Computer Science 161: Computer Security

Nicholas Weaver

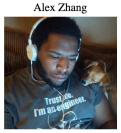
http://inst.eecs.berkeley.edu/~cs161/

And a team of talented TAs


Alex Zhang


Allen Wang


Cameron Rasmussen



Christopher Branner-Augmon


Joanna Yang


Kevyn


Xinhe (Jim) Ren


Nate Wang


Paul Legler


Samridh

What is security?

Enforcing a desired property ***in the presence of an attacker***

- data confidentiality
- user privacy
- data and computation integrity
- authentication
- availability
- …

Today's outline

- Why is security important?
- Course logistics
- Intro to security principles

Why is security important?

- It is important for our
  - physical safety
  - confidentiality/privacy
  - functionality
  - protecting our assets
  - successful business
  - a country's economy and safety
  - and so on…

Physical safety threats

Pacemaker hack can kill via laptop

By Jeremy Kirk, IDG News Service

Oct 21, 2012 11:44 AM

Business

FBI probe of alleged plane hack sparks worries over flight safety

Privacy/confidentiality

91% OF HEALTHCARE ORGANIZATIONS HAVE REPORTED A DATA BREACH IN THE LAST FIVE YEARS.

By elxradmin Posted May 29, 2015 In health IT, security

EVERYDAY MONEY IDENTITY THEFT

Data Breach Tracker: All the Major Companies That Have Been Hacked

Breaches in 2015 [ITRC]:
Number of breaches = 5,497
Number of Records = 818,004,561

Can affect a country's economy

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUNNI
UNPRECEDENTED
UKRAINE'S POWEI

too were nearing the end of their shift. But just as one worker was organizing papers at his desk that day, the cursor on his computer suddenly skittered across the screen of its own accord.

He watched as it navigated purposefully toward buttons controlling the circuit breakers at a substation in the region and then clicked on a box to open the breakers and take the substation offline. A dialogue window popped up on screen asking to confirm the action, and the operator stared dumbfounded as the cursor glided to the box and clicked to affirm. Somewhere in a region outside the city he knew that thousands of residents had just lost their lights and heaters.

And NotPetya...

- Someone (*cough* Russia *cough*) doesn't like Ukraine...
- They compromised the update channel for MeDoc
  - Think "TurboTax For Business in Ukraine":
    One of only two accounting packages which businesses can use to pay taxes
- They then monitored for weeks with their backdoor
  - This gave them a foothold in almost all who have Ukranian business
- Then they released a malicious "worm"
  - A program which self-propagates: spreads from computer to computer in an institution
  - And then disabled all the infected computers with a fake "ransomware" payload
    - This cost Mersk shipping alone ***$100M-300M*** in lost revenue!

What is hackable?

- Everything!
- Especially things connected to the Internet

For The First Time, Hackers Have Used A Refrigerator To Attack Businesses

JULIE BORT
Jan. 16, 2014, 1:36 PM 195,469 39

Course structure

- Intro to security
  - memory safety, OS principles
- Cryptography
- Network Security
- Web Security
- Miscellaneous topics

What Will You Learn In This Class?

- How to ***think adversarially*** about computer systems
- How to ***assess threats*** for their significance
- How to build programs & systems with ***robust security properties***
  - If I find out you start a new project in C or C++, or use unescaped SQL, or allow your web site to support CRSF attacks...
    MY SPIRIT WILL REACH THROUGH YOUR MONITOR AND STRANGLE YOU!!!!
- How to gauge the protections and limitations provided by today's technology
- How attacks work ***in practice***
  - Code injection, logic errors, browser & web server vulnerabilities, network threats, social engineering (because there is no patch for humans)

What's Required?

- Prerequisites:
  - CS 61B, 61C, 70
  - Familiarity with Unix, C, Java, Python
  - A willingness to ***get your hands dirty***
- Engage!
  - In lectures, in section
  - Feedback is highly valuable
- Class accounts – see course home page
- Participate in Piazza (use same name as glookup)
  - Send course-related questions/comments there, or ask in Prof/TA office hours
    - For private matters, contact Prof or TA using Piazza direct message
  - ***Do not post publicly about specifics about problems/projects***

Grading structure

- Absorb material presented in lectures and section
  - **Please attend lecture!**
- 3 course projects (24% total)
  - Done individually or in groups of 2
- 3-5 homework (16% total)
  - Done individually
- Two midterms (30%)
- A comprehensive final exam (30%)

Class Policies

- Late homework: no credit
- Late project: <24 hours: -10%, <48 hours: -20%, <72 hours: -40%, ≥72 hours: no credit
- Never share solutions, code, etc or let other students see them. Work on your own unless it is a group assignment
- Don't use our slides to answer questions during class
- Sign up for a class account
- Participate in Piazza
  - Email doesn't scale: course related questions/comments should be on Piazza or asked during office hours
  - There is also an ***unofficial*** slack channel that I will lurk on
- If you need DSP accommodations (extra time on exams, etc) process them ***now***

A Note on Nick's Office Hours...

- I am here because I ***love this job***
  - It is the students at Cal that make this worth doing
- I will often be in my (not quite a dungeon) 329 Soda Hall office outside my normal office hours
  - Other times I'll be at ICSI, 1947 center street, 6th floor...
- Feel free to drop by, ask questions, or just shoot the breeze
  - If you want to be sure I'm in, just drop me an email
  - Don't be afraid of the Slytherin house rug under my desk...
- And for gosh's sake, don't call me "Professor" or "Dr Weaver": My name is Nick

Textbooks

- No required textbook. If you want additional reading
- ***Optional:*** *Introduction to Computer Security,* Goodrich & Tamassia
- ***Optional:*** *The Craft of System Security,* Smith & Marchesini
- We will also make available interesting readings online

Intellectual Honesty Policy: Detection and ***Retribution***

- We view those who would cheat as "attackers"
  - This includes sharing code on homework or projects, midterms, finals, etc…
  - But through this class we (mostly) assume rational attackers
    - Benefit of attack > ***Expected*** cost of the attack
      - Cost of launching attack + cost of getting caught * probability of getting caught
- We take a detection and response approach
  - We use many tools to detect violations
    - "Obscurity is not security", but obscurity can help. Just let it be known that "We Have Ways"
  - We will go to DEFCON 1 (aka "launch the nukes") ***immediately***
    - "Nick doesn't make threats. ***He keeps promises***"

Ethics Guide for Defense Against the Dark Arts

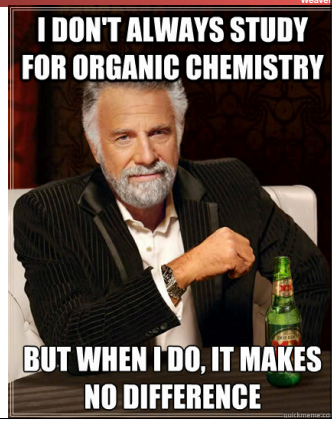
- Of necessity, this class has a fair amount of "dark arts" content
  - As defenders you must understand the offense: You can't learn defense against the dark arts without including the dark arts
  - But a lot of "don't try this at home" stuff
- Big key is ***consent***
  - Its usually OK to break into ***your own stuff*** (modulo the DMCA)
    - Its a great way to evaluate systems
  - Its usually OK to break into someone else's stuff ***with explicit permission to do so***
  - It is both grossly unethical and often ***exceedingly criminal*** to access systems without authorization

Also...

- There exists a classic game theory problem called the Prisoner's Dilemma
- For single-round Prisoner's Dilemma, the optimum strategy is "always-defect"
- For multi-round Prisoner's Dilemma, the optimum strategy in practice is "tit-for-tat"
  - AKA, be nice unless someone isn't nice to you
- Life is ***multi-round***: so be excellent to each other!
  - Making things hostile for others makes the world worse for all
  - Stopping things from being hostile to others makes the world better for you

Stress Management & Mental Health...

- We'll try to not over-stress you too much
  - But there really is a lot to cover and this really is a demanding major
- We are going to somewhat front-load the 3 projects
  - Since everybody else has stuff due at the very end
- If you feel overwhelmed, please use the resources available
  - Academically: Ask on Piazza, Slack, Tutoring, Office hours
  - Non-Academic: Take advantage of University Health Services if you need to
    - ***I did!*** Zoloft (an antidepressant) and therapy saved my life, twice
- Failure is always an option
  - If something bad happens near the end of the semester, there are withdrawals and incompletes.
  - It is OK to fail or just barely pass...
    My grades as a Berkeley Undergrad included a B- in Physics 111BSC & Thermodynamics, a C+ in Chem 112A (O-chem), and a C in Physics 137A (Quantum)...



Webcasts? Yes

- Benefits of webcasts:
  - Allows students to catch up on lecture at some other time
  - Allows me to oversubscribe the class
  - ~~Allows sharing the lecture with a larger community~~
    - This ***would*** be a benefit, but the University won't pay for human-done captions, while YouTube's automatic captions will get the University sued for violating the ADA!
- Costs of webcasts:
  - Students may not attend class because "hey, webcast"
    - It hurts my ego to lecture to an empty classroom. 😭
    - But webcast has less context, you can't ask questions, etc etc etc
  - I have occasional outbursts of profanity
- But we're doing it.

Some Philosophy

- The rest of this lecture is largely focused on philosophical issues
- People and Money
- Threat Model
- Prevention, Detection & Response, Mitigation and Recovery
- False Positives, False Negatives, and Compositions
- And then some real word security tips

It All Comes Down To People... The Attacker(s)

- People attack systems for some reason
  - No attackers? No problem!
- They may do it for money
- They may do it for politics
- They may do it for the lulz
- They may just want to watch the world burn
- Often the most effective security is to attack the ***reasons*** for an attacker
  - "We are sick of playing whak-a-mole on bad guys...
    Instead we play whak-a-mole on bad-guy business models"

Personal Security: Threat Model and Chill...

- Who and why might someone attack ***you***?
- Criminals for money
- Teenagers for laughs or to win in an online game
- Governments
  - Probably not: We aren't important enough
  - And even if important enough we're only worth the B game: aka the same things used against criminals
- Intimate partners
  - A surprisingly powerful and dangerous adversary, often neglected in the security world

Beware the Intimate Partner Threat

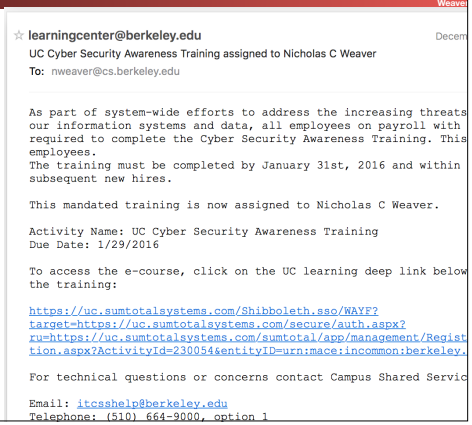
- The IPT is probably the most dangerous attacker you can reasonably expect to face
  - Lives are on the line in these situations
- IPTs have physical access
  - Turn your phone into a bug and location tracker: its easy if your phone is in their hands...
- IPTs have intimate knowledge and strong social engineering
  - I had a colleague who's ex broke into his Facebook account: by abusing the 3-friends password reset option
- IPTs are often motivated to target a particular person
  - No longer a security "bear race"

It All Comes Down to People... The Users

- If a security system is unusable it will be ur
  - Or at least so greatly resented that users will actively a to subvert it: "Let's set the nuclear launch code to 00000000" (oh, and write down the password anyway!)
- Users will subvert systems anyway
- Programmers will make mistakes
  - And mistakes are tied to the tools they use
  - "If you don't loath C and C++ by the time this class is over we have failed"
- And Social Engineering...
  - "Because there is no patch for Human Stupidity"

But Don't Blame The Users...

- Often we blame the user when an attacker takes advantage of them...
  - Yet we've consistently constructed systems that encourage users to do the wrong thing!
- Phishing is a classic example:
  - Which is a phishing email and which is an actual email from Chase?



☆ learningcenter@berkeley.edu Decem

UC Cyber Security Awareness Training assigned to Nicholas C Weaver

To: nweaver@cs.berkeley.edu

As part of system-wide efforts to address the increasing threats our information systems and data, all employees on payroll with required to complete the Cyber Security Awareness Training. This employees.
The training must be completed by January 31st, 2016 and within subsequent new hires.

This mandated training is now assigned to Nicholas C Weaver.

Activity Name: UC Cyber Security Awareness Training
Due Date: 1/29/2016

To access the e-course, click on the UC learning deep link below the training:

https://uc.sumtotalsystems.com/Shibboleth.sso/WAYF?target=https://uc.sumtotalsystems.com/secure/auth.aspx?ru=https://uc.sumtotalsystems.com/sumtotal/app/management/Registration.aspx?ActivityId=230054&entityID=urn:mace:incommon:berkeley.

For technical questions or concerns contact Campus Shared Servic

Email: itcsshelp@berkeley.edu
Telephone: (510) 664-9000, option 1

Oh, and it comes down to money too...

- "You don't put a $10 lock on a $1 rock...
  - Unless the attacker can ***leverage*** that $1 rock to attack something more important
- "You don't risk exposing a $1M zero-day on a nobody"
  - So I'm quite content to use my iPhone in a hostile environment: free market cost of a zero-day (unknown/unpatchable) exploit for iOS is somewhere between $500k to $1.5M
- Cost/benefit analyses appear all throughout security

Prevention

- The goal of prevention is to stop the "bad thing" from happening at all
- On one hand, if prevention works its great
  - E.g. if you don't write in an unsafe language (like C) you will ***never*** worry about buffer overflow exploits
- On the other hand, if you can ***only*** depend on prevention...
  - You get Bitcoin and Bitcoin thefts
  - E.g. $68M stolen from a Bitcoin exchange
  - Or Ethereum's July: four separate multi-million-dollar theft incidents
  - Or Coinbase accounts: Averaging a ***known*** theft a day!

Detection & Response

- Detection: See that something is going wrong
- Response: Actually ***do*** something about it
  - Without some response, what is the point of detecting something being wrong?

Burglar Alarms Cops Won't Answer

Jacquie Simms, left, leader of the Watts neighborhood council, and fellow Watts residents Milton Smith and his wife, Berneice, are seen outside the Smith's home, which is equipped with a burglar alarm, in Los Angeles, Friday, Feb. 7, 2003. AP

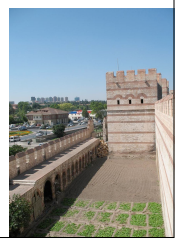
Comment / Share / Tweet / Stumble / Email

False Positive and False Negatives

- False positive:
  - You alert when there is nothing there
- False negative:
  - You fail to alert when something is there
- This is the real cost of detection:
  - Responding to false positives ***is not free***
    - And too many false positives and alarms get removed
  - False negatives mean a failure

Defense in Depth

- The notion of layering multiple types of protection together
  - EG, the Theodesian Walls of Constantinople:
    Moat -> wall -> depression -> even bigger wall
    - And some towers to rain down flaming and pointy death on those caught up in the defenses
- Hypothesis is that attacker needs to breech all the defenses
  - At least until something comes along to make the defense irrelevant like, oh, say siege cannons
- But defense in depth isn't free:
  - You are throwing more resources at the problem
  - You can have a increased false positive rate:
    If D1 has rate FP1 and D2 has rate FP2,
    a composition where either can alert has:
    FP = FP1 + (1-FP1) * FP2

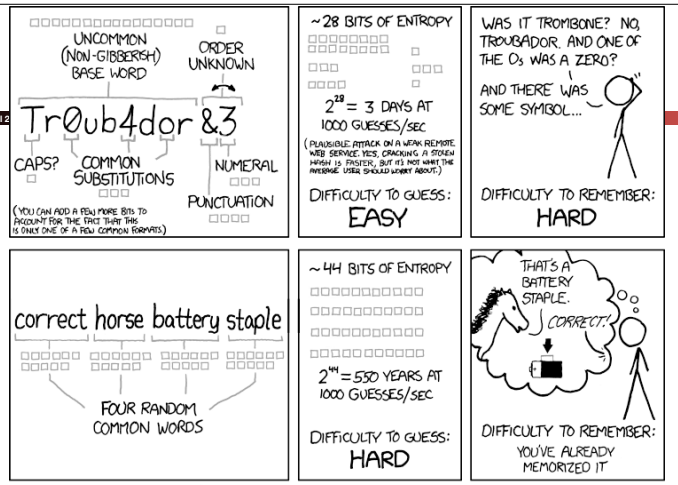


Mitigation & Recovery...

- OK, something bad happened...
  - Now what?
- Assumption: bad things ***will*** happen in the system
  - So can we design things so we can get back working?
- So how do I plan for earthquakes?
  - "1 week of stay put and 50+ miles of get outta town"
- So how do I plan for ransomware?
  - "If my computer and house catches on fire, I have backups"

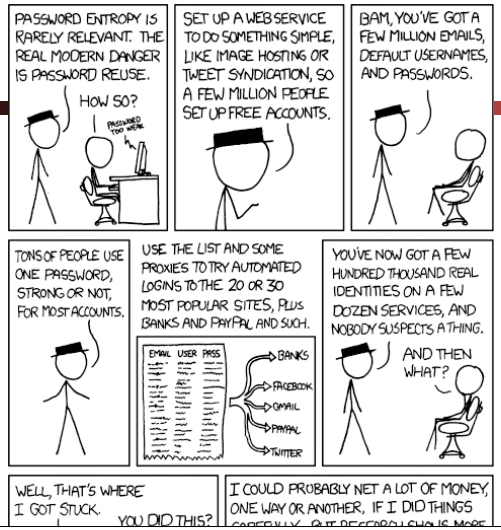
Real World Security...
How is your account breached?

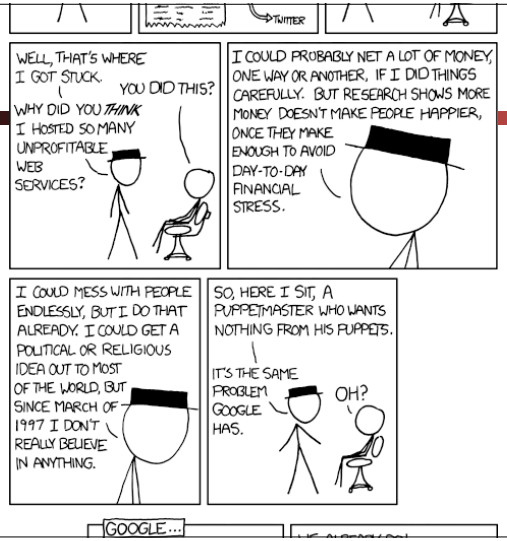
- Humans can't remember good passwords...
  - Well, we can remember a couple good passwords, but that's about it

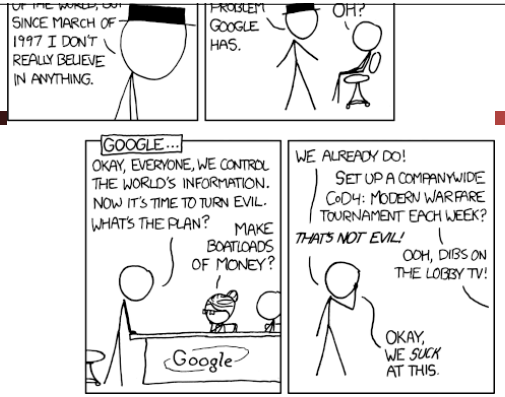


Real World Security...
How is your account breached?

- So we compensate with password ***reuse***
  - You use the same lame password on a large number of sites that ***hopefully*** don't matter
- One of those sites gets breeched...
  - And now the bad guy has your password
  - And can now log into all those other sites where you used the same password...







So what to do?
Password Managers

- A program which runs on your computer or phone
  - You enter a master password to unlock an encrypted store
  - It can then enter passwords for you in websites
  - It can also generate strong, unique, random passwords
- Often include cloud syncing as well
  - So you ***better*** make sure your master password is good
  - But now means you have your master password everywhere
- Several options, I personally like 1password but there are others as well
  - EG, others like Keepass

1password

And Fido U2F Security Keys

- A very powerful second-factor for 2-factor authentication
  - Touch to cryptographically prove that you hold the key...
- We will use this as a case study when we get to cryptography...
- But takeaway for now: This ***can not be phished***:
  - The security key itself knows which site it is talking to through the browser:
    it knows the difference between www.google.com and www.g00gle.com