Computer Science 161: Computer Security

Raluca Ada Popa

David Wagner

http://cs161.org/

Who Am I:
David Wagner

- Professor working on computer security
- I've worked on software security, mobile security, cryptography, security of electronic voting, usable security, system security
- Currently I'm excited about security for machine learning

Who Am I:
Raluca Ada Popa

- Assistant professor in computer security
- Lead the system security research group, and co-run RISELab at UC Berkeley
- Research topics: **broadly** systems security and applied cryptography, and **more specifically**: secure analytics, databases, IoT and ML; decentralized security via blockchains/ledgers
- CTO & co-founder of a cybersecurity company, PreVeil
- Taught this class 3 times

And a team of talented TAs


(Head TA) Catherine Han


Allen Tong


Andrew Law


Peyrin Kao


Sachit Shroff


Seung Jin Yang

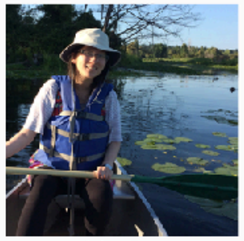

Cathy Lu


Eric Feng


Evan Corriere


Toby Chen


Victor Chan


Vivian Fang


Jason Li XiangJun


Keahooi Hung


Nicholas Ward

What is security?

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

data confidentiality

user privacy

data and computation integrity

authentication

availability

…

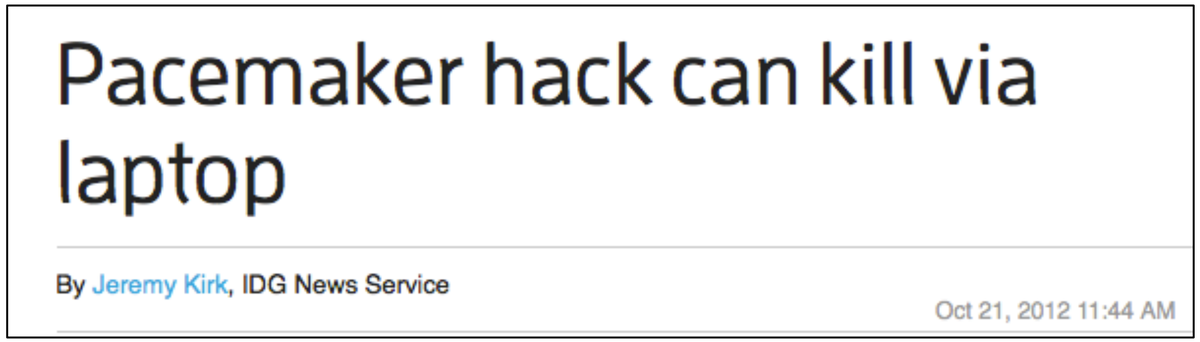
Today's outline

- 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... 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

een ion he en to nat ers.

And It Is National Security!

THE WALL STREET JOURNAL.

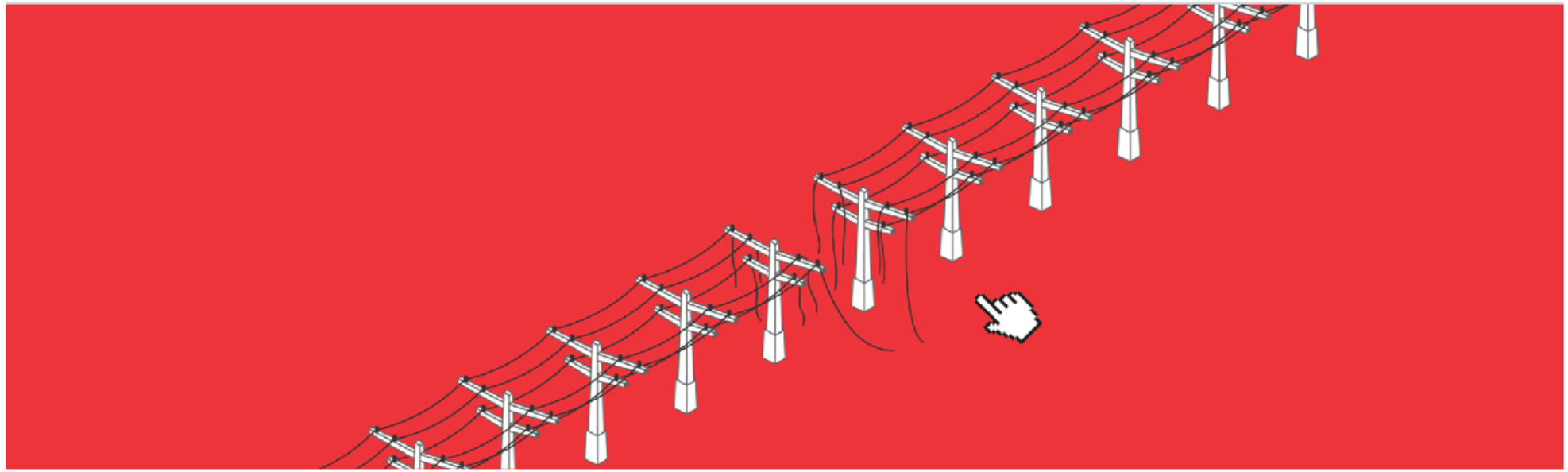


ILLUSTRATION BY JESSICA KURONEN/WSJ

America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It

A Wall Street Journal reconstruction of the worst known hack into the nation's power system reveals attacks on hundreds of small contractors

And NotPetya...

- Attackers compromised the update channel for MeDoc
  - Think "TurboTax For Business in Ukraine":
    One of only two accounting packages which Ukrainian businesses can use to pay taxes
- They then monitored for weeks with their backdoor
  - This gave them a foothold in almost all who have business
- Then they released a malicious "worm
  - It spread from computer to computer, and then with a fake "ransomware" payload
    - This cost Mersk shipping alone ***$100M-300M*** in lost r
      White House estimates $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

Course structure

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

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
- How to gauge the protections and limitations provided by today's technology
- How attacks work in practice

What's Required?

- Prerequisites:
  - CS 61B, 61C, 70
  - Familiarity with Unix, C, Java, Python and an ability to pick up new languages quickly
- 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 instructors using ***private Piazza posts***
  - ***Avoid public posts that reveal solutions to homeworks/projects***

Grading structure

- Absorb material presented in lectures and section
  - **Please attend lecture and discussion!**
- 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

Midterms

- Tentative dates: ??? and April 1
  - TBD: Either in-class or in the evenings
- If you can't make a midterm because of a University event or academic conference or another class having the exam at the same time
  - Notify us ***now*** in the "accommodations" Piazza folder
- If you need DSP accommodations (extra time on exams, etc) or have exam conflicts process them ***now as well***

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

Discussion

- Attend any discussion section you want that isn't full
  - If it is, go to another one, there are lots
- Please respond to Piazza poll for the time you plan to attend; use that to pick a time
- Discussion starts next week

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!

Collaboration

- Asking questions and helping others is encouraged
  - Discussing course topics with other is welcome
  - Submit homework individually
  - Submit projects individually or with a partner

- Limits of collaboration
  - Don’t share solutions with each other (except project partners)
  - You should never see or have possession of anyone else’s solutions — including from past semesters
  - Copying or dishonesty will result in severe penalties

Culture

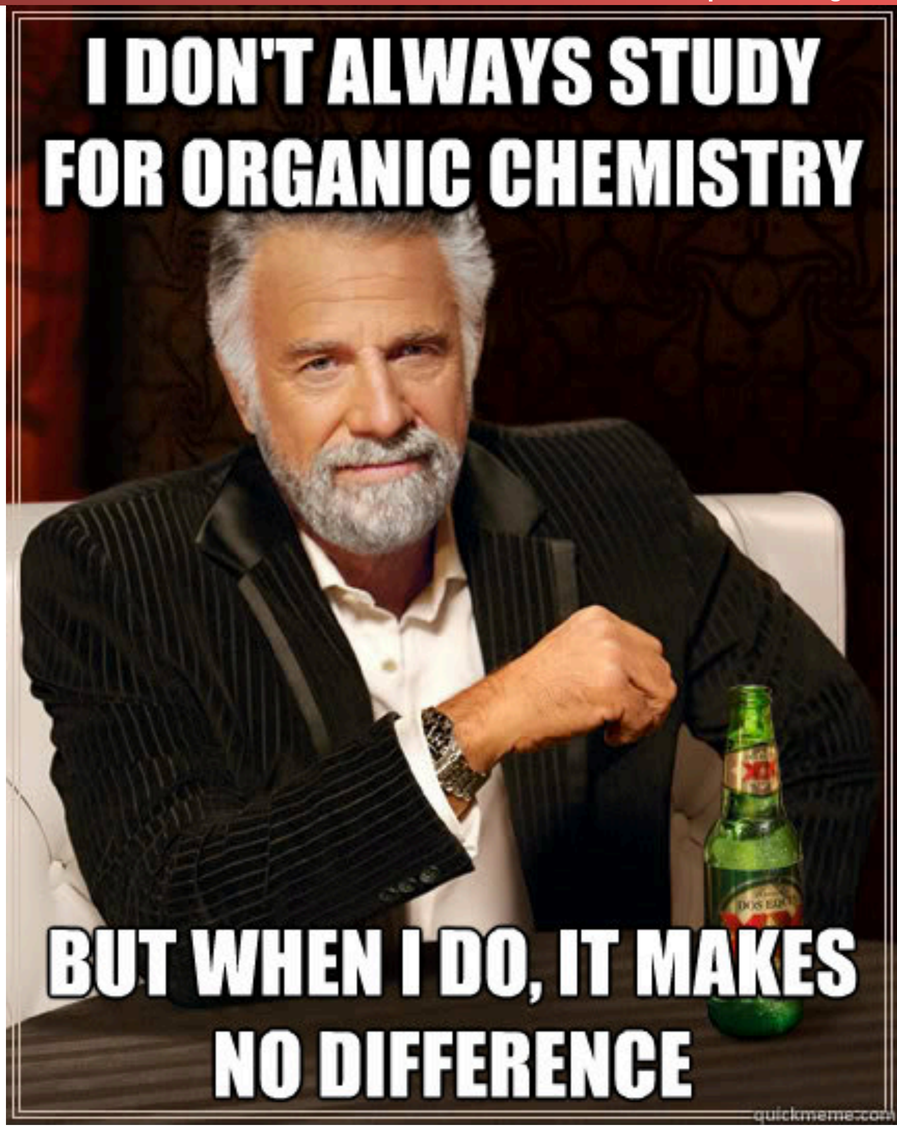
- Learning — please help each other learn
- Community — be excellent to each other
- Course staff — we’re here to help

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***
    - 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

Stress Management & Mental Health...

- We encourage you to take care of yourself
- 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
- Growth mindset
  - People typically look back and say grades were not as important as they seemed at the time

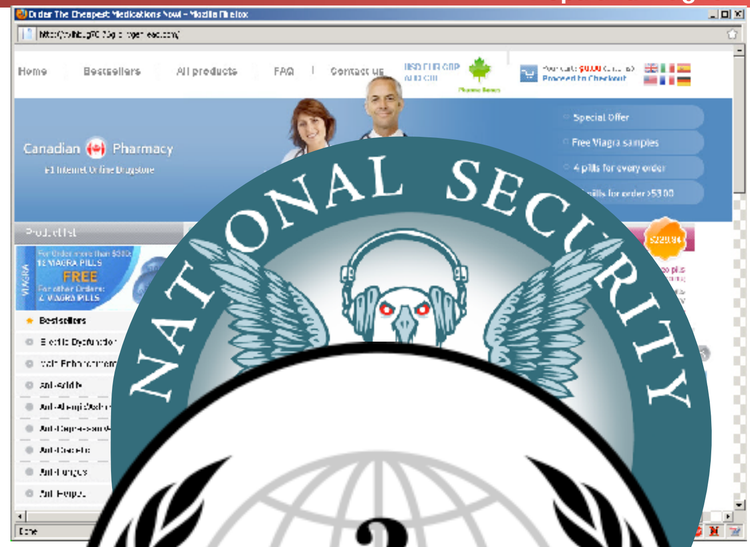


Security Principles

- People and Money
- Threat Model
- Prevention, Detection & Response, Mitigation and Recovery
- False Positives, False Negatives, and Compositions

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

- People attack systems for some reason
  - 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 attacker's motivation



Personal Security:
Threat Model...

- 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 us by criminals
- Intimate partners

It All Comes Down to People... The Users

- If a security system is unusable it will be unused
  - Or at least so greatly resented that users will actively attempt 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 Social Engineering...