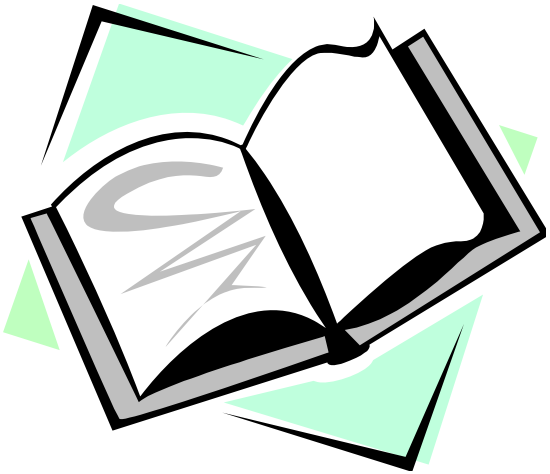
# Readings for This Lecture

Required readings:

- Information Security on Wikipedia

Optional Readings:

- Counter Hack Reloaded
  - Chapter 1: Introduction
- Security in Computing
  - Chapter 1: Is There a Security Problem in Computing



# Coming Attractions …

- Cryptography: terminology and classic ciphers.

- Readings for next lecture:
  - Cryptography on wikipedia
  - Interesting reading
    - The Code Book by Simon Singh