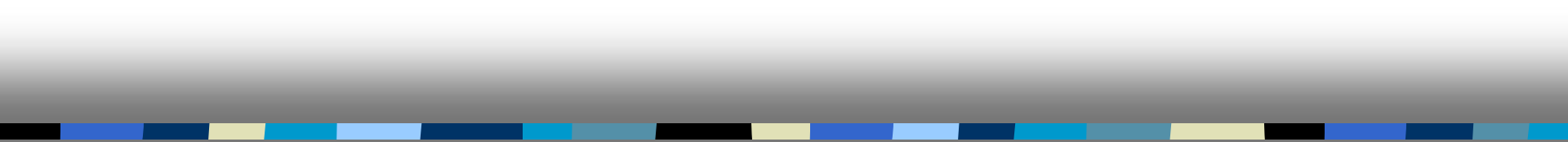


# Computer Security

## CS 426

### Lecture 1



## Overview of the Course

# See the Course Homepage

- [http://www.cs.purdue.edu/homes/ninghui/courses/426\\_Fall07/index.html](http://www.cs.purdue.edu/homes/ninghui/courses/426_Fall07/index.html)

# Why Computer Security?

Computers are under attacks and suffer damages

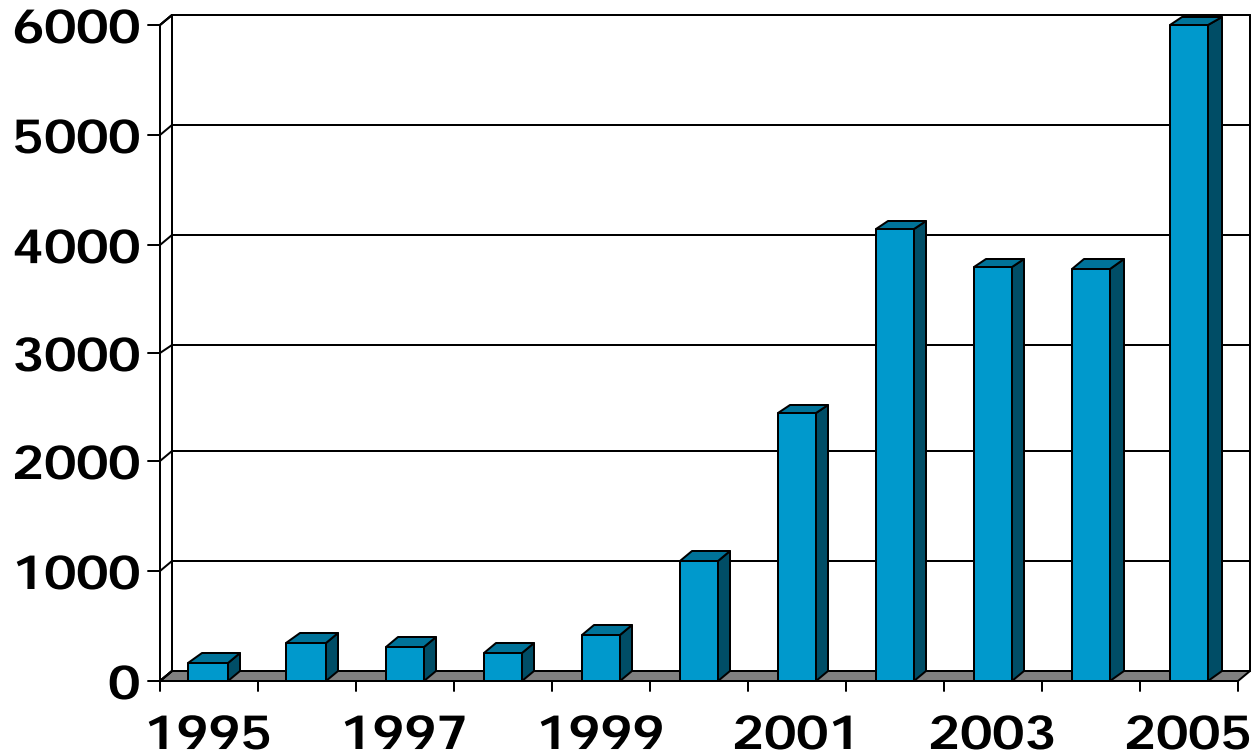
- Who are the attackers?
  - bored teenagers, criminals, organized crime organizations, rogue states, industrial espionage, angry employees, ...
- Why they do it?
  - enjoyment, fame, profit, ...
  - computer systems are where the moneys are

# Computer Security Issues

- Computer worms
  - E.g., Morris worm (1988), Melissa worm (1999)
- Computer viruses
- Distributed denial of service attacks
- Computer break-ins
- Email spams
  - E.g., Nigerian scam, stock recommendations
- Identity theft
- Botnets
- Serious security flaws in many important systems
  - electronic voting machines
- Spyware

# How big is the security problem: One Data Point

CERT Vulnerabilities reported



# Why does this happen?

- Lots of buggy software & wrong configurations...
  - Awareness is the main issue
- Some contributing factors
  - Few courses in computer security
  - Programming text books do not emphasize security
  - Few security audits
  - Unsafe program languages
  - Programmers are lazy
  - Consumers do not care about security
  - Security may make things harder to use
  - Security is difficult, expensive and takes time

# 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

# Security Goals

- Confidentiality (secrecy, privacy)
  - only those who are authorized to know can know
- Integrity
  - only modified by authorized parties and in authorized ways
- Availability
  - those authorized to access can get access

# Terminologies

- Vulnerabilities (weaknesses)
- Threats (potential scenario of attack)
- Attacks
- Controls (security measures)

# Methods of Defense

- Prevention
- Hindrance
- Deterrence
- Deflection
- Detection
- Recovering

# Security Principles

- Principle of weakest link
- Principle of adequate protection
  - Goal is not to maximize security, but to maximize utility while limiting risk to an acceptable level within reasonable cost
- Principle of effectiveness
  - Controls must be used—and used properly—to be effective. they must be efficient, easy to use, and appropriate
  - Psychological acceptability
- Principle of defense in depth
- Security by obscurity doesn't work

# Layers of Computer Systems

- Computer systems has multiple layers
  - Hardware
  - Operating systems
  - System software, e.g., databases
  - Applications
- Computer systems are connected through networks
- Computer systems are used by humans

# 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
- Purpose of this class
  - Learn to prevent malicious attacks
  - Use knowledge for good purposes

# Law enforcement

- David Smith
  - Melissa virus: 20 months in prison
- Ehud Tenenbaum (“The Analyzer”)
  - Broke into US DoD computers
  - sentenced to 18 months in prison, served 8 months
- Dmitry Sklyarov
  - Broke Adobe ebooks
  - Arrested by the FBI, prosecuted under DMCA, stayed in jail for 20 days,

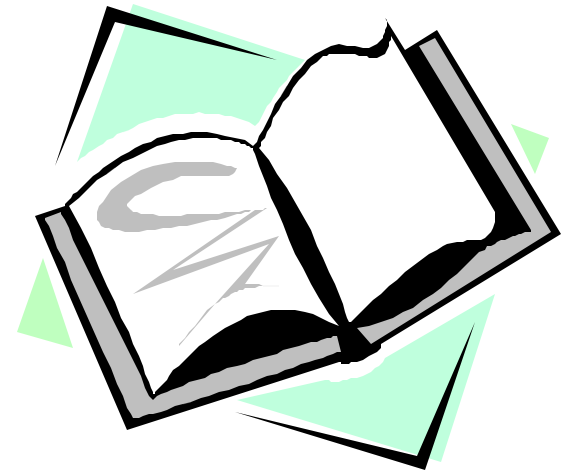
# Readings for This Lecture

## Counter Hack Reloaded

- Chapter 1: Introduction

## Security Engineering

- Chapter 1: What is Security Engineering



# Coming Attractions ...

- Operating Systems Security Basics
- Readings for next several lectures:
  - Counter Hack Reloaded
    - Chapters 2, 3, & 4:
  - Security Engineering:
    - Chapter 4: Access Control

