CS 591: Introduction to Computer Security

Lecture 1: Overview

James Hook

Course Mechanics

- Course web page:
  - http://web.cecs.pdx.edu/~hook/cs491f09
- Contains:
  - Instructor contact information
  - Term paper handout
  - Grading guidelines
  - Topics and Reading Assignments for each lecture
  - Links to lecture notes
  - H1N1 links

Texts

- Anderson
  - Sometimes anecdotal; a good read
  - Second edition (1/2008) is significant revision (9/11 happened)
  - Parts are available on-line for free (all of first ed)
- Original materials linked on web page
  - Some materials in the ACM library are only accessible when using a PSU IP address (license is based on internet address)
- Supplemental: Bishop (formerly required)
  - Encyclopedic; sometimes dry

Grading

- Midterm: 100 points
- Final: 100 points
- Term paper title, abstract, outline and annotated bibliography: 50 points
- Term paper: 100 points
- Quizzes, Discussion and Class participation: 50 points
  - There will be at least one summarize, outline, and evaluate impact assignment
  - These mechanisms will be used primarily to evaluate mastery of the reading assignments

Academic Integrity

- Be truthful
- Always hand in your own work
- Never present the work of others as your own
- Give proper credit to sources
- Present your data accurately
- Violations of academic integrity will be taken very seriously. Grade of 0 on the assignment. Reported to the university in a manner consistent with university policy.

Term Paper

- Select a topic of your choice on computer security
- Explore:
  - Problem space
  - Solution space
- Identify original sources
- Integrate knowledge; organize; critique

Term Paper

- Midterm:
  - Title
  - Abstract (short description of paper)
  - Outline (identifies structure of paper)
  - Annotated bibliography
    - Author
    - Title
    - Complete bibliographic reference
    - Short description of contribution of paper in your own words

Term Paper

- Due at beginning of last class
  - Final paper
  - 10 - 15 pages (no more than 20!)
  - Paper should have a proper bibliography, references, and should be presented in a manner similar to papers appearing in conferences
  - Paper is not expected to present original research results, but is to be written in your own words and represent what you believe based on your study of the literature

Plagiarism

- Copying text or presenting ideas without attribution is plagiarism
- Plagiarism is a violation of academic integrity
- If you commit plagiarism you will get a grade of 0 and be reported to the university
- I know how to use google
- I will accept no excuses
- There will be no second chances

Exams

- Midterm will cover first half of the class
  - Probably similar to past mid-terms (I will prepare it)
  - Blue book exam
  - Study questions in advance
  - Real questions partially overlap study questions
- Final will cover second half of the class
  - The final will be prepared by Professor Binkley
  - It will not be a blue book exam

Readings

- Reading assignments are on the web page
- Please come to class prepared to discuss the readings
  - You will learn more
  - The person sitting next to you will learn more
- I may institute pop quizzes at any time to evaluate your preparation for class
- I may call on students by name to discuss readings in class

Class Mailing List

- Please sign up for the class mailing list

H1N1Flu

- There is a high probability of a flu outbreak on campus
- Please follow guidelines for minimizing spread of the flu
  - Wash your hands
  - Cover your cough
- If you are sick, please stay home

Flu

- University has published policies on flu (see links from web page)
- Doctors notes are not required
- All reasonable requests for accommodation will be considered
- Instructors may ask students to leave if they show signs of flu
- If you are sick, please stay home!
  - I will!

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?
- What is Engineering?
  - http://en.wikipedia.org/wiki/Engineering

Engineering (Wikipedia)

Engineering is the discipline and profession of applying technical and scientific knowledge and utilizing natural laws and physical resources in order to design and implement materials, structures, machines, devices, systems, and processes that realize a desired objective and meet specified criteria. The American Engineers' Council for Professional Development (ECPD, the predecessor of ABET[1]) has defined engineering as follows:

"[T]he creative application of scientific principles to design or develop structures, machines, apparatus, or manufacturing processes, or works utilizing them singly or in combination; or to construct or operate the same with full cognizance of their design; or to forecast their behavior under specific operating conditions; all as respects an intended function, economics of operation and safety to life and property."[2][3][4]

CS as Engineering

- Are we meeting the reasonable expectations of society to
  - Appropriately apply relevant science to the construction of artifacts
  - forecast their behavior under specific operating conditions

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]

NY Times, January 2008:

"The 2000 election illustrated the cardinal rule of voting systems: if they produce ambiguous results, they are doomed to suspicion. The election is never settled in the mind of the public. To this date, many Gore supporters refuse to accept the legitimacy of George W. Bush's presidency; and by ultimately deciding the 2000 presidential election, the Supreme Court was pilloried for appearing overly partisan."

Reaction to 2000 election

- Help America Vote Act (HAVA) of 2002
  - $3.9 billion for new technology
  - "Computers seemed like the perfect answer to the hanging chad.
    - Touch-screen machines would be clear and legible, …
    - The results could be tabulated very quickly …
    - And best of all, the vote totals would be conclusive…
    - (Touch-screen machines were also promoted as a way to allow the blind or paralyzed to vote … HAVA required each poll station to have at least one "accessible" machine.)"

Touch Screen Voting Today

- Computers have not solved the problem
- There is still a crisis of confidence in voting
  - http://news.google.com/news?hl=en&ned=us&q=voting+machines&btnG=Search

New Jersey

- In February 2008, New Jersey used Sequoia voting machines in their primary election
- Election officials noted anomalies

Candidate Totals

Candidate		Total
***	2-DEM	***
*	president 11th delegate A1	(1)
D13	BARACK OBAMA	57
E13	DENNIS KUCINICH	0
F13	JOHN EDWARDS	3
G13	JOE BIDEN	1
H13	BILL RICHARDSON	1
I13	HILLARY CLINTON	204
J13	Personal Choice	0
***	1-REP	***
*	President A2	(1)
D24	RUDY GIULIANI	1
E24	FRED THOMPSON	0
F24	MITT ROMNEY	11
G24	JOHN McCAIN	9
H24	RON PAUL	0
I24	MIKE HUCKABEE	1
J24	Personal Choice	0

Write In Votes
No Write In Votes In Memory

Option Switch Totals

1	UNUSED	0
2	UNUSED	0
3	UNUSED	0
4	UNUSED	0
5	UNUSED	0
6	2-DEM	267
7	UNUSED	0
8	UNUSED	0
9	UNUSED	0
10	UNUSED	0
11	UNUSED	0
12	1-REP	21
Total		283

Election Officers
Please Complete After Closing The Polls
We the undersigned Election Officers do hereby certify that on the 5 day of Feb 2008 this board under the scrutiny of each member, closed the polls from further voting, obtained this printed record of votes

New Jersey election tape, February 2008, source: Freedom to Tinker blog:

57+3+1+1+204 = 266

1 + 11 + 9 + 1 = 22

Several incidents

- The web site http://citp.princeton.edu/njvotingdocuments/ includes nine tapes from Union County New Jersey (and now several other counties)
- Union County election officials solicited the help of Ed Felten's lab at Princeton

Sequoia's Response

Sender: Smith, Ed [address redacted]@sequoiavote.com
To: felten@cs.princeton.edu, appel@princeton.edu
Subject: Sequoia Advantage voting machines from New Jersey
Date: Fri, Mar 14, 2008 at 6:16 PM

Dear Professors Felten and Appel:

As you have likely read in the news media, certain New Jersey election officials have stated that they plan to send to you one or more Sequoia Advantage voting machines for analysis. I want to make you aware that if the County does so, it violates their established Sequoia licensing Agreement for use of the voting system. Sequoia has also retained counsel to stop any infringement of our intellectual properties, including any non-compliant analysis. We will also take appropriate steps to protect against any publication of Sequoia software, its behavior, reports regarding same or any other infringement of our intellectual property.

Very truly yours,
Edwin Smith
VP, Compliance/Quality/Certification
Sequoia Voting Systems

[contact information and boilerplate redacted]

Princeton gains access

- Law suit originally filed in 2004 was brought to trial in 2008
- Trial judge ordered machines be made available to Princeton affiliated expert witnesses (Appel et al.)
- Machines were studied in July and August 2008
- Findings released October 17, 2008 http://citp.princeton.edu/voting/advantage/

Why?

"THE QUESTION, OF COURSE, is whether the machines should be trusted to record votes accurately. Ed Felten doesn't think so.

Felten is a computer scientist at Princeton University, and he has become famous for analyzing — and criticizing — touch-screen machines.

In fact, the first serious critics of the machines — beginning 10 years ago — were computer scientists." [NY Times; January 2008]

Why? (cont)

"One might expect computer scientists to be fans of computer-based vote-counting devices, but it turns out that the more you know about computers, the more likely you are to be terrified that they're running elections."

[NY Times; January 2008]

Leading Critics

- David Dill, Stanford: http://www.verifiedvotingfoundation.org/
- Matt Bishop, UC Davis http://evote.cs.ucdavis.edu/
- Ed Felten http://itpolicy.princeton.edu/voting/

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?
- Can a voting machine be secure if the voting process is corrupt?
- Ultimately, security is an end-to-end concern

[Note Anderson section 1.7]

Voting: Policies and Mechanisms

- 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)

Policy

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

Felten’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

Video

- http://itpolicy.princeton.edu/voting/videos.html

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)

Facets of Security

- Confidentiality
  - Keeping secrets
- Integrity
  - Users trust the system
- Availability
  - The system must be ready when needed

Confidentiality

- Concealment of information or resources
- Government/Military: "Need to Know"
- Mechanisms:
  - Access Control

Integrity

- Trustworthiness of data or resources
- Data Integrity
  - Integrity of content (the vote talleys add up)
- Origin Integrity
  - Source of data is known (each vote was cast by a voter)
- 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

Trust

- Every time I drive I trust the brake system on my car
- Before I drive, I do not systematically check the brake system in any way
  - The brake system is a “trusted component” of my car
    - The safety of my operation of the car assumes the brake system is functioning correctly
  - In contrast, I inspect the brakes on my bicycle before I ride and typically test them before I go down a hill

Trustworthy

- Are the brakes on my car “trustworthy”? I.e. is that trust justified?
  - Car is well maintained
  - Brake system “idiot light” is off
  - Brake system hydraulics meet modern standards for redundancy and independence
  - Independent “emergency brake” system is available if primary braking system fails

Trustworthy

- What about my bike brakes?
  - Bike is also well maintained
  - Front and Rear brake systems are independent
  - Simplicity of system affords reduction of "trust base" (the set of "trusted components" that I assume to work) to cables, rims, brake calipers, and pads (and structural integrity of bike, tires)

Threat environment

- Threats to my brakes:
  - Normal wear
  - Extraordinary wear due to maladjustment
  - Manufacturing defect
  - Corrosion and rust
  - Loss of integrity of other components
- How are these threats mitigated?

Malicious threats

- What if I’m worried about sabotage?

Prioritizing Threats

- "Security engineers … need to be able to put risks and threats in context, make realistic assessments of what might go wrong, and give our clients good advice. That depends on a wide understanding of what worked, what their consequences were, and how they were stopped (if it was worthwhile to do so)."

  Ross Anderson, Section 1.2

Definitions

- Trust: a relationship, typically with respect to a property
  - I trust the brake cables on my bike
  - My integrity depends upon the integrity of my bike brakes
  - The fact that I trust something does not make it trustworthy!
- Trusted component: one whose failure can break the property (security policy)
  - Frame, wheelset, cables, tires, brake mechanism

Definitions

- Trustworthy: an attribute of an object
  - Is the object worthy of trust?

Definitions

- Trusted Base: A set of components that are trusted as an assumption
- Trusted Computing Base (TCB): the set of components in a computer system (including hardware and software) that are assumed to work as part of a security analysis

Example

- The TCB often includes
  - Correct function of the hardware (CPU and memory)
  - The low level boot code
  - The operating system (or at least parts of the operating system)
- Exercise
  - As you read the Princeton paper, consider what the TCB of the Diebold machine actually is
  - Could you make it smaller?

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

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

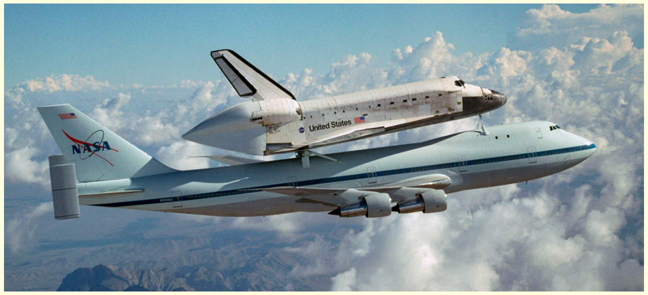
- How little can we trust?
- If we trust the processor do we have to trust the boot loader?
- Can we verify that we have the expected operating system before executing it?

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?

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"

- “Only amateurs attack machines; professionals target people”
  - Bruce Schneier (Quoted by Anderson)

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

Pretexting

- This summer I got a request for a telephone recommendation from someone claiming to want to employ a student
- I sent the student a note requesting a FERPA waiver so I could grant the request
- The student was not applying for any jobs
- A decade ago I would have responded without hesitation

Pretexting

- Examples?
- Countermeasures?
- Is it a technology problem?

Phishing

- Started in 2003, targeting banks
- Has increased in sophistication
- Share anecdotes
  - "Spear phishing"
  - Phishing in information warfare

Psychology Research

- Cognitive psychology and the Human-Computer Interaction (HCI) research community know a lot about how well people perform tasks
- These principles are used to design and evaluate airplane cockpits
- They are routinely applied in mature engineering disciplines
- In practice are these principles applied in the design of computer systems?

Human errors

- A practiced actions is performed instead of an intended one
  - Drive home, skipping store
  - Click “ok” too many times
  - Post-completion error
- When following rules, may follow the wrong rule
  - URL starts https: means things are secure
- Cognitive failure to understand the problem
  - Victim of a “picture in picture” attack

Gender bias

- Gender HCI
- Burnett and colleagues at OSU
  - Women tinker less, but more effectively
  - Issues:
    - Low self-esteem
    - Risk aversion
- "Is it unlawful sex discrimination for a bank to expect its customers to detect phishing attacks by parsing URLs?" -- Anderson

Passwords

- "One of the biggest practical problems facing security engineers today"
- The problem:
  - Authentication
- Solutions:
  - Something you have
  - Something you know
  - Something you are

Password Issues

- Reliable password entry
- Difficulty remembering
- Naïve Choice

Passwords

- Train users to choose good passwords
- Anderson study:
  - Red: usual (six characters, one number)
  - Green: passphrase to give string
  - Yellow: Random from table
- Results
  - Red and Green remembered
  - Green and Yellow were hard to crack

Recommendation: Green

Passwords

- Social engineering
  - Very senior manager's administrative assistant

Model good behavior

- PSU emergency email vendor sends mail that looks like phish
  - Return address in mailto doesn't match displayed address
  - Comes from an unknown domain
- This trains users to engage in dangerous behavior
- Makes it easier to harvest passwords from "webmail" spear phishing attack later in year

Two factor authentication

- Challenge response boxes
- Something you have
- Can we use cell phones?
  - Two –channel authentication
  - Some vulnerability to man-in-the-middle
  - Can be eliminated with redundant entry of key data (such as transaction amount)
  - Problematic as a UI issue

Conclusions

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

Next Lecture

- Format:
  - Next lecture will begin with a discussion section on the reading
  - Please be prepared to participate in the discussion
  - I will supply name tags
  - I will call on individuals

Next Lecture

- Voting Case Study
- Reading:
  - Voting Discussion:
    - NY Times article on voting
    - Felten paper on Diebold voting machines
    - Anderson, Section 23.5 [Bleeding edge: Elections]
    - Freedom to Tinker blog on voting