CS 591: Introduction to Computer Security

Lecture 1: Overview

James Hook

Objectives

- Discuss the scope of Computer Security
- Introduce a vocabulary to discuss security
- Sketch the course

CS as Engineering

- Is Computer Science, or Computer Security, an engineering discipline?
- Are we meeting the reasonable expectations of society to
  - Codify best practices
  - Not repeat mistakes
  - Appropriately apply relevant science to the construction of artifacts

Case Study

- Voting
- Do electronic voting machines meet the reasonable expectations of society to provide a technology that is trustworthy and cost effective?

Trustworthy: Worthy of confidence; dependable [Webster's on-line]

Expectations of Voting

- Vote is by secret ballot
- The vote should be correctly tallied; all votes cast should be counted in the election
- Every eligible voter who presents themselves at the polling place should be able to vote

Confidentiality

Integrity

Availability

Security or Computer Security?

- Are the expectations of integrity, confidentiality, and availability specific to computers?
- Can the properties of the computer system be considered independently of its use?

Voting: Policies and Mechanisms

Policy

- Who can vote?
  - Legal requirements for eligibility
    - Must be a citizen residing in the precinct
    - Must be of voting age
  - Administrative requirements to register to vote
    - Fill out an application
    - Present evidence of residence (can be by mail or fax)

Mechanism

Voting Mechanisms

- Paper ballot in a ballot box (or mail)
  - May be implemented as a scan form
- Punch cards
- Mechanical voting machines
- Direct Recording Electronic
- Voter-verifiable paper audit trail

Evaluating mechanisms

- How do we evaluate these options?
- Evaluation must be relevant to a threat model

Voting threat models

- Correlating ballot with voter
- Ballot stuffing
- Casting multiple votes
- Losing ballot boxes
- Ballot modification
- Incorrect reporting of results
- Denial of access to polls
- Vandalism
- Physical intimidation

Electronic voting in the news

- After the 2000 election in Florida there has been a national initiative to improve automation in voting
  - Access: must improve accessibility of polls
  - Mechanism: must improve the repeatability of vote counting (ambiguity of the "hanging chad" or "pregnant chad")
- Electronic voting was suggested as solution

Voting in news

- Computer hardware manufacturers brought forward Direct Recording Electronic voting machines
- Computer Scientists questioned this, including:
  - David Dill, Stanford: http://www.verifiedvotingfoundation.org/
  - Matt Bishop, UC Davis http://nob.cs.ucdavis.edu/~bishop/notes/2006-inter/index.html
  - Ed Felton http://itpolicy.princeton.edu/voting/

Felton's paper

- Security Analysis of the Diebold AccuVote-TS Voting Machine
  - Felton's team injected malware in a voting machine that could alter the outcome of an election or disable a voting machine during an election
  - Malware was spread by sharing memory cards

Goals of the class:

- Provide a vocabulary to discuss issues relevant to the trustworthiness of systems that include computers
- Provide a set of models and design rules to assist in building and assessing trustworthy systems
- Introduce mechanisms that, when used correctly, can increase trust (e.g. crypto, access control)
- Survey common exploitable vulnerabilities (stack attacks, malware, bots)

Components

- Confidentiality
  - Keeping secrets
- Integrity
  - Bank: the balances sum to zero; only authorized actions change the balance
- Availability
  - Bank: making balances available to ATMs

Confidentiality

- Concealment of information or resources
- Government/Military: "Need to Know"
- Mechanisms: Access Control
- Sometimes existence of data is as confidential as content
  - You don't need to read "LayoffList.doc" to know something bad is going to happen

Integrity

- Trustworthiness of data or resources
- Data Integrity
  - Integrity of content (balances sum to zero)
- Origin Integrity
  - Source of data is known (audit trail identifying all changes to bank balances)
- Mechanisms
  - Prevention: block unauthorized changes
  - Detection: analyze data to verify expected properties (e.g. file system consistency check)

Availability

- If an adversary can cause information or resources to become unavailable they have compromised system security
- Denial of Service attacks compromise Availability

Who can you trust?

- What is trust?
- What is trusted?
- What is trustworthy?

  … if an NSA employee is observed in a toilet stall at BWI selling key material to a [foreign] diplomat, then (assuming his operation was not authorized) he can be described as "trusted but not trustworthy" [Ross Anderson, p9-10]

Threats

- Potential violation of security
- Classes
  - Disclosure: unauthorized access
  - Deception: acceptance of false data
  - Disruption: interruption or prevention of safe operation
  - Usurpation: unauthorized control of some part of a system

Classic Threats

- Disclosure
- Deception
- Disruption
- Usurpation

- Snooping:
  - (passive) wiretapping
- Modification (alteration)
  - Active wiretapping; man-in-the-middle
- Masquerading (spoofing)
  - Impersonation with intent to deceive
  - Cf. Delegation: one entity authorizes another to perform functions on its behalf

More Classic Threats

- Disclosure
- Deception
- Disruption
- Usurpation

- Repudiation of Origin
  - A false denial that an entity sent something
- Denial of Receipt
  - A false denial that an entity received something
- Delay
  - Temporary inhibition of a service
- Denial of Service
  - A long term inhibition of a service

Policy and Mechanism

- Security Policy: A statement of what is, and what is not, allowed
- Security Mechanism: A method, tool, or procedure for enforcing a security policy

PSU Computer & Network Acceptable Use Policy

- This acceptable use policy governs the use of computers and networks at Portland State University (PSU). As a user of these resources, you are responsible for reading and understanding this document. …
- Portland State University encourages the use and application of information technologies to support the research, instruction, and public service mission of the institution. PSU computers and networks can provide access to resources on and off campus, as well as the ability to communicate with other users worldwide. Such open access is a privilege and requires that individual users act responsibly. Users must respect the rights of other users, respect the integrity of systems and related physical resources, and observe all relevant laws, regulations, and contractual obligations.

PSU AUP (cont)

- ***Acceptable use terms and conditions:***
  - The primary purpose of electronic systems and communications resources is for University-related activities only.
  - Users do not own accounts on University computers, but are granted the privilege of exclusive use. Users may not share their accounts with others, and must keep account passwords confidential.
  - Each account granted on a University system is the responsibility of the individual who applies for the account. Groups seeking accounts must select an individual with responsibility for accounts that represent groups.
  - The University cannot guarantee that messages or files are private or secure. The University may monitor and record usage to enforce its policies and may use information gained in this way in disciplinary and criminal proceedings.
  - Users must adhere strictly to licensing agreements and copyright laws that govern all material accessed or stored using PSU computers and networks.
  - When accessing remote systems from PSU systems, users are responsible for obeying the policies set forth herein as well as the policies of other organizations.
  - Misuse of University computing, networking, or information resources may result in the immediate loss of computing and/or network access. Any violation of this policy or local, state, or federal laws may be referred to appropriate University offices and/or, as appropriate, law enforcement authorities.

PSU AUP (cont)

- ***Conduct which violates this policy includes, but is not limited to the following:***
  - Unauthorized attempts to view and/or use another person's accounts, computer files, programs, or data.
  - Using PSU computers, accounts, and/or networks to gain unauthorized access to University systems or other systems.
  - Using PSU computers, accounts, and/or networks for: threat of imminent physical harm, sexual or other harassment, stalking, forgery, fraud, generally offensive conduct, or any criminal activity.
  - Attempting to degrade performance of University computers and/or networks.
  - Attempting to deprive other users of University technology resources or access to systems/networks.
  - Using University resources for commercial activity such as creating products or services for sale.
  - Copying, storing, sharing, installing or distributing software, movies, music, and other materials currently protected by copyright, except as permitted by licensing agreements or fair use laws.
  - Unauthorized mass e-mailings to newsgroups, mailing lists, or individuals, i.e. "spamming" or propagating electronic chain letters.
  - Unauthorized "broadcasting" of unsolicited mail, material, or information using University computers/networks.

Goals of Security

- Prevention: Guarantee that an attack will fail
- Detection: Determine that a system is under attack, or has been attacked, and report it
- Recovery:
  - Off-line recovery: stop an attack, assess and repair damage
  - On-line recovery: respond to an attack reactively to maintain essential services

Assumptions

- Since the adversary or attacker is unconstrained, the security problem is always "open"
- Assumptions, either explicit or implicit, are the only constraints on the adversary

Trust

- Every system must trust something
- Trust is an underlying assumption
- To understand a system we must know what it trusts
- Typical examples of trusted entities:
  - We trust the system administrator to not abuse the ability to bypass mechanisms that enforce policy (e.g. access control)
  - We trust the hardware to behave as expected

Minimizing what we trust

- How little can we trust?
- If we trust the processor do we have to trust the boot loader?
- Can we verify that we have the expected operating system before executing it?

Relating Policy and Mechanism

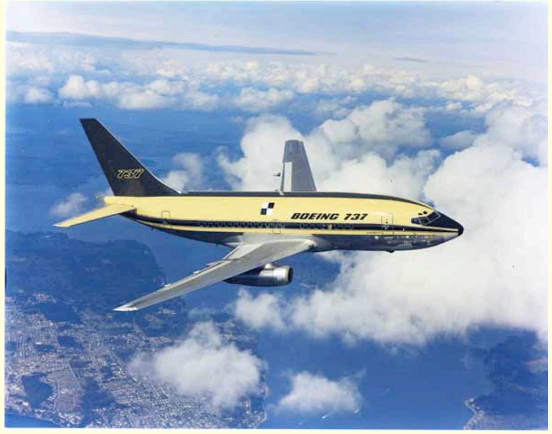
- Formally policy can be seen as identifying a subset of system states that are "secure".
  - State space: P
  - Secure States: Q
- Mechanisms can be identified with restrictions of the state space
  - Reachable states: R
- Policy classification
  - **Secure**: All reachable states are secure ($R \subseteq Q$)
  - **Precise**: The reachable states are exactly the secure states ($R=Q$)
  - **Broad**: There are reachable states that are not secure ($\exists\, r \in R \,.\, R \notin Q$)

Assurance

- An attempt to quantify “how much” to trust a system
- Baseline:
  - What you expect it to do
  - Why you expect it to do that
    - Trust the process
    - Studied the artifact
    - Experience

Why do you trust an Airplane?

- Which of these do you trust more? Why?



NASA images from web site: http://www.dfrc.nasa.gov/Gallery/Photo/

Boeing images from web site: http://www.boeing.com/companyoffices/gallery/flash.html

Framework for Assurance

- Specification: What the system does
  - May be formal or informal
  - Says what, but not how
- Design: An approach to solving the problem; typically identifies components of the solution
  - Design satisfies specification if it does not permit implementations that violate the spec
  - Software design might include component communication and component specifications
- Implementation: A system satisfying the design (transitively the specification)
    - Software: Might be implementations of components described in design in a programming language

Operational Issues

- Policy and Mechanism must be appropriate for context
- Consider policy on vehicle keys in urban and rural settings
  - In urban settings you always take your keys; discourage joy riding/theft
  - In some rural settings people leave keys in vehicles so they are available to someone if they need to move (or use) the vehicle
- How do you make these decisions rationally?

Cost-Benefit Analysis

- What does it cost to provide a security mechanism (or to adopt a security policy)?
- What are the benefits?

Risk Analysis

- What is the likelihood of an attack?
  - Risk is a function of the environment
  - Risks change with time
  - Some risks are sufficiently remote to be "acceptable"
  - Avoid "analysis paralysis"

People

- Ultimately it is the system in use by people that must be secure
- If security mechanisms “are more trouble than they are worth” then users will circumvent them
- Security must be a value of the organization
- Policy and mechanism must be appropriate to the context as perceived by members of the organization

People as threat/weak link

- Insider threat
  - Release passwords
  - Release information
- Untrained personnel
  - Accidental insider threat
- Unheeded warnings
  - System administrators can fail to notice attacks, even if mechanisms report them
- User error
  - Even experts commit user error!
  - Misconfiguration is a significant risk

Conclusions

- Vocabulary for Security:
  - Confidentiality, Integrity, Availability
  - Threats and Attacks
  - Policy and Mechanism
  - Assumptions and Trust
  - Prevention, Detection, Recovery
  - Assurance
  - Operational issues: cost/benefit, risk
- Ultimate goal: A system used by people in an organization to achieve security goals appropriate to their situation

Next Lecture

- Access Control & Foundational Results
- Reading:
  - Felton paper on voting machines
  - Bishop chapters 1, 2 and 3
  - Anderson chapter 1
- Poll: How many have taken CS 581 (Theory of Computation)