Foundations of Computer Security

Lecture 1: Introduction

Dr. Bill Young
Department of Computer Sciences
University of Texas at Austin

Course Topics

Topics we will cover include:

- What is computer security?
- Why is computer security important?
- Why is security difficult?
- Security policies
- Elementary information theory
- Elementary cryptography
- Cryptographic protocols
- Availability
- System evaluation and certification.

What Does Security Mean?

The term *security* is used in a variety of contexts. What's the common thread?

- Personal security
- Corporate security
- Personnel security
- Energy security
- Homeland security
- Operational security
- Communications security
- Network security
- System security

What Does Security Mean?

In the most general terms, *security* seems to mean something like "protection of assets against threats."

- What assets?
- What kinds of threats?
- What does "protection" mean?
- Does the nature of protection vary depending on the threat?

Security on a Personal Level

Suppose you're visiting an online retailer, and need to enter personal information. What protections do you want? From what threats?

- Authentication (protection from phishing)
- Authorization
- Privacy of your data
- Integrity of your data
- Availability
- Non-repudiation
- What else?

Security on an Institutional Level

Consider the following scenarios:

1. A large corporation's computer systems are penetrated and data on thousands of customers is stolen.
2. A student hacks into university registrar's system and changes his grade in several classes he has taken.
3. An online retailer's website is overwhelmed by malicious traffic, making it unavailable for legitimate customer purchases.

Does this suggest why it's hard to define "security" in the context of digital systems?

Why are Attacks Becoming More Prevalent?

- Increased connectivity
- Many valuable assets online
- Low threshhold to access
- Sophisticated attack tools and strategies available
- Others?

Some Sobering Facts

- There were over 1 million new unique malware samples discovered in each of the past two quarters. Unlike the worms and mass-mailers of the past, many of these were extremely targeted to particular industries, companies and even users. (www.insecureaboutsecurity.com, 10/19/2009)
- Once PCs are infected they tend to stay infected. The median length of infection is 300 days. (www.insecureaboutsecurity.com, 10/19/2009)

Some Sobering Facts

- A recent study of 32,000 Websites found that *nearly 97% of sites carry a severe vulnerability*. –Web Application Security Consortium, Sept 2008
- "NSA found that inappropriate or incorrect software security configurations (most often caused by configuration errors at the local base level) were responsible for 80 percent of Air Force vulnerabilities." –CSIS report on *Securing Cyberspace for the 44th Presidency*, Dec. 2008, p. 55.

Why Should We Care?

A dozen determined computer programmers can, if they find a vulnerability to exploit, threaten the United States' global logistics network, steal its operational plans, blind its intelligence capabilities or hinder its ability to deliver weapons on target. – *William J. Lynn, U.S. Deputy Secy of Defense, Foreign Affairs (2010)*

A top FBI official warned today that many cyber-adversaries of the U.S. have the ability to access virtually any computer system, posing a risk that's so great it could "challenge our country's very existence."
–Computerworld, March 24, 2010

Educate Yourself

Educating yourself about computer security can:

- enhance your own protection;
- contribute to security in your workplace;
- enhance the quality and safety of interpersonal and business transactions;
- improve overall security in cyberspace.

Next lecture: Why Security is Hard.