CS 591: Introduction to Computer Security

Lecture 1: Overview

James Hook

1/10/12 14:03

Course Mechanics

- Course web page:
  - http://web.cecs.pdx.edu/~hook/cs491w12/index.html
- Contains:
  - Instructor contact information
  - Term paper handout
  - Grading guidelines
  - Topics and Reading Assignments for each lecture
  - Links to lecture notes

1/10/12 14:03

Class Format

- "Don't Lecture Me"
  - Plan to try more question-focused peer-teaching
  - Expect to discuss reading in class in small and large groups
  - Some discussion questions may be taken from the guide. In some cases I will share questions or specific optics of interest in advance
  - This is an experiment for me; feedback is appreciated

1/10/12

Texts

- Anderson
  - Sometimes anecdotal; a good read
  - Second edition (1/2008) is significant revision
  - 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

1/10/12 14:03

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

1/10/12 14:03

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.

1/10/12 14:04

Term Paper

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

1/10/12 14:04

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

1/10/12 14:04

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
  - I have collected past exam questions and study questions into a "guide" organized by lecture topic
  - Please consult these for continuous self-assessment and midterm exam preparation
- Final will cover second half of the class
  - The final exam will be comprehensive
  - It will also 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

Class Mailing List

- Please sign up for the class mailing list

1/10/12 14:04

NY Times: 17 Oct 2011

- **U.S. Debated Cyberwarfare in Attack Plan on Libya**
- **By ERIC SCHMITT and THOM SHANKER**
- WASHINGTON — Just before the American-led strikes against Libya in March, the Obama administration intensely debated whether to open the mission with a new kind of warfare: a cyberoffensive to disrupt and even disable the Qaddafi government's air-defense system, which threatened allied warplanes.
- While the exact techniques under consideration remain classified, the goal would have been to break through the firewalls of the Libyan government's computer networks to sever military communications links and prevent the early-warning radars from gathering information and relaying it to missile batteries aiming at NATO warplanes.

1/10/12

Schmitt, Shanker; NYT; 17 Oct 2011

- But administration officials and even some military officers balked, fearing that it might set a precedent for other nations, in particular Russia or China, to carry out such offensives of their own, and questioning whether the attack could be mounted on such short notice. They were also unable to resolve whether the president had the power to proceed with such an attack without informing Congress.
- In the end, American officials rejected cyberwarfare and used conventional aircraft, cruise missiles and drones to strike the Libyan air-defense missiles and radars used by Col. Muammar el-Qaddafi's government.

1/10/12

Schmitt, Shanker; NYT; 17 Oct 2011

- This previously undisclosed debate among a small circle of advisers demonstrates that cyberoffensives are a growing form of warfare. The question the United States faces is whether and when to cross the threshold into overt cyberattacks.
- Last year, a Stuxnet computer worm apparently wiped out a part of Iran's nuclear centrifuges and delayed its ability to produce nuclear fuel. Although no entity has acknowledged being the source of the poisonous code, some evidence suggests that the virus was an American-Israeli project. And the Pentagon and military contractors regularly repel attacks on their computer networks — many coming from China and Russia.

1/10/12

Schmitt, Shanker; NYT; 17 Oct 2011

- "These cybercapabilities are still like the Ferrari that you keep in the garage and only take out for the big race and not just for a run around town, unless nothing else can get you there," said one Obama administration official briefed on the discussions.

1/10/12

Schmitt, Shanker; NYT; 17 Oct 2011

- In the days ahead of the American-led airstrikes to take down Libya's integrated air-defense system, a more serious debate considered the military effectiveness — and potential legal complications — of using cyberattacks to blind Libyan radars and missiles.
- "They were seriously considered because they could cripple Libya's air defense and lower the risk to pilots, but it just didn't pan out," said a senior Defense Department official.
- After a discussion described as thorough and never vituperative, the cyberwarfare proposals were rejected before they reached the senior political levels of the White House.

1/10/12

Stuxnet
NYT; 11 February 2011

- **Malware Aimed at Iran Hit Five Sites, Report Says**
- **By JOHN MARKOFF**
- The Stuxnet software worm repeatedly sought to infect five industrial facilities in Iran over a 10-month period, a new report says, in what could be a clue into how it might have infected the Iranian uranium enrichment complex at Natanz.
- The report, released Friday by Symantec, a computer security software firm, said there were three waves of attacks. Liam O Murchu, a security researcher at the firm, said his team was able to chart the path of the infection because of an unusual feature of the malware: Stuxnet recorded information on the location and type of each computer it infected.

1/10/12

- The Symantec researchers also said they had determined that the malware program carried two different attack modules aimed at different centrifuge arrays, but that one of them had been disabled.
- Stuxnet first infected Windows-based industrial control computers while it hunted for particular types of equipment made by the Siemens Corporation. It was programmed to then damage a uranium centrifuge array by repeatedly speeding it up, while at the same time hiding its attack from the control computers by sending false information to displays that monitored the system.

1/10/12

- The New York Times reported in January that Israel had built an elaborate test facility at a classified nuclear weapons site that contained a replica array of the Iranian uranium enrichment plant. Such a test site would have been necessary for the design of the attack software.
- "We know the exact configuration of the system they were looking for," Mr. O Murchu said. "We know they were looking for a certain number of frequency converters. And each of those frequency converters controls a certain number of motors. And those numbers fit in with what you expect to see in an uranium enrichment facility."

More on Stuxnet

- Wired:
  How Digital Detectives Deciphered Stuxnet, the Most Menacing Malware in History,
  by Kim Zetter
  - http://www.wired.com/threatlevel/2011/07/how-digital-detectives-deciphered-stuxnet/all/1
- Symantec: W32.Stuxnet Dossier
  - Version 1.4 (February 2011)
  - Nicolas Falliere, Liam O Murchu, and Eric Chien
  - http://www.symantec.com/connect/blogs/w32stuxnet-dossier

SCADA: Not just a computer

- Stuxnet targets Siemens Programmable Logic Controllers, an industrial control computer "widely used in … industrial plants and factories to regulate and operate machinery."
- Example of a "Supervisory Control and Data Acquisition" (SCADA) system
  - Dams; Power plants; Reactors; Power grid

SCADA evolved dangerously

- Initially assumed physical security of plant, no communication
- Programmed by domain engineers (not security engineers or computer scientists)
- Low level programming on vulnerable platforms
- Then:
  - add a modem (attack by phone)
  - replace a computer and accidentally add a wireless network (drive-by attack by wireless)
  - connect to the internet (attack from home!)

Stuxnet raises stakes

- Launched in 2009
- Creates a carrier infection on PC's using exploits in MS operating systems
- Jumps to the SCADA system by infecting a memory stick
- September 2010 hits popular press

Stuxnet

- Information warfare can create physical hazards, not "just" blue screens of death and user inconvenience
- What are the reasonable expectations of society about the state of our information infrastructure? Are we meeting those expectations as a discipline?

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]

1/10/12 14:07

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

1/10/12 14:07

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]

1/10/12 14:07

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."

1/10/12 14:08

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.)"

1/10/12 14:08

Touch Screen Voting Today

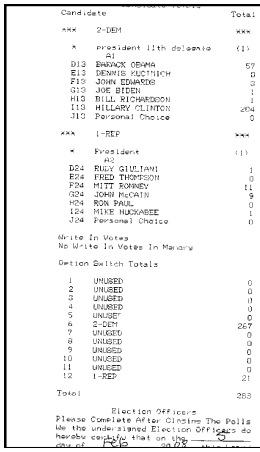
- Computers have not solved the problem
- There is still a crisis of confidence in voting
  - Search for "electronic voting machines" on google news.

1/10/12 14:08

New Jersey

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

1/10/12 14:08



Candidate	Total
*** 2-DEM	***
* President (1th delegate At)	(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 (1) At	(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		288

Election Officers
Please Complete After Closing The Polls
We the undersigned Election Officers do
hereby certify that on the 5th
day of Feb 2008

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/research/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

1/10/12 14:12

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]

1/10/12 14:03

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/

1/10/12 14:03

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]

1/10/12 14:03

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]

1/10/12 14:03

Leading Critics

- David Dill, Stanford: http://www.verifiedvotingfoundation.org/
- Matt Bishop, UC Davis http://nob.cs.ucdavis.edu/bishop/index.html
- Ed Felten and colleagues, Princeton, Center for Information Technology Policy, http://citp.princeton.edu/ https://freedom-to-tinker.com/tags/voting

1/10/12 14:13

Expectations of Voting

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

1/10/12 14:14

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]

1/10/12 14:14

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

1/10/12 14:14

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

1/10/12 14:14

Evaluating mechanisms

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

1/10/12 14:14

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

1/10/12 14:14

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

1/10/12 14:14

Video

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

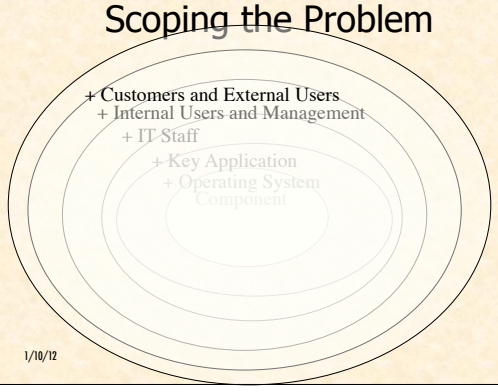
1/10/12 14:14

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, authentication)
- Survey common exploitable vulnerabilities (stack attacks, malware, bots)

1/10/12 14:14

Scoping the Problem



1/10/12

The Cast

- Subject
  - A real physical person
- Person
  - A physical or legal person (including corporations) [lawyer speak; unfortunate]
- Principal
  - An entity that participates in a security system

1/10/12

Conventions

- Principals are often named
  - Alice
  - Bob
  - Cherie
  - David
  - Eve
- (in alphabetical order; sometimes Eve is evil)

1/10/12

Vocabulary

- Identity
  - Correspondence between the names of two principals
- Group
  - Set of principals
- Role
  - set of functions assumed by different persons in succession ("incident commander", "officer of the watch")

1/10/12

Vocabulary (Anderson)

- Secrecy
  - Limit the principals who can access information
- Confidentiality
  - Obligation to protect some other person's secrets
- Privacy
  - Ability and/or right to protect your personal information and to prevent invasions of your personal space

1/10/12

Vocabulary (Bishop)

- 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

1/10/12 14:16

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)
- Future Exercise
  - As you read the Princeton paper, consider what the TCB of the Diebold machine actually is
  - Could you make it smaller?

1/10/12 14:16

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

1/10/12 14:16

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

1/10/12 14:17

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

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

- Format:
  - Next lecture will begin with a discussion section on the reading
  - Please be prepared to participate in the discussion

Next Lecture

- Voting Case Study and Access Control
- Reading:
  - Cyber Warfare articles
    - NY Times
  - Voting Discussion:
    - NY Times article on voting
  - Usability
    - Anderson, Chapter 2