Introduction
CS 136
Computer Security

Peter Reiher

January 5, 2021

Purpose of Class

- To introduce students to computer security issues
- To familiarize students with secure software development
- To learn to handle security in today’s installations and systems

Description of Class

- Topics to be covered
- Prerequisites
- Grading
- Reading materials
- Homework
- Office hours
- Web page

Topics to Be Covered

- Cryptography and authentication
  - Use, not design and analysis
- Access control and security models
- Secure software design and programming
- Secure protocols
- Network security – threats and countermeasures
- Operating systems security
- Security analysis and forensics
- Malware, common attacks, and important defenses
- Privacy
- Practical computer security defenses

Prerequisites

- CS111 (Operating Systems)
- CS118 (Computer Networks)
- Or equivalent classes elsewhere
- If you aren’t familiar with this material, you’ll be at a disadvantage
  - People have had serious problems with this unfamiliarity recently

Teaching Assistant

- Evan Czyzycki
  - eczy@cs.ucla.edu
- Weekly recitation sections Fridays
  - Section 1A: 12-1:50 AM
  - Via Zoom
  - Link to be announced

TA Duties

- Won’t cover new material in recitation sections
- Will help clarifying problems with lectures
- Will present information on using Deter testbed and performing labs
- Will also handle all other lab issues
- Office hours:
  - TBA

Grading

- Midterm – 25%
- Exercises – 36%
- Final – 38%
- Evaluation – 1%
- Grading will be done on this basis
  - Do not expect me to alter percentages for your particular case

How Do I Grade?

- Grades are assigned based on each student’s performance on all graded materials
- Your grade depends on how well you did compared to the rest of the class
- Not a formal curve
- But definitely NOT any guarantee that a particular percentage gets a particular letter grade
  - If someone’s told you there’s a “grade guarantee,” they’re wrong

Extra Credit

- Some of the exercises have possibilities for extra credit
- That’s the only extra credit available in the class
- If you blow off the midterm, I won’t offer you other extra credit possibilities

Class Format

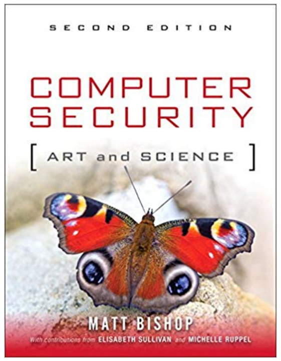
- A lecture class
- Questions and discussions always welcomed

Reading Materials

- Textbook
- Non-required supplemental text
- Links to papers and web pages

Textbook

- *Computer Security: Art and Science*
  - By Matt Bishop
- Second edition
  - Don’t get a used first edition
- Should be available in the book store


SECOND EDITION
COMPUTER SECURITY
[ART and SCIENCE]
MATT BISHOP
With Contributions from ELISABETH SULLIVAN and MICHELLE RUPPEL

Supplemental Text

- *Secrets and Lies*
  - By Bruce Schneier
- Not a textbook at all
- A philosophy of computer security
- Great for appreciating the field and problems
- Not great for depth of technical details
- Not required
  - No readings will be assigned from this book
  - But if you plan to work in this field, read it

Papers and Web Pages

- Mostly required reading material
  - Unless indicated otherwise
- Might or might not be assigned each week
- Made available electronically
  - Through class web page
- Generally relevant news stories or discussion of security topics

Exercises

- Five assignments
  - Plus a simple warmup
- Requiring practical work
- Performed on the Deter testbed
  - Accessible via the web from any connected location
  - Except exercise 5
- Individual, not group, assignments
  - Except exercise 5

Exercise Topics

0. Deter lab warmup
   - Week 1
1. Access control and permissions
   - Week 3
2. Exploits
   - Week 4
3. Analysis of attacks and forensics
   - Week 5
4. Man in the middle attacks
   - Week 7
5. Security analysis of a system
   - Week 10

More on Exercises

- Each exercise has an associated web page
  - With full instructions and pointers to necessary tools
- Due by midnight on indicated date
  - TAs may alter these dates
- Class TAs will provide advice and assistance on exercises

The Deter Testbed

- A set of machines devoted to security research and education
- Located at ISI and SRI
- Accessible remotely
- Special accounts set up for this class
- First discussion section will provide instructions on using Deter
  - With further assistance from TA

The Final Exercise

- A group exercise
  - Details of group composition to be provided
- Groups will perform a security evaluation of a piece of source code
- Resulting in a written report
- Full description provided later in the quarter

Tests

- Midterm – Tuesday, February 9
  - Via Zoom
- Final – Wednesday, March 17
  - Also via Zoom
- Open book/notes tests
- Students can take them during any time over a 24 hour period

Office Hours

- TTh 1-2
- Held via Zoom
  - Link will be provided in email
- Other times possible by appointment

Class Web Page

- On standard CCLE web site
- Slides for classes will be posted there
  - By 5 PM the previous afternoon
  - In Powerpoint and PDF
- Readings will be posted there
  - With links to web pages

A Few Words on Academic Honesty

- I expect all students to do their own work
  - Except on team projects
- I expect students not to cheat on tests
- All cases of suspected academic dishonesty will be reported to the Dean
  - Putting them out of my hands
- More details on class syllabus
- Or talk to me if in doubt

Introduction to Computer Security

- Why do we need computer security?
- What are our goals and what threatens them?

Why Is Security Necessary?

- Because people aren’t always nice
- Because a lot of money is handled by computers
- Because a lot of important information is handled by computers
- Because our society is increasingly dependent on correct operation of computers

History of the Security Problem

- In the beginning, there was no computer security problem
- Later, there was a problem, but nobody cared
- Now, there's a big problem and people care
  - Only a matter of time before a real disaster
  - At least one company went out of business due to a DDoS attack
  - Identity theft and phishing claim vast number of victims
  - Stuxnet seriously damaged Iran's nuclear capability
  - Video showed cyberattack causing an electric transformer to fail
  - There's an underground business in cyber thievery
  - Increased industry spending on cybersecurity

Some Examples of Large Scale Security Problems

- Malicious code attacks
- Distributed denial of service attacks
- Vulnerabilities in commonly used systems

Malicious Code Attacks

- Multiple new viruses, worms, botnets, and Trojan horses appear every week
- Cryptojacking of everything from servers to web cameras
  - To mine cryptocurrency
- Stuxnet worm targeted at nuclear facilities
  - Unspecified amounts of damage done to Iran’s nuclear program
- Increasing attacks on Internet of Things

Distributed Denial of Service Attacks

- Use large number of compromised machines to attack one target
  - By exploiting vulnerabilities
  - Or just generating lots of traffic
- Very common today
  - Major attack on Wikipedia in Europe and Middle East
  - 2018 attacks on online gaming companies
  - Attacks based on compromised Huawei routers
- In general form, an extremely hard problem

Vulnerabilities in Commonly Used Systems

- Recently, critical vulnerabilities in Android, Windows, iOS and macOS
- Many popular applications and middleware have vulnerabilities
  - Recent vulnerabilities in Webmin, Apache Solr, WordPress, Adobe Flash, Acrobat, Reader, etc.
- Many security systems have vulnerabilities
  - GlobalProtect Secure Socket Layer VPN, WPA3 Wifi security, Pulse Secure SSL VPN recently
- Critical hardware flaws in Intel and AMD processors
  - Fixes lead to slower processor

The SolarWinds Attack

- An extremely serious recent attack
- SolarWinds is a company that builds software to manage IT
- It was compromised and its Orion software corrupted
- Which then got deployed to its customers . . .

The Results of The Attack?

- The SolarWinds software controlled the customers' systems
- The corrupted version was controlled by the hackers
- So the hackers controlled the customers' systems

Who Were the Customers?

- US government agencies
  - Departments of Commerce,Treasury, Homeland Security, Energy
- Major corporations
  - Microsoft, Cisco, Intel, Nvidia, Deloitte LLC, VMWare, Belkin
- Computer security companies
  - Like FireEye (which discovered the problem)

Electronic Commerce Attacks

- As Willie Sutton said when asked why he robbed banks,
  - "Because that's where the money is"
- Increasingly, the money is on the Internet
- Criminals have followed
- Common problems:
  - Identity theft (phishing is a common method)
  - Loss of valuable data from laptop theft
  - Extortion via DDoS attacks or threatened release of confidential data
  - Cryptocurrency mining on compromised machines
- Ponemon Institute estimates average cost of a data breach is $3.9 million

Some Recent Statistics

- 2018 Verizon report found over 2200 data breaches from surveyed organizations
  - Two thirds of successful attacks only discovered months later
  - Health care organizations had ¼ of the breaches
- FBI Cybercrime report for 2017 showed over 300,000 reports
  - And losses of $1.4 billion
- Predictions (possibly inflated) of losses of $6 trillion worldwide in 2021

Cyberwarfare

- Nation states have developed capabilities to use computer networks for such purposes
- DDoS attacks on Estonia and Georgia
  - Probably just hackers
- Some regard Stuxnet as real cyberwarfare
  - Pretty clear it was done by US
- Attacks on Ukrainian power grid
- Continuous cyberspying by many nations
- Vulnerabilities of critical infrastructure
  - The smart grid increases the danger
- Russian election hacking in 2016

Something Else to Worry About

- Are some of the attempts to deal with cybersecurity damaging liberty?
- Does data mining for terrori s pose a threat to ordinary peopl
    - The NSA is looki . . .
  - And they aren't the only ones

Short answer: No.

- Can I trust Facebook/Google/Amazon/whoever with my private information?
- Are we in danger of losing all privacy?

Why Aren’t All Computer Systems Secure?

- Partly due to hard technical problems
- But also due to cost/benefit issues
- Security costs
- Security usually only pays off when there’s trouble
- Many users perceive no personal threat to themselves
  - “I don’t have anything valuable on my computer”
  - “I don’t have any secrets and I don’t care what the government/Google/my neighbor knows about me”
- Ignorance also plays a role
  - Increasing numbers of users are unsophisticated
  - Important that computer security professionals don’t regard this ignorance as a character flaw
  - It’s a fact of life we must deal with

Legacy and Retrofitting

- We are constrained by legacy issues
  - Core Internet design
  - Popular programming languages
  - Commercial operating systems
- All developed before security was a concern
  - With little or no attention to security
- Retrofitting security works poorly
  - Consider the history of patching

Problems With Patching

- Usually done under pressure
  - So generally quick and dirty
- Tends to deal with obvious and immediate problem
  - Not with underlying cause
- Hard (sometimes impossible) to get patch to everyone
- Since it's not organic security, patches sometimes introduce new security problems
  - E.g., Microsoft 2018 patch for Meltdown "allowed any process to read the complete memory contents at gigabytes per second"

Speed Is Increasingly Killing Us

- Attacks are developed more quickly
  - Often easier to adapt attack than defense
- Malware spreads faster
  - Verizon report shows 87% of attacks took minutes or less to succeed
- More attackers generating more attacks
  - US DoD computers received 36 million malicious emails **daily** in 2018

Some Important Definitions

- Security
- Protection
- Vulnerabilities
- Exploits
- Trust

Security and Protection

- *Security* is a policy
  - E.g., "no unauthorized user may access this file"
- *Protection* is a mechanism
  - E.g., "the system checks user identity against access permissions"
- Protection mechanisms implement security policies

Vulnerabilities and Exploits

- A *vulnerability* is a weakness that can allow an attacker to cause problems
  - Not all vulnerabilities can cause all problems
  - Most vulnerabilities are never exploited
- An *exploit* is an actual incident of taking advantage of a vulnerability
  - Allowing attacker to do something bad on some particular machine
  - Term also refers to the code or methodology used to take advantage of a vulnerability

Trust

- An extremely important security concept
- You do certain things for those you trust
- You don’t do them for those you don’t
- Seems simple, but . . .

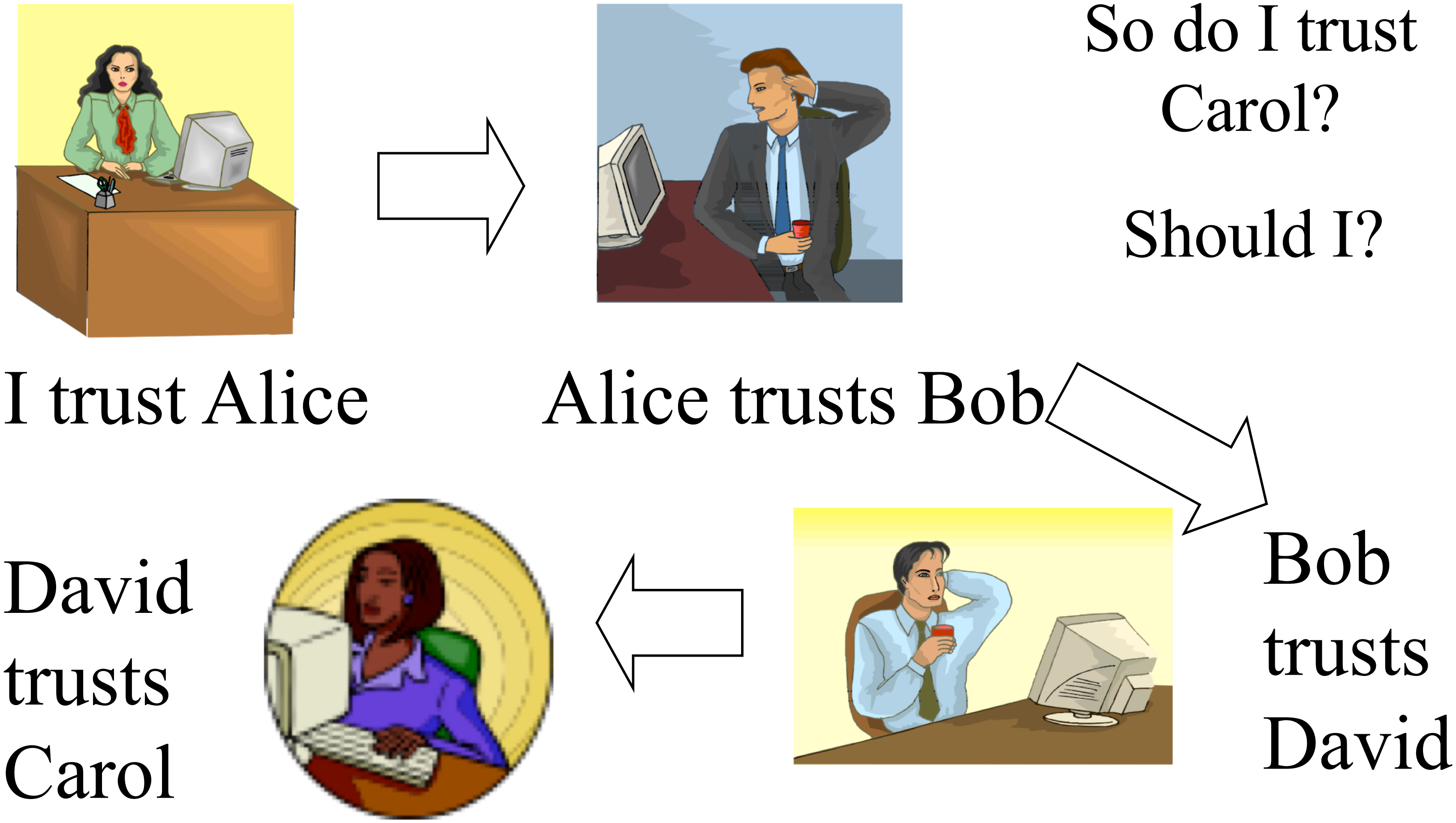
Problems With Trust

- How do you express trust?
- Why do you trust something?
- How can you be sure who you're dealing with?
- What if trust is situational?
- What if trust changes?

Trust Is Not a Theoretical Issue

- Most vulnerabilities that are actually exploited are based on trust problems
- Attackers exploit overly trusting elements of the computer
  - From the access control model to the actual human user
- Taking advantage of misplaced trust
- Such a ubiquitous problem that some aren't aware of its existence

Transitive Trust



I trust Alice

Alice trusts Bob

Bob trusts David

David trusts Carol

So do I trust Carol?

Should I?

Examples of Transitive Trust

- Trust systems in peer applications
- Chains of certificates
- But also less obvious things
  - Like a web server that calls a database
  - The database perhaps trusts the web server
  - But does the database necessarily trust the user who invoked the server?
- Programs that call programs that call programs are important cases of transitive trust
  - And this is how we build modern systems

What Are Our Security Goals?

- CIA
- **C**onfidentiality
  - If it’s supposed to be a secret, be careful who hears it
- **I**ntegrity
  - Don’t let someone change something they shouldn’t
- **A**vailability
  - Don’t let someone stop others from using services

What Are the Threats?

- Theft (of data)
- Privacy
- Destruction
- Interruption or interference with computer-controlled services
- Misuse of computer controlled services

Active Threats Vs. Passive Threats

- *Passive threats* are forms of eavesdropping
  - No modification, injections of requests, etc.
- *Active threats* are more aggressive
- Passive threats are mostly to secrecy
- Active threats are to all properties

Social Engineering and Security

- The best computer security practices are easily subverted by bad human practices
  - E.g., giving passwords out over the phone to anyone who asks
  - Or responding to bogus email with your credit card number
- Social engineering attacks tend to be cheap, easy, effective
- So all our work may be for naught

Social Engineering Example

- Phishing
- Attackers send plausible email requesting you to visit a web site
- To “update” your information
- Typically a bank, popular web site, etc.
- The attacker controls the site and uses it to obtain your credit card, SSN, etc.
- Likelihood of success based on attacker’s ability to convince the victim that he’s real
  - And that the victim had better go to the site or suffer dire consequences

How Popular is Phishing?

- ~200,000 unique phishing web sites per month in late 2020[1]
  - Targeting ~500 different brands
  - Around 120,000 unique phishing campaigns per month
- Based on gullibility of humans more than computer vulnerability
- But can computer scientists do something to help?

[1] http://www.antiphishing.org/

Why Isn’t Security Easy?

- Security is different than most other problems in CS
- The “universe” we’re working in is much more hostile
- Human opponents seek to outwit us
- Fundamentally, we want to share secrets in a controlled way
  - A classically hard problem in human relations

Three can keep a secret, if two of them are dead.

What Makes Security Hard?

- You have to get <u>everything</u> right
  - Any mistake is an opportunity for your opponent
- When was the last time you saw a computer system that did <u>everything</u> right?
- So, must we wait for bug-free software to achieve security?

How Common Are Software Security Flaws?

- SANS used to publish weekly compendium of newly discovered security flaws
- About 1500 security flaws found per year
  – Only counting popular software
  – Only flaws with real security implications
  – And only those that were publicized
- SANS stopped doing this because it's not reasonable to expect anyone to keep up

Security Is Actually Even Harder

- The computer itself isn't the only point of vulnerability
- If the computer security is good enough, the foe will attack:
  - The users
  - The programmers
  - The system administrators
  - Or something you never thought of

A Further Problem With Security

- Security costs
  - Computing resources
  - People’s time and attention
- If people use them badly, most security measures won’t do the job
- Security must work 100% effectively
- With 0% overhead or inconvenience or learning

Another Problem

- Most computer practitioners know little or nothing about security
- Few programmers understand secure programming practices
- Few sysadmins know much about secure system configuration
- Typical users know even less

The Principle of Easiest Penetration

- *An intruder must be expected to use any available means of penetration. This is not necessarily the most obvious means, nor is it necessarily the one against which the most solid defense has been installed.*
- Put another way,
  - The smart opponent attacks you where you’re weak, not where you’re strong
  - And most opponents aren’t stupid

But Sometimes Security Isn't That Hard

- The Principle of Adequate Protection:
  - *Computer items must be protected only until they lose their value. They must be protected to a degree consistent with their value.*
- So worthless things need little protection
- And things with timely value need only be protected for a while

Conclusion

- Security is important
- Security is hard
- A security expert’s work is never done
  - At least, not for very long
- Security is full-contact computer science
  - Probably the most adversarial area in CS
- Intensely interesting, intensely difficult, and “the problem” will never be solved