Overview of the Course

Elisa Bertino
Purdue University
IN, USA
bertino@cs.purdue.edu

Course Homepage
http://www.cs.purdue.edu/homes/bertino/426Fall2009/426fall.htm
Well Known Security and Privacy Problems

- Computer worms
- Computer viruses
- Distributed denial of service attacks
- Email spams
  - E.g., Nigerian scam, stock recommendations
- Identity theft
- Botnets
- Spyware

Causes of Software Security Incidents

- Buggy software and wrong configurations...
  - Unsafe program languages
  - Complex programs
  - Security considered rather an add-on
- Lack of awareness and education
  - Few courses in computer security
  - Programming text books do not emphasize security
- Poor usability
  - Security sometimes makes things harder to use
- Economic factors
  - Consumers do not care about security
  - Security is difficult, expensive and takes time
  - Few security audits
- Human nature
Human Factor

• Who are the attackers?
  – bored teenagers, criminals, organized crime, organizations, rogue states, industrial, espionage, angry employees, …
• Why do they attack systems?
  – enjoyment, curiosity, fame, profit
  – data represents an extremely valuable asset and often the main goal of attackers is to get valuable or sensitive data

Goals of this Course

• Learn to protect data and databases
• Learn to understand and apply security principles
• 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

Course Outline

• Security principles
• Review of cryptography
• Operating systems security
• Database security and privacy
• Elements of network security
• Legal and ethical issues

CERT Vulnerabilities Reported
http://www.cert.org.stats

<table>
<thead>
<tr>
<th>Year</th>
<th>Total vulnerabilities cataloged</th>
</tr>
</thead>
<tbody>
<tr>
<td>1995</td>
<td>417</td>
</tr>
<tr>
<td>1996</td>
<td>345</td>
</tr>
<tr>
<td>1997</td>
<td>311</td>
</tr>
<tr>
<td>1998</td>
<td>262</td>
</tr>
<tr>
<td>1999</td>
<td>417</td>
</tr>
<tr>
<td>2000</td>
<td>1,090</td>
</tr>
<tr>
<td>2001</td>
<td>2,437</td>
</tr>
<tr>
<td>2002</td>
<td>4,129</td>
</tr>
<tr>
<td>2003</td>
<td>3,784</td>
</tr>
<tr>
<td>2004</td>
<td>3,780</td>
</tr>
<tr>
<td>2005</td>
<td>5,990</td>
</tr>
<tr>
<td>2006</td>
<td>8,064</td>
</tr>
<tr>
<td>2007</td>
<td>9,058</td>
</tr>
<tr>
<td>Q1-Q3, 2008</td>
<td>6,098</td>
</tr>
<tr>
<td>Totals</td>
<td>44,074</td>
</tr>
</tbody>
</table>
Reference Material

- Textbook
- Additional papers will be assigned in class

Basic security-related requirements: the CIA triad

Confidentiality
- Ensuring that information is accessible only to those authorized to have access

Integrity
- Maintaining the resource/service deliverable to intended users
- Maintaining data validity against malicious or accidental altering

Availability

Note: Integrity is a broader notion preserving integrity of an item means that the item is:
- precise, accurate, consistent, meaningful and useful
- modified only in acceptable ways, by authorized people, by authorized processes

Other requirements

Confidentiality
- Ensuring that information is accessible only to those authorized to have access

Integrity
- Maintaining the resource/service deliverable to intended users
- Maintaining data validity against malicious or accidental altering

Availability

Other Requirements

- Accountability: Holding a subject accountable for her actions/results
- A particular case of accountability is non-repudiation, where responsibility for an action cannot be denied
- NIST defines non repudiation as:
  - Assurance that the sender of information is provided with proof of delivery and the recipient is provided with proof of the sender’s identity, so neither can later deny having processed the information.
Other Requirements

- Privacy: maintaining confidentiality of personally identifiable information
- (1) The ability of an individual or organization to control the collection, storage, sharing, and dissemination of personal and organizational information.
- Note: The concept of privacy cannot be very precise, because privacy relates to 'rights' that depend on legislation.

Terminology

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

Methods of Defense

- Prevention
- Deterrence
- Deflection
- Detection
- Recovery

Controls

- Encryption
- Software controls
- Hardware controls
- Policies and procedures
- Physical controls
Layers of Computer Systems

• Computer systems have multiple layers
  – Hardware
  – Operating systems
  – Database systems
  – Applications
• Computer systems are connected through networks
• Computer systems are used by humans

Readings for this Lecture

Security in Computing
Chapter 1: Introduction

Acknowledgments

The course slides are partially based on slides by:
Prof. Ninghui Li
Prof. Lorenzo D. Martino
Prof. Cristina Nita-Rotaru