Computer Science 161: Computer Security

Prof. Raluca Ada Popa

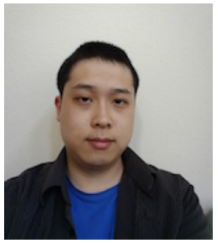
Nicholas Weaver

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

And a team of talented TAs


Apoorva Dornadula

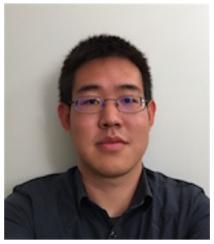

Rebecca Portnoff


Warren He


Mitar


Rohan Mathuria


Rohit Sinha


Calvin Li

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?

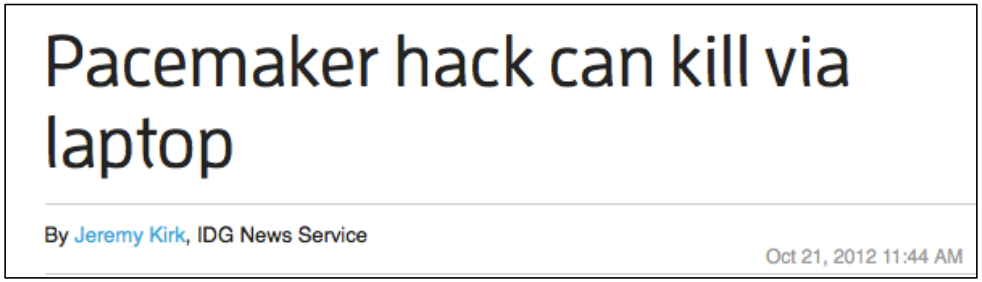
Obama unveils cybersecurity proposals: 'Cyber threats are urgent and growing danger'

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.

. . .

Why World War III will be fought on the internet

S.E. Smith

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

One needs to consider security for any part of computer systems

Course logistics

Course structure

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

Grading structure

- Absorb material presented in lectures and section
  - **Please attend lecture!**
- 3 course projects (24% total)
  - Done individually or in small groups
- 3-4 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

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, 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.

Webcasts?
Yes

- Benefits of webcasts:
  - Allows students to catch up on lecture at some other time
  - ~~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 could get the University sued!
- Costs of webcasts:
  - Students may not attend class because "hey, webcast"
    - But webcast has less context, and we will have your TAs note if you avoid lecture
  - Both of us like to use the blackboard
    - Which is not captured in this room
  - Nick has occasional outbursts of profanity
- But we're doing it.

Some Philosophy

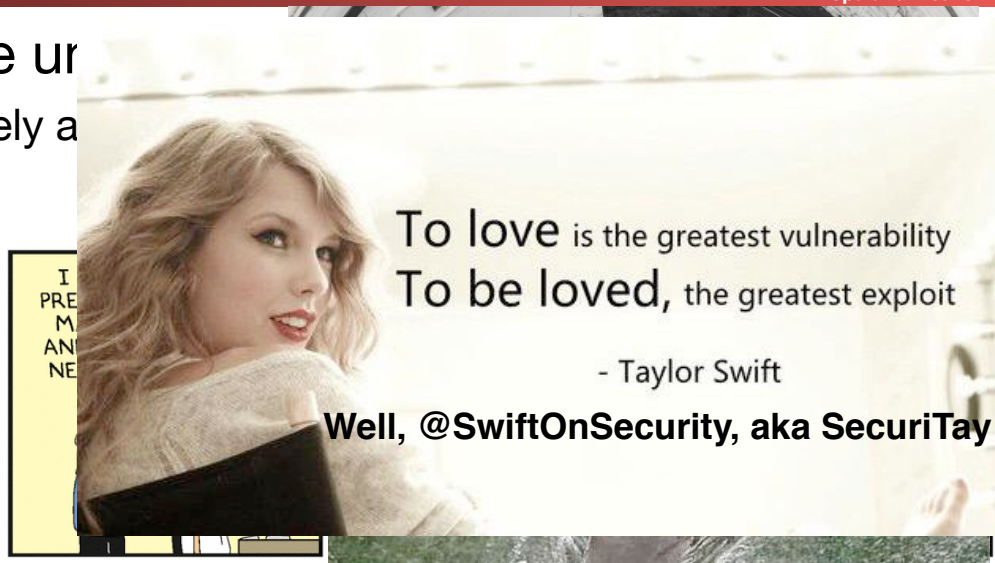
- The rest of this lecture is largely focused on philosophical issues
- People and Money
- Threat Model
- OODA loops and decision cycles
- Prevention, Detection & Response, Mitigation and Recovery
- False Positives, False Negatives, and Compositions
- And then some real word security tips

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

- People attack systems for some reason
  - If there are no attackers, there is no computer security 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"

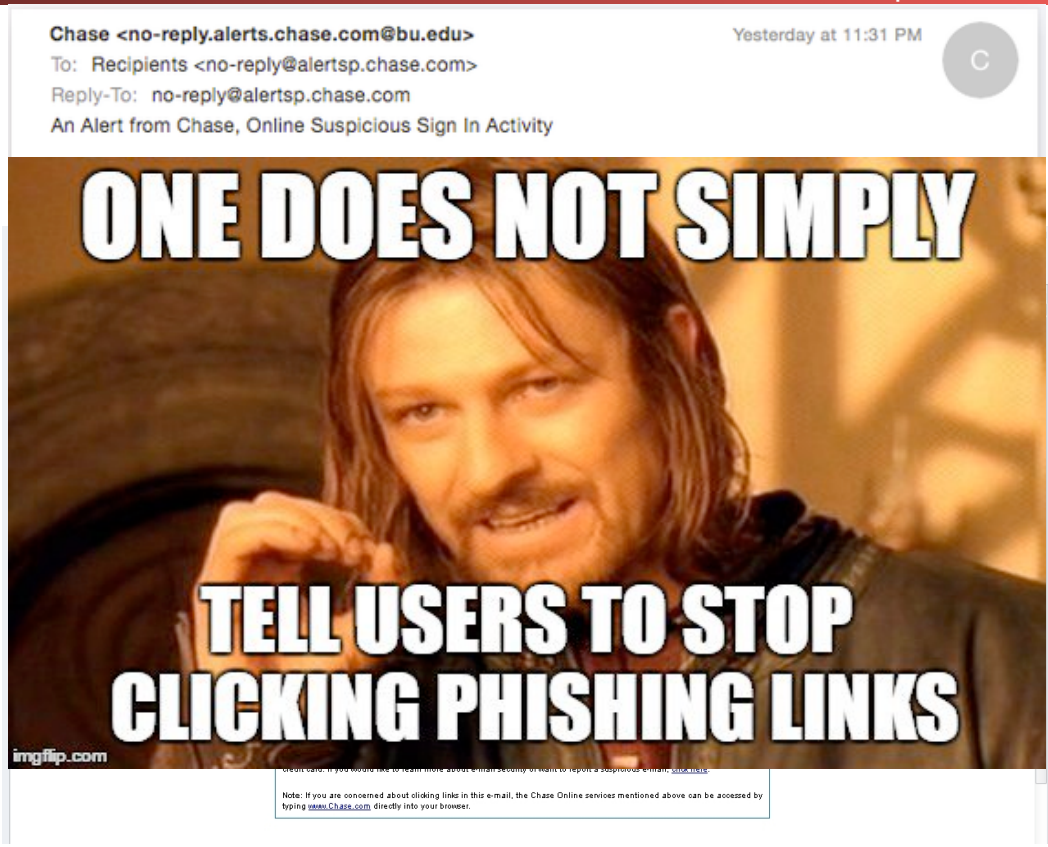
It All Comes Down to People... The Users

- 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?



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 $500k to $1M.
- Cost/benefit analyses appear all throughout security

At the Same Time: Update your iPhones...

- I share an office with Bill Marczak...
  - He works with peace activists in the Middle East...
  - One of them received a suspicious text
    - It looked like an iOS attack
- He took my GF's old iPhone...
  - Set it through a monitored network tunnel...
  - Click on link...
  - We wait
  - And wait...
  - And the phone got pwned!
- More on how it got pwned on Tuesday...

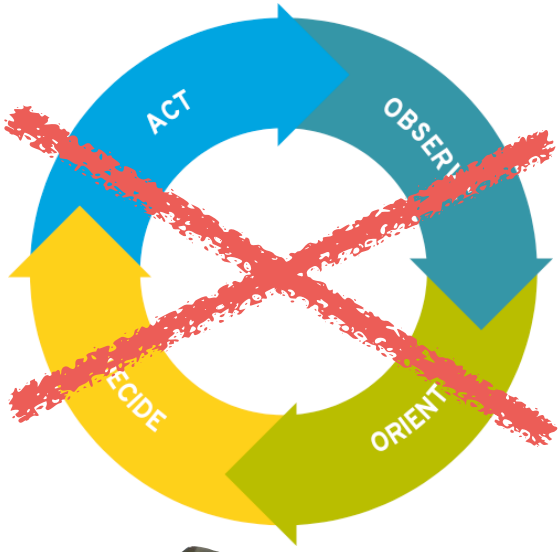
Needs to replace phone with $300 iPod Touch

NSO GROUP

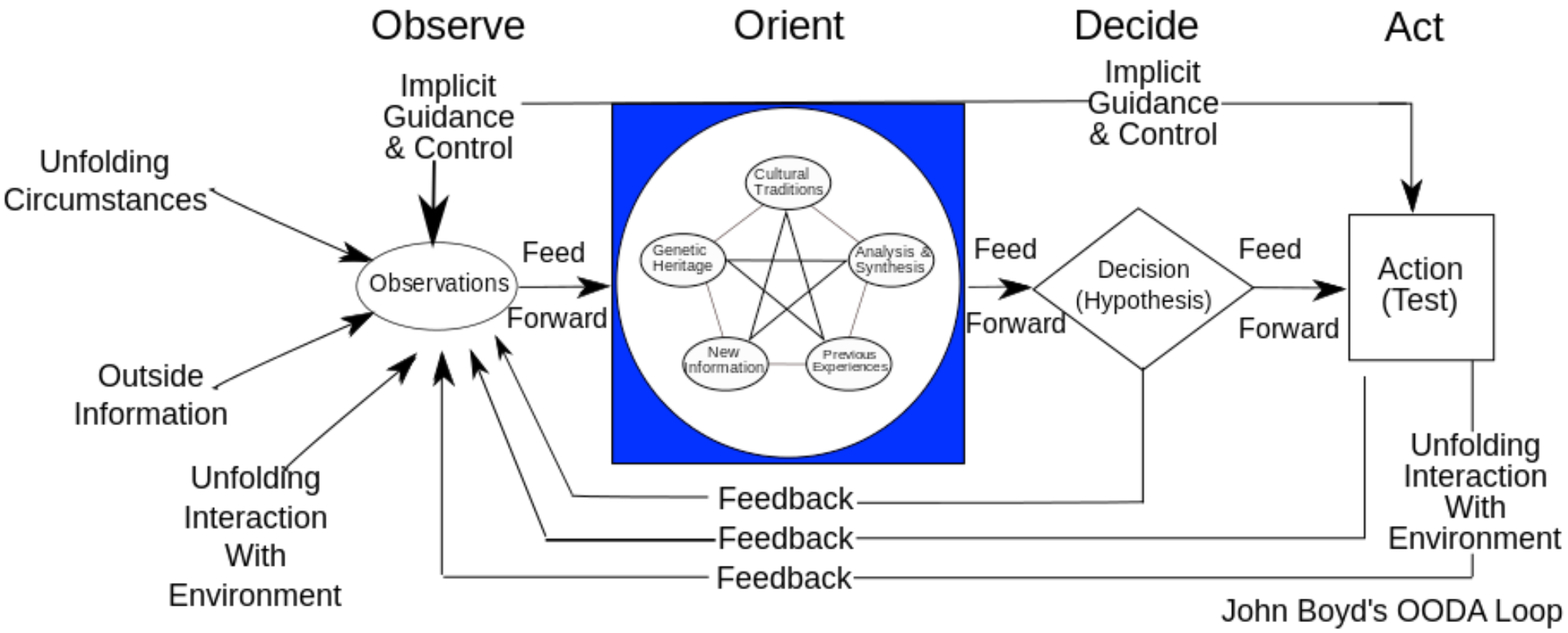
Needs to Replace $1M Exploit That No Longer Works

A Bit of Military Jargon: The OODA Loop

- You may have heard of the "OODA Loop"
  - Observe, Orient, Decide, Act cycle
- Originally developed by a military fighter pilot, Colonel John Boyd, as a way of modeling how adversaries think
  - If you can outthink your adversary, you win!
- Designed to provide a framework to think about thinking



The Real OODA Loop



https://en.wikipedia.org/wiki/OODA_loop#/media/File:OODA.Boyd.svg by Patrick Moran

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
  - The latest: $68M stolen from a Bitcoin exchange

by Lulu Yilun Chen t luluyilun Yuji Nakamura t ynakamura56

Detection & Response

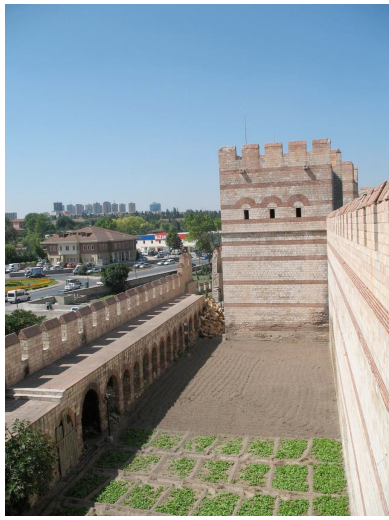
- Detection: See that something is going wrong
- Response: Actually ***do*** something about it
  - Without some response, what is the point of detecting something being wrong?

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

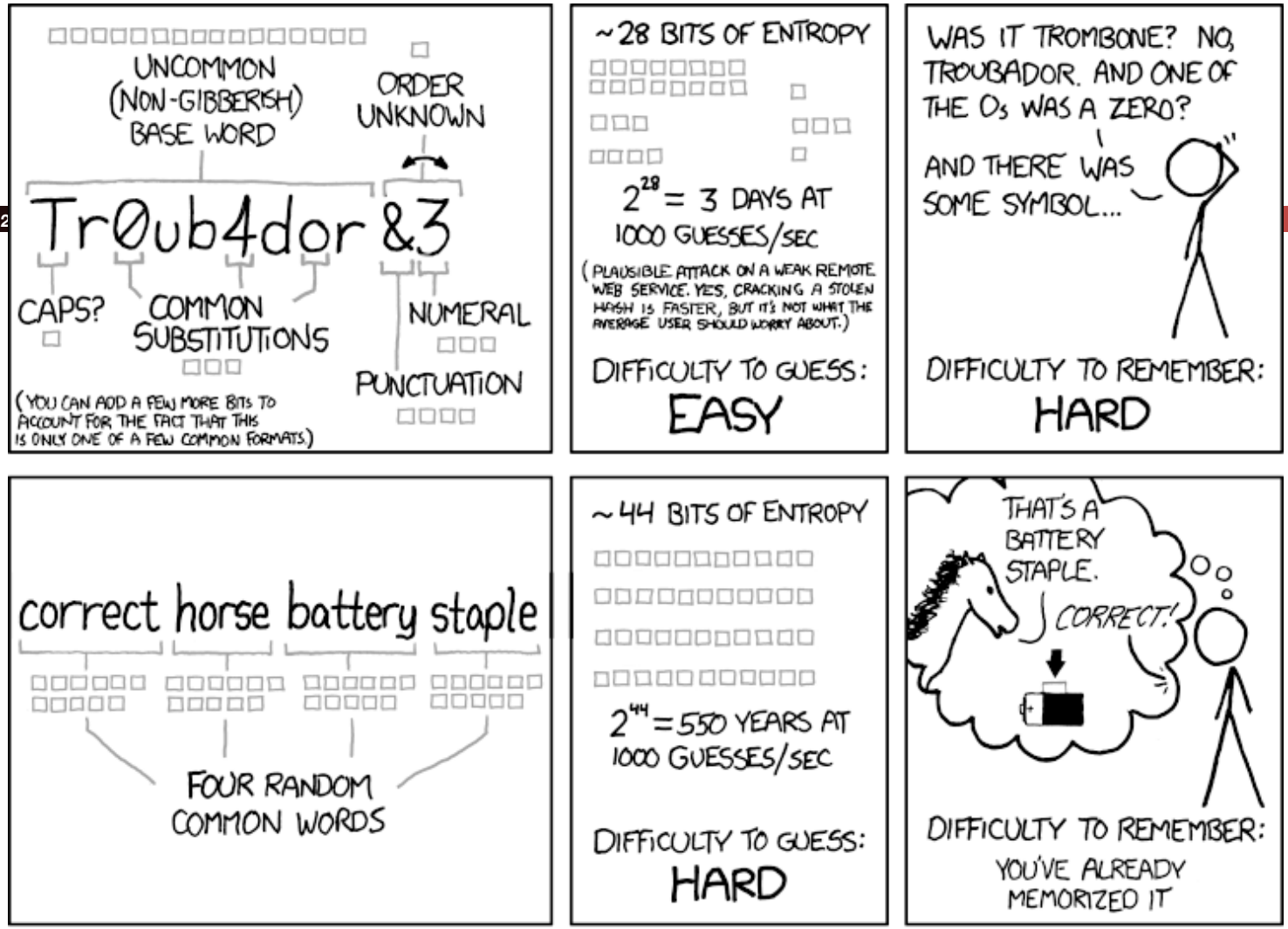


Mitigation & Recovery...

- 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"

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

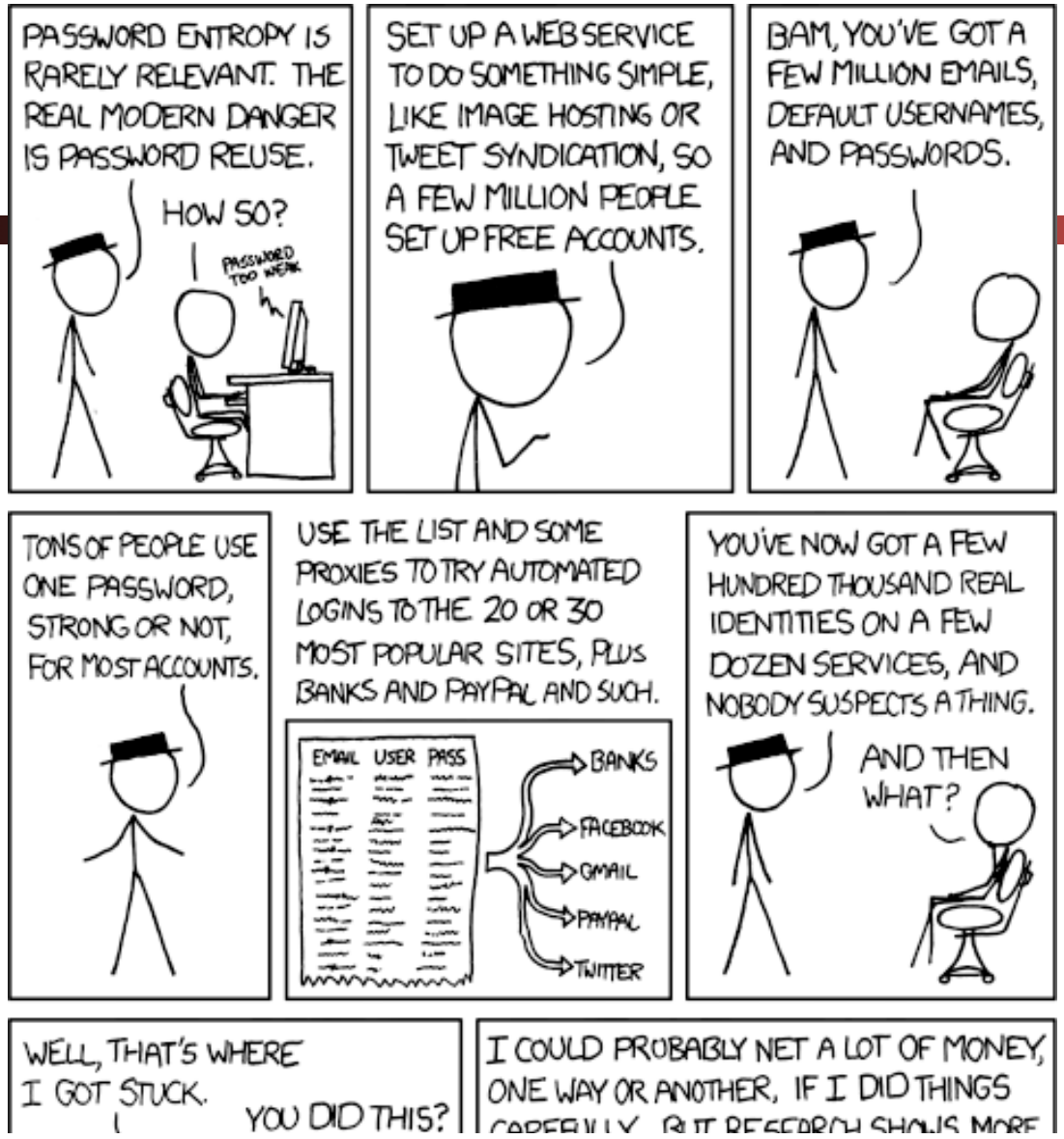
- Humans can't remember good passwords...
  - Well, we can remember a couple good passwords, but that's about it

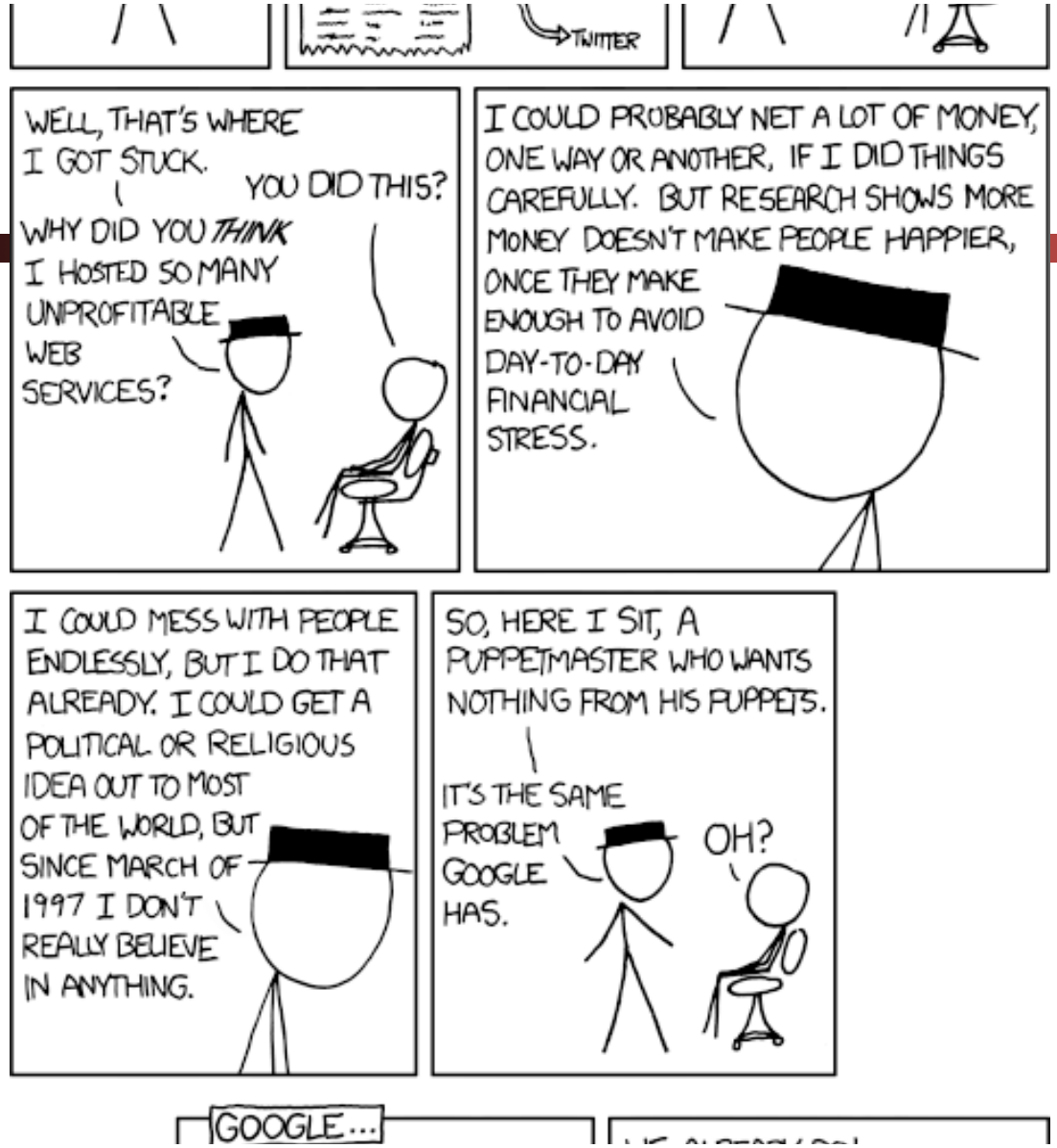


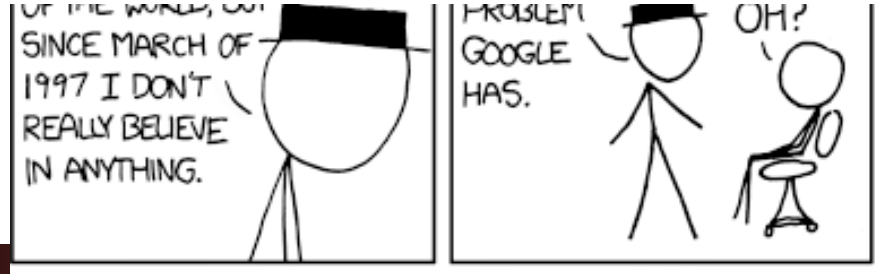
THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.

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...


PASSWORD ENTROPY IS RARELY RELEVANT. THE REAL MODERN DANGER IS PASSWORD REUSE.
HOW SO?
PASSWORD TOO WEAK
SET UP A WEB SERVICE TO DO SOMETHING SIMPLE, LIKE IMAGE HOSTING OR TWEET SYNDICATION, SO A FEW MILLION PEOPLE SET UP FREE ACCOUNTS.
BAM, YOU'VE GOT A FEW MILLION EMAILS, DEFAULT USERNAMES, AND PASSWORDS.
TONS OF PEOPLE USE ONE PASSWORD, STRONG OR NOT, FOR MOST ACCOUNTS.
USE THE LIST AND SOME PROXIES TO TRY AUTOMATED LOGINS TO THE 20 OR 30 MOST POPULAR SITES, PLUS BANKS AND PAYPAL AND SUCH.
EMAIL USER PASS
BANKS
FACEBOOK
GMAIL
PAYPAL
TWITTER
YOU'VE NOW GOT A FEW HUNDRED THOUSAND REAL IDENTITIES ON A FEW DOZEN SERVICES, AND NOBODY SUSPECTS A THING.
AND THEN WHAT?
WELL, THAT'S WHERE I GOT STUCK.
YOU DID THIS?
I COULD PROBABLY NET A LOT OF MONEY, ONE WAY OR ANOTHER, IF I DID THINGS


TWITTER
WELL, THAT'S WHERE I GOT STUCK.
YOU DID THIS?
WHY DID YOU THINK I HOSTED SO MANY UNPROFITABLE WEB SERVICES?
I COULD PROBABLY NET A LOT OF MONEY, ONE WAY OR ANOTHER, IF I DID THINGS CAREFULLY. BUT RESEARCH SHOWS MORE MONEY DOESN'T MAKE PEOPLE HAPPIER, ONCE THEY MAKE ENOUGH TO AVOID DAY-TO-DAY FINANCIAL STRESS.
I COULD MESS WITH PEOPLE ENDLESSLY, BUT I DO THAT ALREADY. I COULD GET A POLITICAL OR RELIGIOUS IDEA OUT TO MOST OF THE WORLD, BUT SINCE MARCH OF 1997 I DON'T REALLY BELIEVE IN ANYTHING.
SO, HERE I SIT, A PUPPETMASTER WHO WANTS NOTHING FROM HIS PUPPETS.
IT'S THE SAME PROBLEM GOOGLE HAS.
OH?
GOOGLE...


SINCE MARCH OF 1997 I DON'T REALLY BELIEVE IN ANYTHING.
GOOGLE HAS.
OH?


GOOGLE...
OKAY, EVERYONE, WE CONTROL THE WORLD'S INFORMATION. NOW IT'S TIME TO TURN EVIL.
WHAT'S THE PLAN?
MAKE BOATLOADS OF MONEY?
Google
WE ALREADY DO!
SET UP A COMPANYWIDE CoD4: MODERN WARFARE TOURNAMENT EACH WEEK?
THAT'S NOT EVIL!
OOH, DIBS ON THE LOBBY TV!
OKAY, WE SUCK AT THIS.

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