CS 392/681 - Computer Security

Module 0 - Introduction

Polytechnic UNIVERSITY
Course Policies and Logistics

- CS 681 and CS 392 – Same course. Almost 😊
- 681 and SFS students will be required to do extra work.
- Course web page. You are required to check regularly (daily) for:
  - Information and announcements. Lecture notes. Homework
- My Poly Page
  - Grades
- Course Policies
  - Grades – 50% HW, 25% Midterm and Final
  - Late assignments not accepted. Period.
- ISIS – Room 219 Rodgers Hall.
  - Some students can be given VPN access.
- HW 0 assigned. Due next week!!!
2001 AD - The Wild Wild West!!

- Out-of-the-box Linux PC hooked to Internet, not announced:
- [30 seconds] First service probes/scans detected
- [1 hour] First compromise attempts detected
- [12 hours] PC fully compromised:
  - Administrative access obtained
  - Event logging selectively disabled
  - System software modified to suit intruder
  - Attack software installed
  - PC actively probing for new hosts to intrude

Source – CERT Report
The Situation We Have Today

- Novice Intruders Use Crude Exploit Tools
- Advanced Intruders Discover New Vulnerability
- Crude Exploit Tools Distributed
- Automated Scanning/Exploit Tools Developed
- Widespread Use of Automated Scanning/Exploit Tools
- Intruders Begin Using New Types of Exploits

Source – CERT Report
So Why Are We So Vulnerable?

- Poor Software and Systems Design
  - Buffer Overflow is the cause of almost half the known vulnerabilities
  - Shrinking time to market leads to improperly tested software
  - Security not considered during design time but only added later on

- Lack of Education
  - Secure programming techniques not taught in typical curriculum.
  - Lack of awareness about security issues.

- Lack of Deterrence Mechanisms
  - Most criminal acts go unpunished
Do We Care? Is security important?

Slammer hits Davis-Besse Nuclear Power Station:
“[…] But an incident in January at the Davis-Besse Nuclear Power Station, run by the FirstEnergy Corporation outside Toledo, Ohio, showed that this was not always the case. The nuclear plant has not been generating power since early 2002, but a computer system there that was not supposed to be linked to the Internet was invaded by a worm known as Slammer, causing the system to shut down for five hours. The event was not made public until Kevin Poulsen reported it on Aug. 20 on SecurityFocus.com …” New York Times, September 7

Sobig affects Amtrak trains, Air Canada
“[…] a spokesman for CSX, said the company noticed Wednesday at about 1:15 a.m. that a variant of the Blaster virus was interfering with its train operations and dispatching system.”
“[…] A variant of the Blaster virus on Tuesday affected about half of Air Canada's phone-reservation capacity and some of its airport check-in operations, said spokesman John Rebel.” Wall Street Journal, August 21

AT&T to invest $3 billion in 2003 for global network
“AT&T will spend US$3 billion in capital expenditures this year to completely transform its global network from having a voice-based carrier infrastructure into a single Internet Protocol (IP)-based network…” InfoWorld, September 11
So What Can We Do About It?
Identify and Remove Vulnerabilities

- Perform vulnerability analysis
- Perform risk assessment
- Start removing vulnerabilities in order of decreasing risk.

*But this is more like focusing on developing antibiotics whereas the water supply itself is contaminated*
Cleaning up the Water Supply

- Hold vendors responsible for faulty software
  - Litigate, Regulate, Legislate
- Develop novel architectures and techniques that lead to secure systems
  - Multi-disciplinary research teams
- Educate
  - Safe programming practices
  - Basic principles of secure system design
  - Broad based awareness of secure systems engineering
Some terminology and definitions
Threats, Vulnerabilities and Attacks

- A *threat* to a system is any potential occurrence, malicious or otherwise, that can have an adverse effect on the assets and resources associated with the system.

- A *vulnerability* of a system is some characteristic that makes it possible for a threat to occur.

- An *attack* on a system is some action that involves exploitation of some vulnerability in order to cause an existing threat to occur.
Types of Threats

- Can be classified into four broad categories
  - Disclosure - unauthorized access to information
  - Deception - acceptance of false data
  - Disruption – interruption or prevention of correct operation
  - Usurpation – unauthorized control of some part of a system

- Examples include – snooping, spoofing, delay, repudiation, masquerading, denial of receipt, unauthorized information modification or creation, theft of computational resources etc.

- **Security** – freedom from risk and danger.
- In early days of computers security meant physical security and confidentiality.
- Integrity and access control then became important with multi-tasking computers.
- In recent years availability is a big issue.
- Now security is hard to define!!
Computer Security Definitions.

- Security is the ability of a system to protect information and system resources with respect to confidentiality, integrity, and availability.

- Computer Security deals with the prevention and detection of unauthorized actions by users of a computer system.

- Computer security is preventing attackers from achieving objectives through unauthorized access or unauthorized use of computers and networks.
Basic Components

- Confidentiality
  - Keeping data and resources hidden

- Integrity
  - Data integrity (integrity)
  - Origin integrity (authentication)

- Availability
  - Enabling access to data and resources

- Cheswick and Bellovin – “keeping anyone from doing things you do not want them to do, with, on, or from your computers or any peripheral devices.”

- Garfinkel and Spafford - “A computer is secure if you can depend on it and its software to behave as you expect … This concept is often called trust; you trust the system to preserve and protect your data.”
There are other issues that arise in the design of secure systems besides confidentiality, availability and integrity:

- Access Control
- Usage Control
- Authentication
- Auditing
- Privacy
- Vulnerability Analysis
- Evaluation of Secure Systems
- etc
Goals of Security

- Given a policy that specifies what is “secure” and what is “non-secure” goal of security is to put in place mechanisms that provide:
  - Prevention
    - Involves implementing mechanisms that users cannot override and are trusted to be implemented in correct and unalterable ways.
  - Detection
    - Goal is to determine that an attack is underway, or has occurred and report it.
  - Recovery
    - Resuming correct operation either after an attack or even while an attack is underway.
Methods of Defense

- Security policies.
- Cryptography and cryptographic protocols.
- Software controls.
  - Internal program controls.
  - Operating system controls.
  - Development controls.
- Hardware controls.
- Physical controls.
Policies, mechanisms and procedures make assumptions and one trusts these assumptions hold.

SA receives security patch and installs it. Has she increased the security of the system?

Aspirin from drugstore is considered trustworthy. The basis of this trust is:

- Testing and certification by FDA.
- Manufacturing standard of company and regulatory mechanisms that ensure it.
- Safety seal on the bottle.

Similarly, for a secure system to achieve trust, specific steps need to be taken.
Policy and Mechanism

- A *security policy* is a statement of what is, and is not, allowed.
  - Expressed mathematically. Axiomatic.
  - List of allowed and disallowed actions

- A *security mechanism* is a procedure, tool, or method of enforcing security policy.
  - Can be non-technical
Security Policy

- A security policy is a set of rules stating which actions or permitted and which are not.
- Can be informal or highly mathematical.
- If we consider a computer system to be a finite state automaton with state transitions then
  - A security policy is a statement that partitions the states of a system into a set of authorized or secure states and a set of unauthorized or non-secure states.
  - A secure system is a system that starts in an authorized state and cannot enter an unauthorized state.
  - A breach of security occurs when a system enters an unauthorized state.
- We expect a trusted system to enforce the required security policies.
A security policy considers all relevant aspects of confidentiality, integrity and availability.

- Confidentiality policy: Identifies information leakage and controls information flow.
- Integrity Policy: Identifies authorized ways in which information may be altered. Enforces separation of duties.
- Availability policy: Describes what services must be provided: example - a browser may download pages but no Java applets.
Mechanism and Policy

- **Example:** University policy disallows cheating - copying another students homework assignment. Student A has her homework file world readable. Student B copies it. Who has violated policy?

- Mechanism should not be confused with policy.
- A **security mechanism** is an entity or procedure that enforces some part of a security policy.
- We will learn many cryptographic and non-cryptographic mechanisms.
CS Department Security Policy

- [http://cis.poly.edu/security-policy.html](http://cis.poly.edu/security-policy.html)
Computer Security and Trust.

- Tomas Olovsson – “A secure system is a system on which enough trust can be put to use it together with sensitive information.”

- “You can't trust code that you did not totally create yourself!!” - Reflections on trusting trust – Ken Thompson’s Turing Award Lecture.

- The open source movement and Linux. Install Linux today!!
## Qualities of Security and Trustedness

<table>
<thead>
<tr>
<th>Secure</th>
<th>Trusted</th>
</tr>
</thead>
<tbody>
<tr>
<td><em>Either-or:</em> Something is secure or not secure.</td>
<td><em>Graded:</em> There are degrees of trustedness.</td>
</tr>
<tr>
<td>Property of <em>presenter</em></td>
<td>Property of <em>receiver</em></td>
</tr>
<tr>
<td><em>Asserted:</em> based on product characteristics</td>
<td><em>Judged:</em> based on evidence and analysis</td>
</tr>
<tr>
<td><em>Absolute:</em> not quantified as to how, when, where or by whom.</td>
<td><em>Relative:</em> viewed in context of use</td>
</tr>
<tr>
<td>A <em>goal</em></td>
<td>A <em>characteristic.</em></td>
</tr>
</tbody>
</table>
Assumptions and Trust

Let $A$ be the set of secure states (as specified by some security policy). Let the security mechanisms restrict the system to some set of states $R$.

- A security mechanism is secure if $R \subseteq A$; it is precise if $R = A$; and it is broad if there are states $r$ such that $r \in R$ and $r \notin R$

- Trusting the mechanism requires us to assume:
  - Each mechanism designed to implement part of policy
  - Union of mechanisms implement all aspects of policy
  - Implemented correctly
  - Installed and administered correctly
Assurance

- How do we quantify trust?

- System specification, design and implementation can provide a basis for determining how much to trust – assurance.

- When you buy a bottle of aspirin from a drug store you trust it. Why?
  - FDA, Manufacturing standards, safety seal on bottle provide assurance.
Specification, Design and Implementation

- A specification is a statement of the desired functioning of the system.
- Design of a system translates the specifications into components that will implement the specifications.
- Given a design, an implementation creates a system that satisfies the design.
Operational Issues

- Cost-Benefit Analysis: Difficult to do in a precise manner.
- Risk Analysis: Is often subjective.
- Laws and Custom.
- Human Issues
Further Reading

- Must read chapter 1 of text.
- Recommended “What is There to Worry About? An Introduction to the Computer Security Problem” by Brinkley and Schell.
- Recommended read – “Reflections on trusting trust” - Ken Thompson’s Turing Award Lecture.