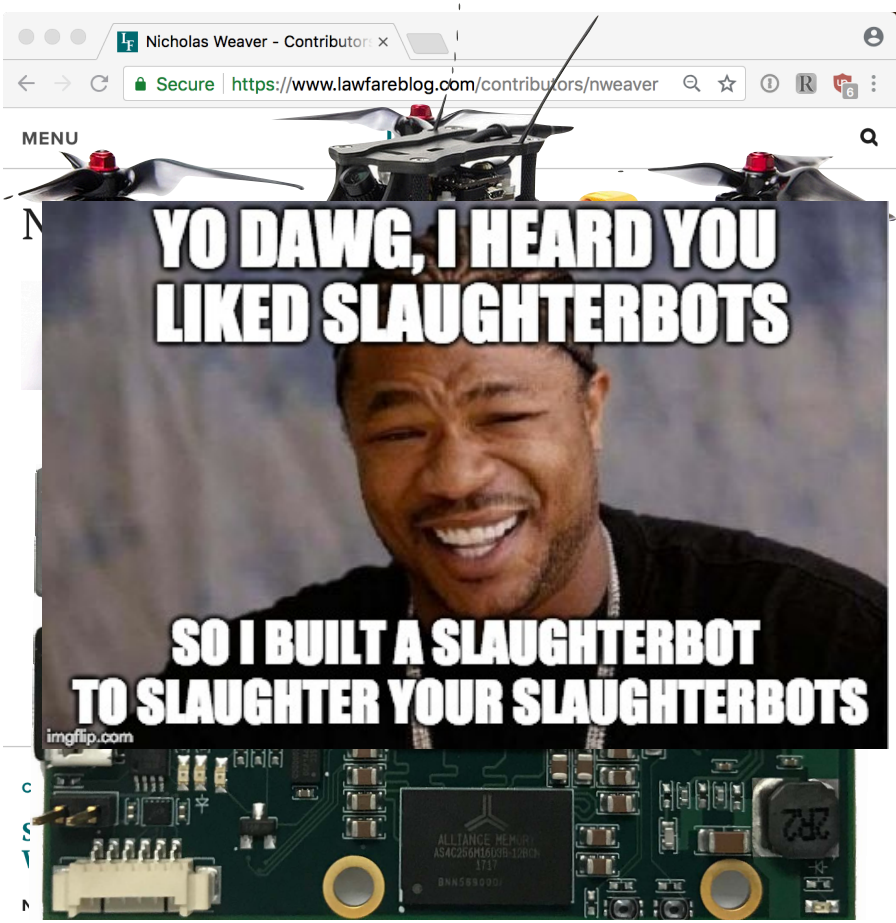
Computer Science 161: Computer Security

Nicholas Weaver

https://cs161.org

Who Am I?

- A ***lecturer*** in the CS department
  - + I am paid ***exclusively*** to care about my students & TA staff
- A researcher at the International Computer Science Institute
- Research focuses
  - Online criminality
    - Including cryptocurrency
  - Online privacy
  - Public policy
  - Drones...



And a team of talented TAs

(Head TA) Keyhan Vakil


Gustavo De Leon


Catherine Han

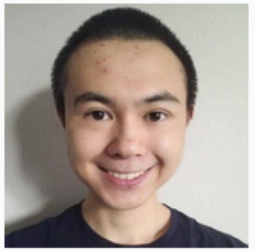

Ganesh Jaladanki


Matthew Jeng

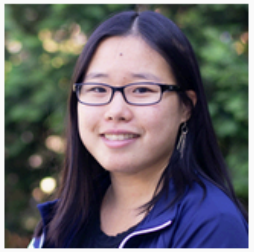

Spencer McCall


Sachit Shroff


Alex Stennet


Alex Thomas


Allen Tong


Karen Tu

Seung Jin Yang

What is security?

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

data confidentiality

user privacy

data and computation integrity

authentication

availability

…

Related ***but distinct*** from privacy engineering...

- Security is often about protecting data from unauthorized access
- Privacy is about making sure that the data is either not collected in the first place or, if collected, not misused

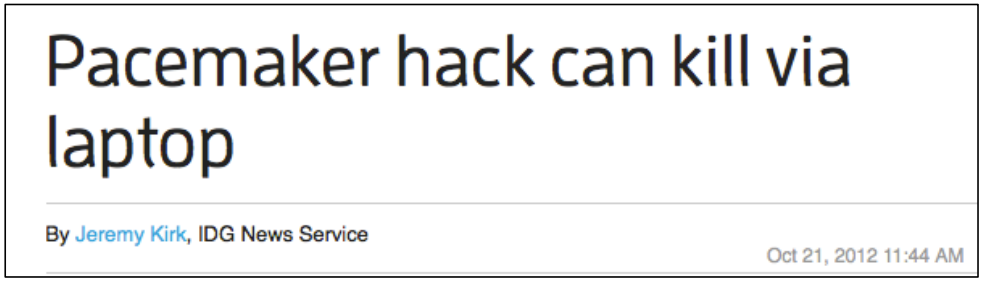
Today's outline

- Why is security important?
- Course logistics
- Security Principle: People

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 2018 [ITRC]:

- Number of breaches = 1200
- Number of Records = 450,000,000

Can affect a country's economy...
Multiple times!

KIM ZETTER SECURITY 03.03.16 7:00 AM

INSIDE THE CUN
UNPRECEDENTE
UKRAINE'S POW

A Cyber-Weapon Warhead Test

By **Nicholas Weaver** Wednesday, June 14, 2017, 11:38 AM

The *Daily Beast* has a story on "CrashOverride", a computer program best described as transient anti-infrastructure warhead designed to disrupt the power grid. It was tested live against a Ukrainian substation in December 2016 creating a small blackout. Kim Zetter has another good report at *Motherboard*, and Dragos has the technical details.

Dragos attributes the attack as conducted by "ELECTRUM", a group it assesses as being associated with Sandworm—an evaluation that is only slightly better than rolling attribution dice. It is probably more accurate to phrase the attribution as "probably Russia, and probably affiliated with the previous Ukrainian power grid attack in 2015." (The December 2016 attack was the second assault on the Ukranian

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! White House estimates report $10B! in damage!?!!!!

SECURITY 08.22.18 05:00 AM

THE UNTOLD STORY OF NOTPETYA, THE MOST DEVASTATING CYBERATTACK IN HISTORY

Crippled ports. Paralyzed corporations. Frozen government agencies. How a single piece of code crashed the world.

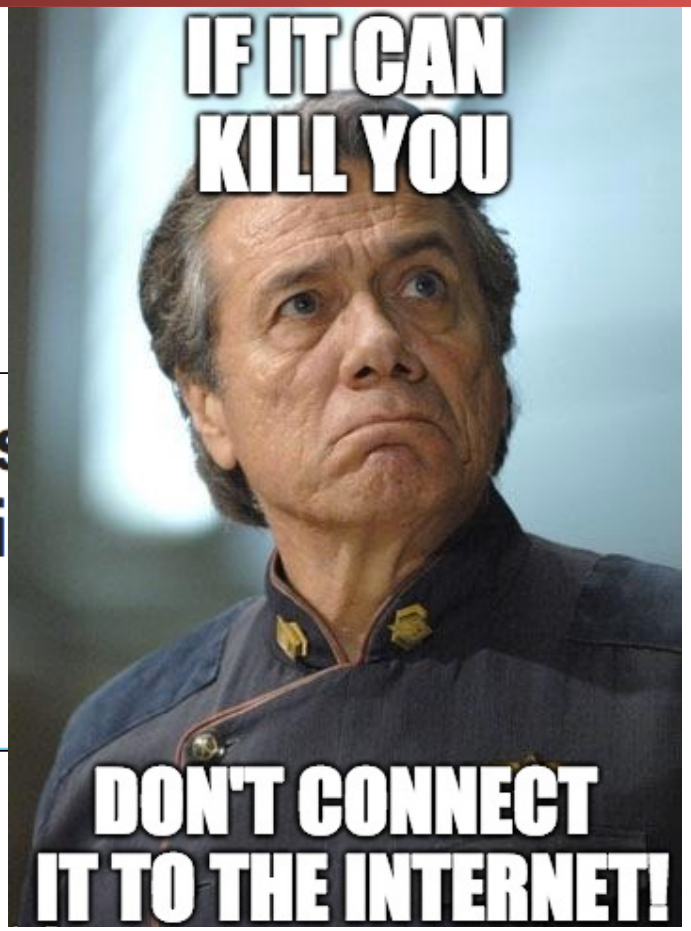
BY ANDY GREENBERG

IT WAS A perfect sunny summer afternoon in Copenhagen when the world's largest shipping conglomerate began to lose its mind.

The headquarters of A.P. Møller-Maersk sits beside the breezy

What is hackable?

- Everything!
- Especially things connected to the Internet



Course structure

- Intro to security
- Memory safety & OS principles
- Cryptography
- Web Security
- Network 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

What's Required?

- Prerequisites:
  - CS 61B, 61C, 70
    - If you haven't had 61C yet, go to the info session tonight and read "smashing the stack for fun and profit"
  - Familiarity with Unix, C, Java, Python and an ability to pick up new languages quickly
    - Project 2 will be in Go
  - A willingness to ***get your hands dirty: See "Homework 0" on Piazza***
- Engage!
  - In lectures, in section
  - Feedback is highly valuable
- Class accounts – see course home page
- Participate in Piazza (use same name as gradescope)
  - 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 and discussion!**
- 3-4 course projects (30% total)
  - Done individually or in groups of 2
- 3-5 homework (10% total)
  - Done individually
- Two midterms (30%)
- A comprehensive final exam (30%)
- A little bit (1%) of bonus points for Piazza participation
  - Will not be used in calculating the curve
- I grade to a curve and target the EECS department guidelines
  - Which says 3.0-3.5 GPA for the class, and I bias to the high side because this is a hard class

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
  - Its OK to talk however: Collaboration is important.
- 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
    And unless you have a particular reason, send to ***all instructors***, not just one

Missing Midterms and Final Policy...

- If you can't make a midterm because of a University event or Academic conference
  - Arrange ***now*** in the "accommodations" Piazza folder so that we can have a remote proctor (University staff, staff of another university) to give you the exam at the same time remotely
- If you can't make a midterm or final because of another class having the exam at the same time
  - Arrange ***now*** to notify us in the accommodations Piazza folder as well. We will have a make-up exam ***immediately after*** the scheduled exam.
    If you can't make either, sorry, 🤷
- If you need DSP accommodations (extra time on exams, etc) or have exam conflicts process them ***now as well***

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 FFS, 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
- However, readings that are freely available and posted are ***required***

Discussion

- Attend any discussion section you want that isn't full
  - If it is, go to another one, there are lots
- We ***WILL NOT*** have discussion this week
- We are going to try to let everyone in
  - Concurrent Enrollment requests won't be processed until week 3 however

Online Resources & Accounts...

- We will use gradescope for homeworks, exams, and recording project grades
- We will use Piazza for class announcements etc...
- Webcasts should show up on bcourses
- We will use your class account (cs161-xxx) for various load balancing purposes and other tasks
  - So set up all these up ASAP!

Piazza and Gradescope…

- You should be auto-enrolled if you were in the class/on the waitlist on August 26th
  - Since I just downloaded the roster and did bulk add…
- If you aren't yet (e.g. late add, concurrent enrollment, etc…)
  - Piazza: piazza.com/berkeley/fall2019/cs161
  - Gradescope: Entry code 9B5R8B

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***
    - You will, ***at minimum***, receive negative points
    - “Nick doesn’t make threats. ***He keeps promises***”

Ethics Guide for Defense Against the Dark Arts

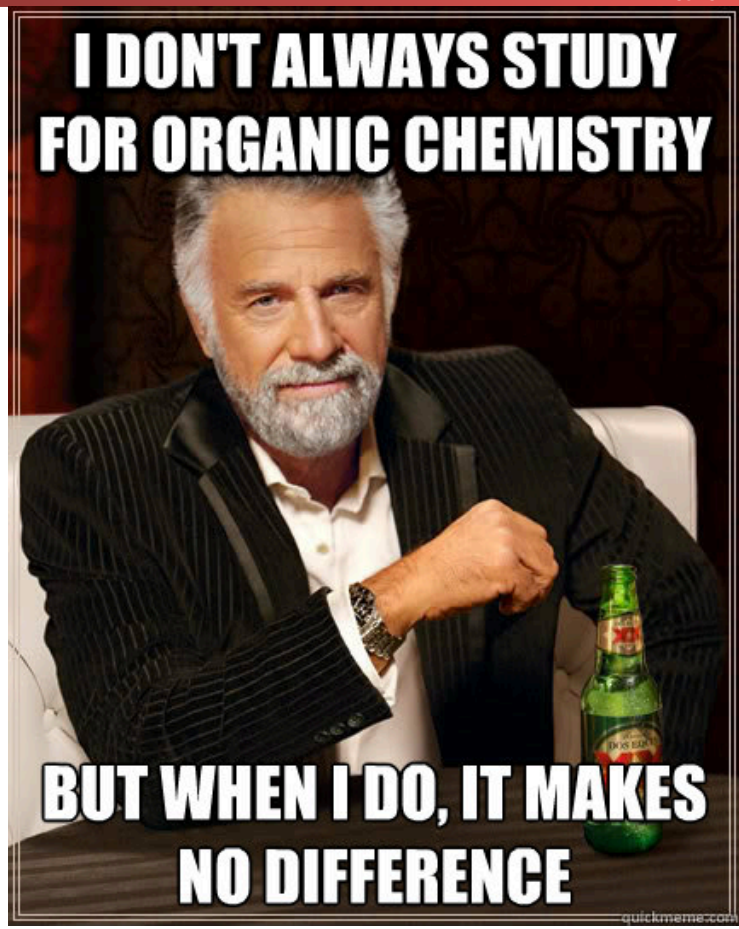
- Of necessity, this class has a fair amount of "dark arts" content
  - As defenders you must understand the offense:
    You can't learn defense against the dark arts without including the dark arts
  - But a lot of "don't try this at home" stuff
- Big key is ***consent***
  - Its usually OK to break 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'd like 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 projects
  - Since everybody else has stuff due at the very end, if there is a 4th it will be small
- 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)... Don't believe me? Stop by my office and see my transcript!



Webcasts?
Yes

- Benefits of webcasts:
  - Allows students to catch up on lecture at some other time
  - Allows me to oversubscribe the class: I intend to let ***everybody*** in!
  - ~~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!
    - If anyone has a significant hearing disability, please contact me. We may be able to get the DSP program to provide real captions so we can publish them
- 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

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"

The Parable of The Bear Race…

Personal Security:
Threat Model and Chill...

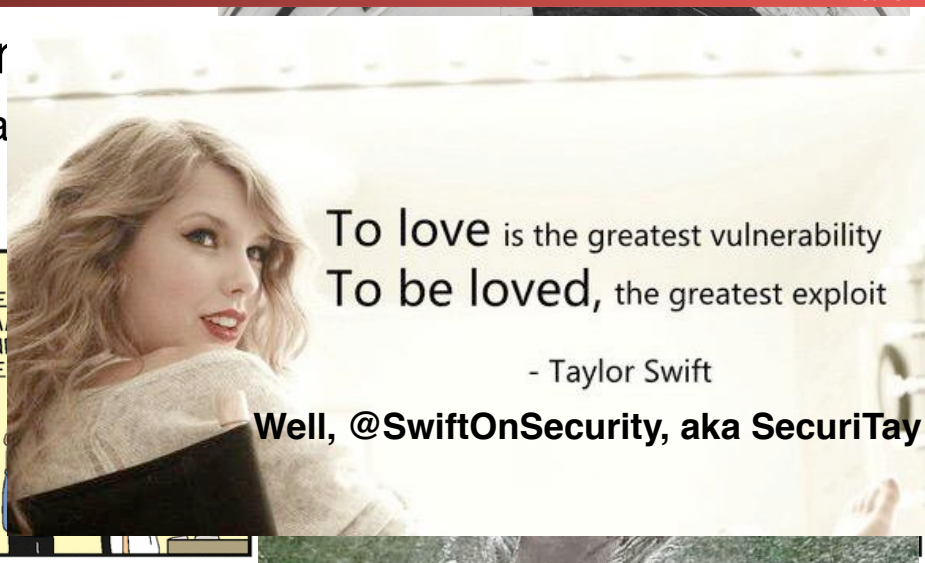
- Who and why might someone attack ***you***?
- Criminals for money
- Teenagers for laughs or to win in an online game
- Governments
  - Probably not: We aren't important enough
  - And even if important enough we're only worth the D game:
    aka the same things used against us by criminals
- Intimate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

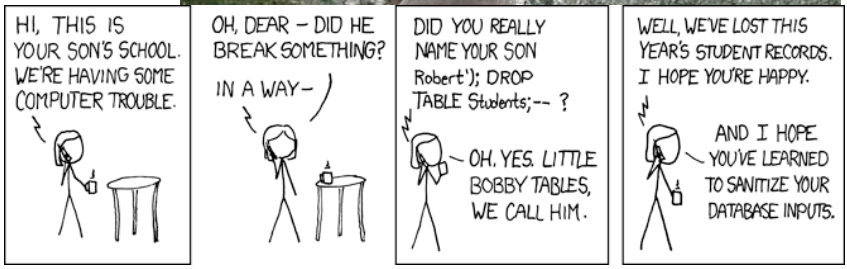
Beware the Intimate Partner Threat

- The IPT is probably the most dangerous attacker you or others 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 and they know the password...
- 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 "bear race"
- A good summary from Karen Levy
  https://slate.com/technology/2018/03/apps-cant-stop-exes-who-use-technology-for-stalking.html

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** Decemb

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 a
required to complete the Cyber Security Awareness Training. This
employees.
The training must be completed by January 31st, 2016 and within 6
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/Registr
tion.aspx?ActivityId=230054&entityID=urn:mace:incommon:berkeley.e

For technical questions or concerns contact Campus Shared Service

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