
HART'S
SEEDS
Quality Seeds Since 1892
RULE 777
IF YOU DON'T MAKE IT USABLE & SECURE
USERS WILL MAKE IT USABLE & INSECURE
imgflip.com

Computer Science 161: Computer Security

Nicholas Weaver

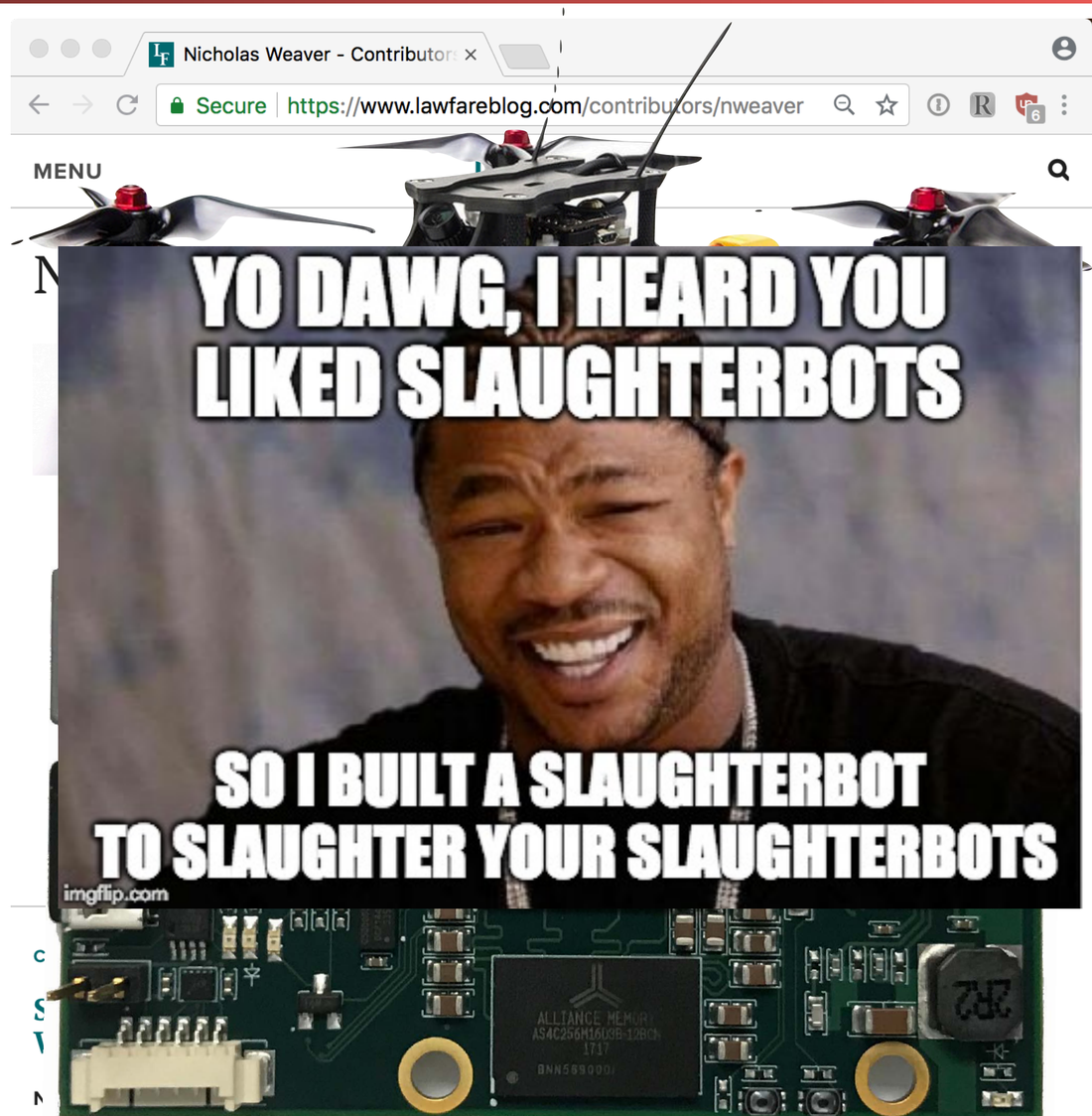
https://cs161.org

Zoom Comments...

- Before I begin, I know this SUCKS compared with live lectures....
- But there is one huge advantage: the chat/Q&A
  - Today the chat wasn't working, but Q&A was... We will see if that sticks
- So please use them... If you have questions, just ask!
  - Chat actually works better than live for asking questions because I can poll the chat rather than receive interrupts
  - In the After Times, I will be using a similar live chat during lectures!

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

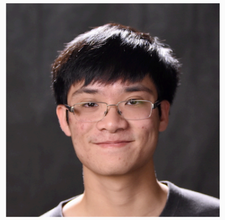
Peyrin Kao (head TA)
he/him
peyrin@

Andrew Law
he/him

Ben Hoberman
he/him
bhoberman@

Conor Gilsenan
he/him
conorgilsenan@

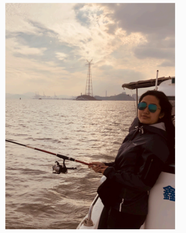
Evan Corriere
he/him
evancorriere@



Nicholas Ngai
he/him
nicholas.ngai@

Nikita Samarin
he/him
nsamarin@

Noura Alomar
she/her
nnalomar@



Sheqi Zhang
she/her
sheqi@

Shivam
he/him
shivamshorewala@

Shomil Jain
he/him
shomil@

Siddharth Bansal
he/him
sidbansal@

Solomon Joseph
he/him
solomon.joseph@

EvanBot
any/all
evanbot@

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 or safety...

- 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
- Safety is about making sure that systems still work as expected...
  - But the "adversary" is mother nature rather than deliberate human action

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

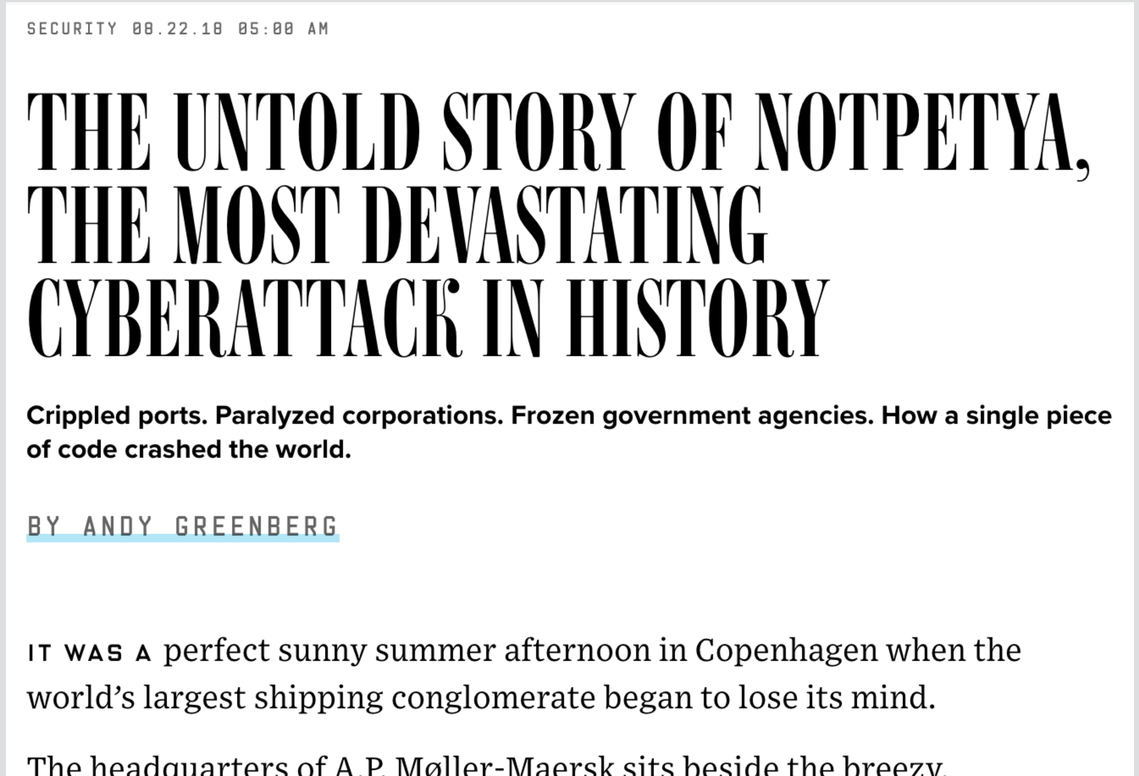
By **Nicholas Weaver** Wednesday, June 14, 2017, 11:38 AM

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.

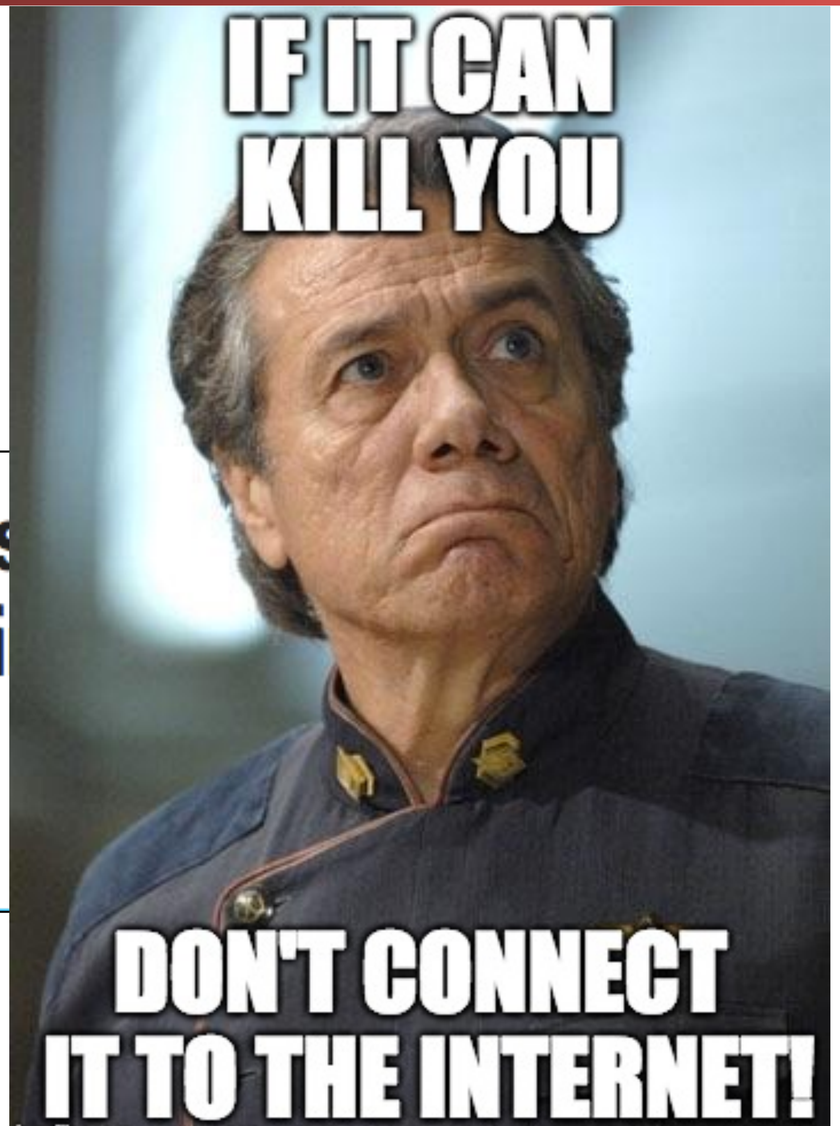
BY ANDY GREENBERG

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, read "smashing the stack for fun and profit":
      There will be a 61C review session as well
  - 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 Homework 1
- Participate in Piazza (use same name as Gradescope if possible)
  - 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 course projects (30% total)
  - Done individually or in groups of 2
- Labs (15%)
  - But you can replace your lab grade with your homework or project grade (whichever is greater)
- 7 homeworks (15% total)
  - Done individually: instant-feedback grading
- One midterm (15%)
- A comprehensive final exam (25%)
- A little bit (1%) of bonus points for Piazza/lecture/discussion participation
  - Will not be used in calculating the curve, and it is the max 2 of 3
- 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
  - But lowest-score homework is dropped
- Late project or lab:
  - <24 hours: -10%, <48 hours: -20%,
    <72 hours: -40%, ≥72 hours: no credit
  - ***BUT YOU HAVE 6 slip days***
    - They will be applied to projects and labs at the end of the semester in the method which gives you the most benefit
- 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.
- 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 or final because of another class having the exam at the same time
  - Notify us using the exam conflict form (will be released closer to the exam). We will have a make-up exam ***immediately after*** the scheduled exam.
  - We will also have a much later time-slot for those on the other side of the planet...

DSP and other accommodations...

- We have a standard form for late homework/lab/projects: https://cs161.org/extensions
  - This is going to be a hard semester, so we wish to be understanding when something bad happens
    - But please make accommodation requests before the time an assignment is due
  - Plus you have the 6 slip days
- For those with a DSP accommodation, please make sure you have a letter submitted from the DSP office
  - Those with a late-assignment DSP accommodation will automatically get 3 days, if you need more have your DSP coordinator confirm
- We also are taking measures to protect those requesting accommodations: Access control policy on the data
  - Raw requests are only available to myself, Peyrin (head TA), the TAs in charge of DSP logistics (Evan, Sid, Nikita), and Michael-David Sasson (course manager)
  - The results are available to the TA handling grading...
    But only as Student ID, not name

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
- And I'll also be able to do meetings by appointment over a wider window starting in a week or two
  - Goal is to understand how well setting up appointment slots works instead
- 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
  - If it is, go to another one, there are lots
- We ***WILL NOT*** have discussion this 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 the course website
  - We have to use bCourses/Kaltura

Piazza and Gradescope…

- You should be auto-enrolled if you were in the class/on the waitlist a week ago
  - Since we did a bulk add…
- If you aren't yet (e.g. late add, concurrent enrollment, etc…)
  - Piazza: piazza.com/berkeley/spring2021/cs161
    Gradescope: Entry code 3YP8BD

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***”

Exam Proctoring...

- We will be using remote proctoring through Zoom for the midterm and final
  - We also use other techniques to detect cheating which we won't tell you about
- IF we didn't and we told you we had no other cheating detection mechanisms...
  - I'd be ***insulted*** if the cheating rate was NOT 100%

Ethics Guide for Defense Against the Dark Arts

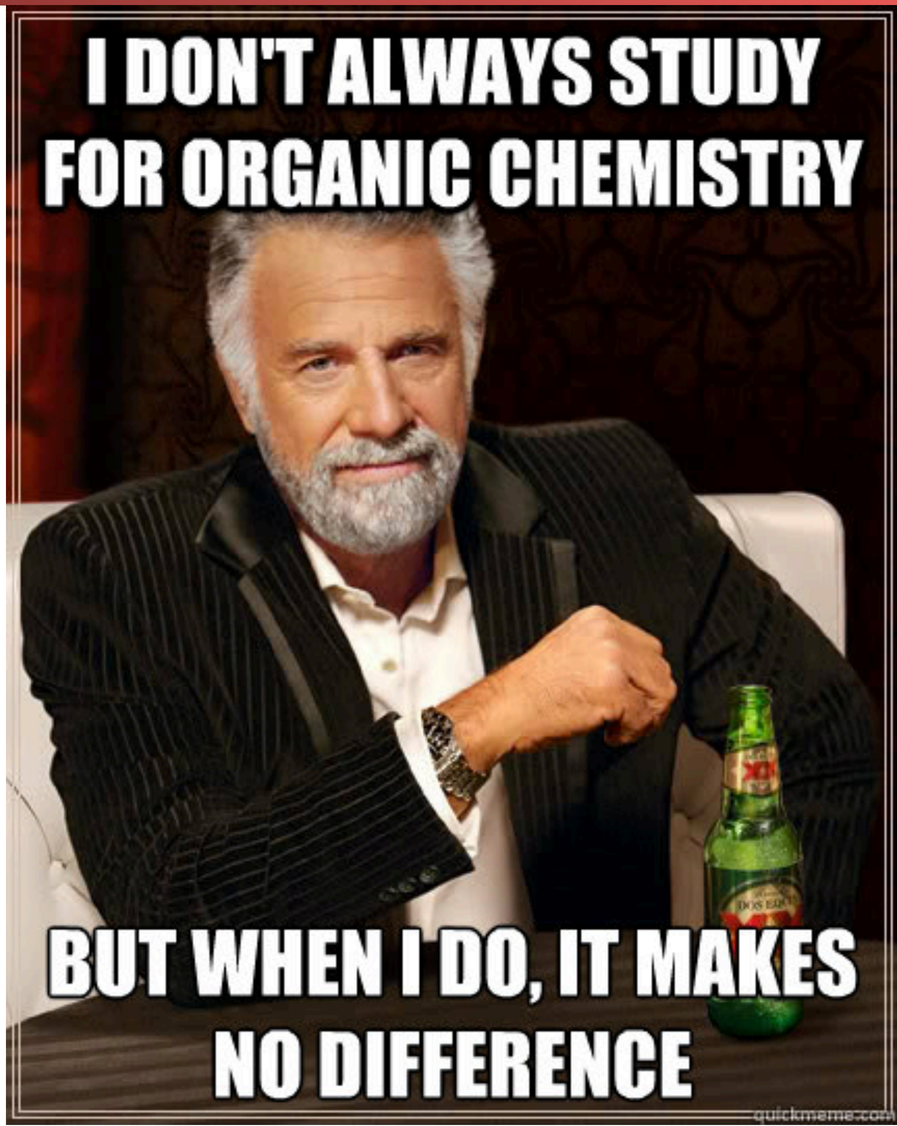
- Of necessity, this class has a fair amount of "dark arts" content
  - As defenders you must understand the offense:
    You can't learn defense against the dark arts without including the dark arts
  - But a lot of "don't try this at home" stuff
- Big key is ***consent***
  - Its usually OK to break 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 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 in the After Times and see my transcript!



And SARS-CoV-19: Embrace the Suck

- The ***best*** in person we may be able to do is outdoor office hours
- Why?
  - The risk to students is actually reasonable:
    The infection/fatality rate for someone age 20 is probably in the same ballpark as joining a fraternity
    - But students would act as a reserve for the rest of society:
      Across the population this has a 0.5% infection/fatality rate...
      AKA kill off >1M people in the US
  - And our nation is insane:
    20% suffer from a debilitating mental disorder called "Fox News Brain"

And Finally...
Tales and Lore...

- A lot of security lessons are best expressed as tales and stories
  - Lessons learned through the pain of others
- I'm particularly heavy on the lore myself
  - It is how I learned a lot of it...
- Gray background on slides means lore
- Which means you should understand the ***lesson***, but you don't need to remember (and won't be tested) on the details

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...

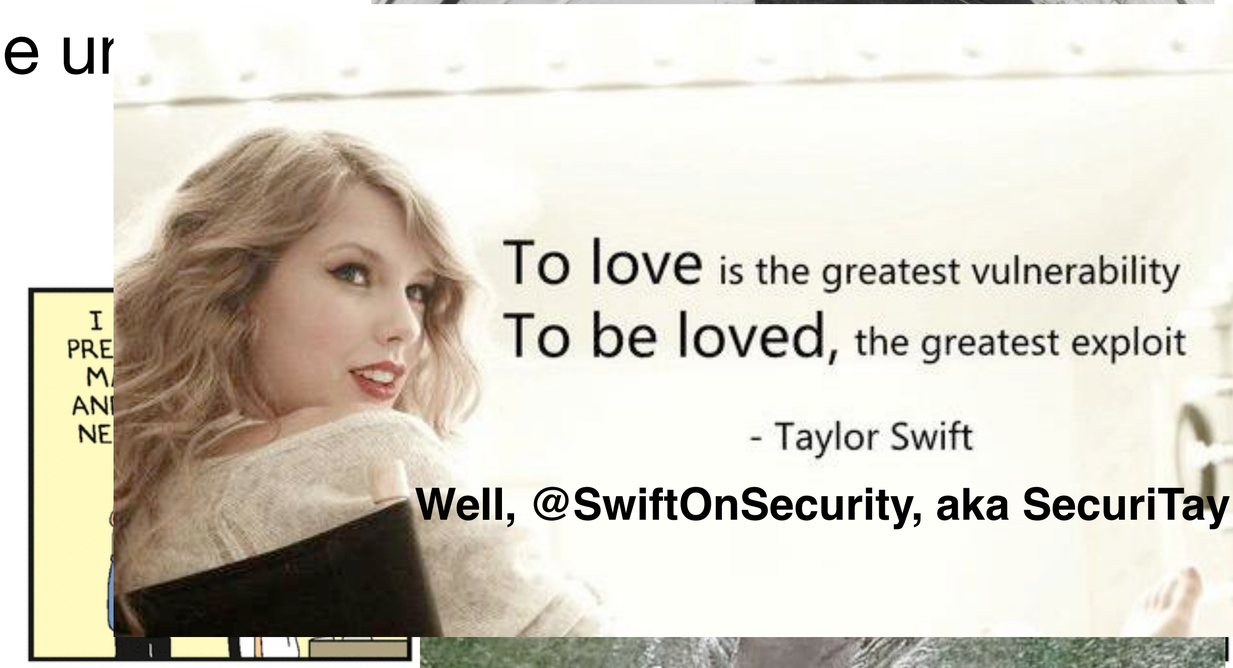
- Who and why might someone attack ***you***?
- Criminals for money
- Teenagers for laughs or to win in an online game
- Governments
  - Probably not: We aren't important enough
  - And even if important enough we're only worth the D game:
    aka the same things used against us by criminals
- Intimate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

Security often comes down comes down to money...

- "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 network: free market cost of a zero-day (unknown/unpatchable) exploit chain 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 2018: four separate multi-million-dollar theft incidents
  - Or Coinbase accounts: Averaging a ***known*** theft a day!

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?

Burglar Alarms Cops Won't Answer

Jacquie Simms, left, leader of the Watts neighborhood council, and fellow Watts residents Milton Smith and his wife, Bernece, 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 an eclectic mix of 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
  - And although it can be better, it is less than the sum of the parts...

Composing Detectors for Defense In Depth... TINSTAAFL

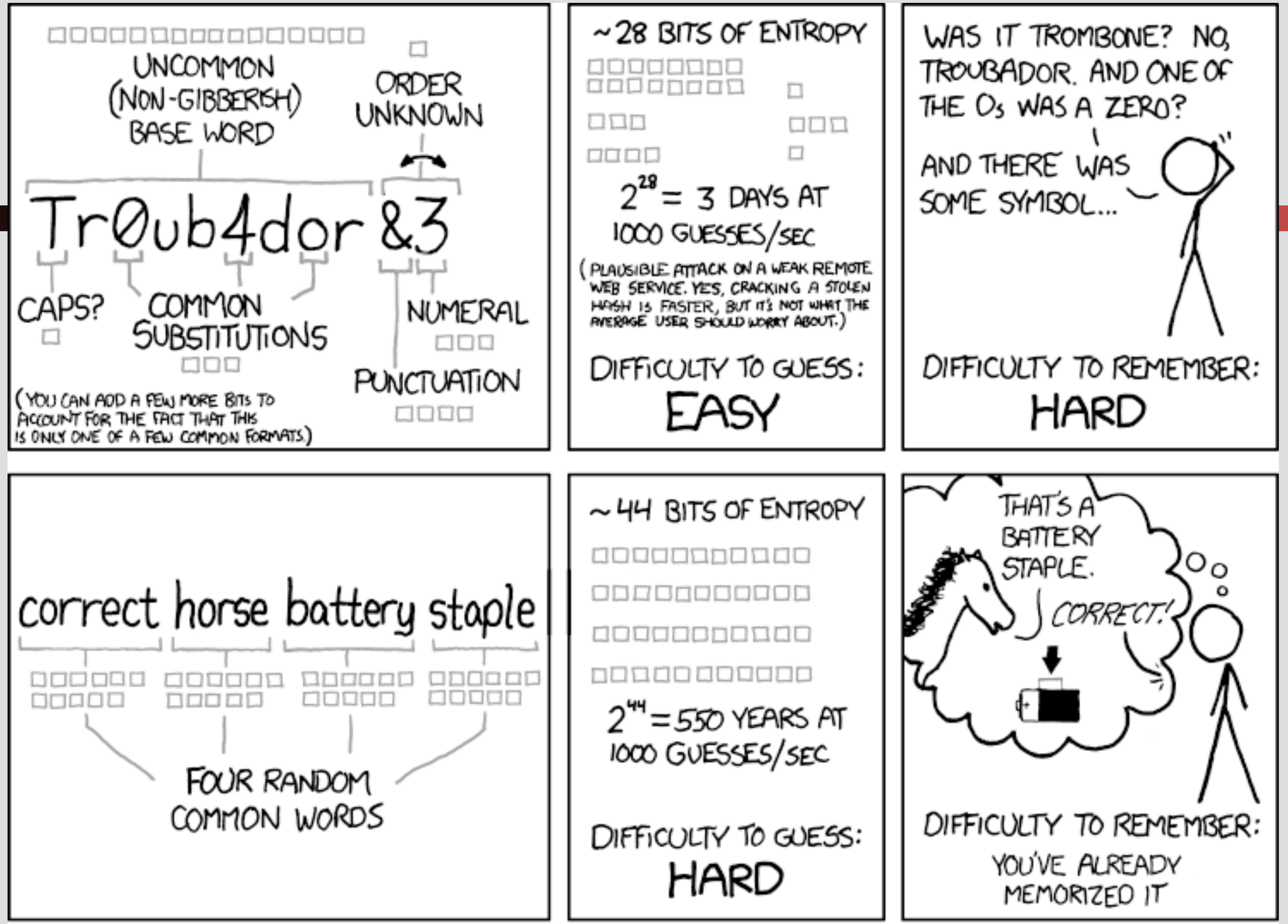
- There Is No Such Thing As A Free Lunch!
- The best case: the two detectors are ***independent***
  - With FP1 and FP2 false positive rates and FN1 and FN2 false negative rates
    - Rate is 0-1:
      0 is it never has a false positive/negative,
      1 is it is always a false positive/negative...
- Parallel composition: ***either*** detector may alert to trigger a response
  - ***Reduces*** false negatives: new rate is FN1*FN2
  - ***Increases*** false positive rate: new rate is FP1 + (1-FP1)*FP2
- Serial composition: ***both*** detectors must alert
  - ***Reduces*** false positives: new rate is FP1*FP2
  - ***Increases*** false negatives: new rate is FN1 + (1-FN1) * FN2

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"... AKA, "If you love it, ***back it up!***"

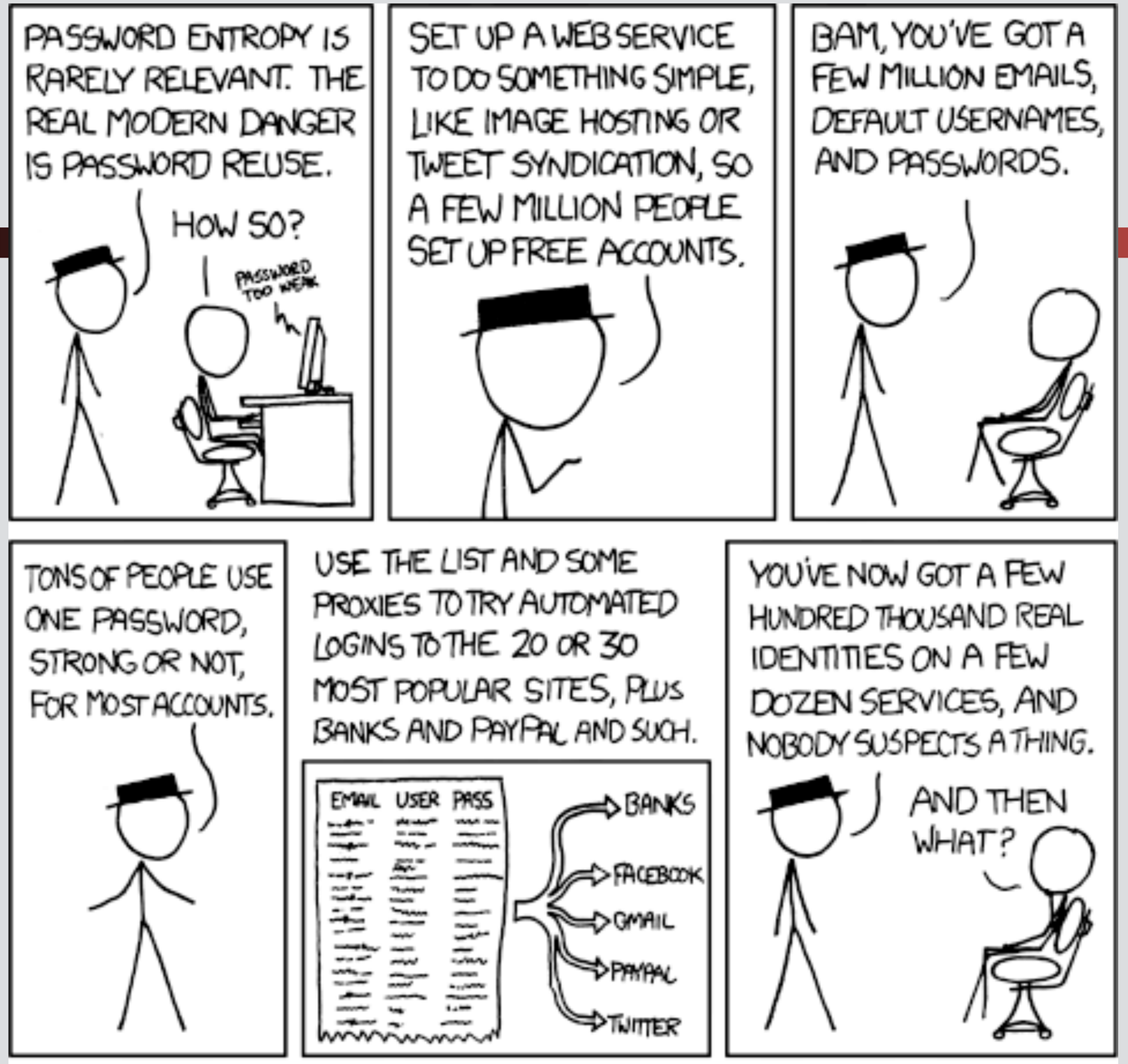
Real World Security...
How is your account breached?

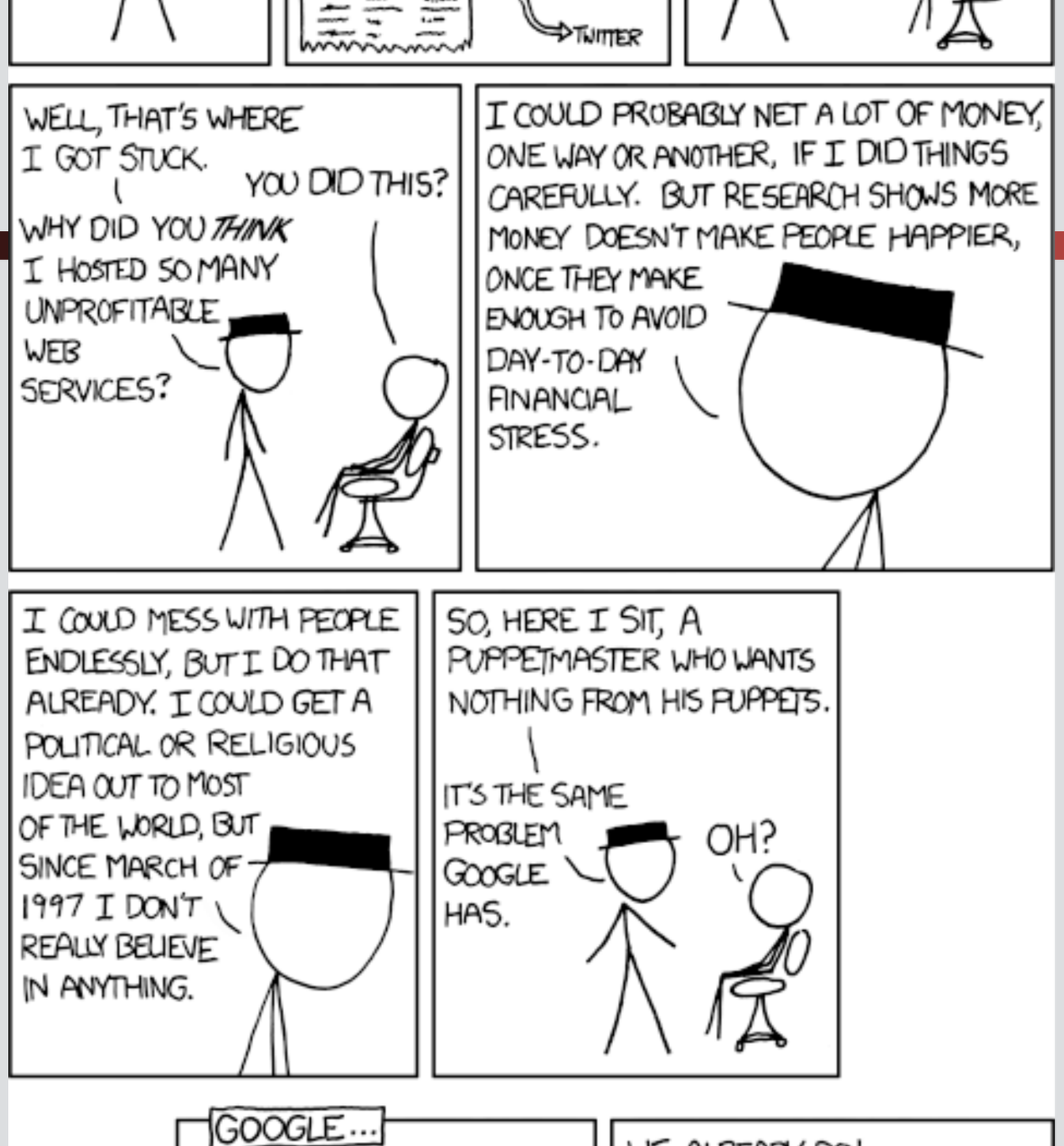
- Humans can't remember good passwords...
  - Well, we can remember a couple good passwords, but that's about it

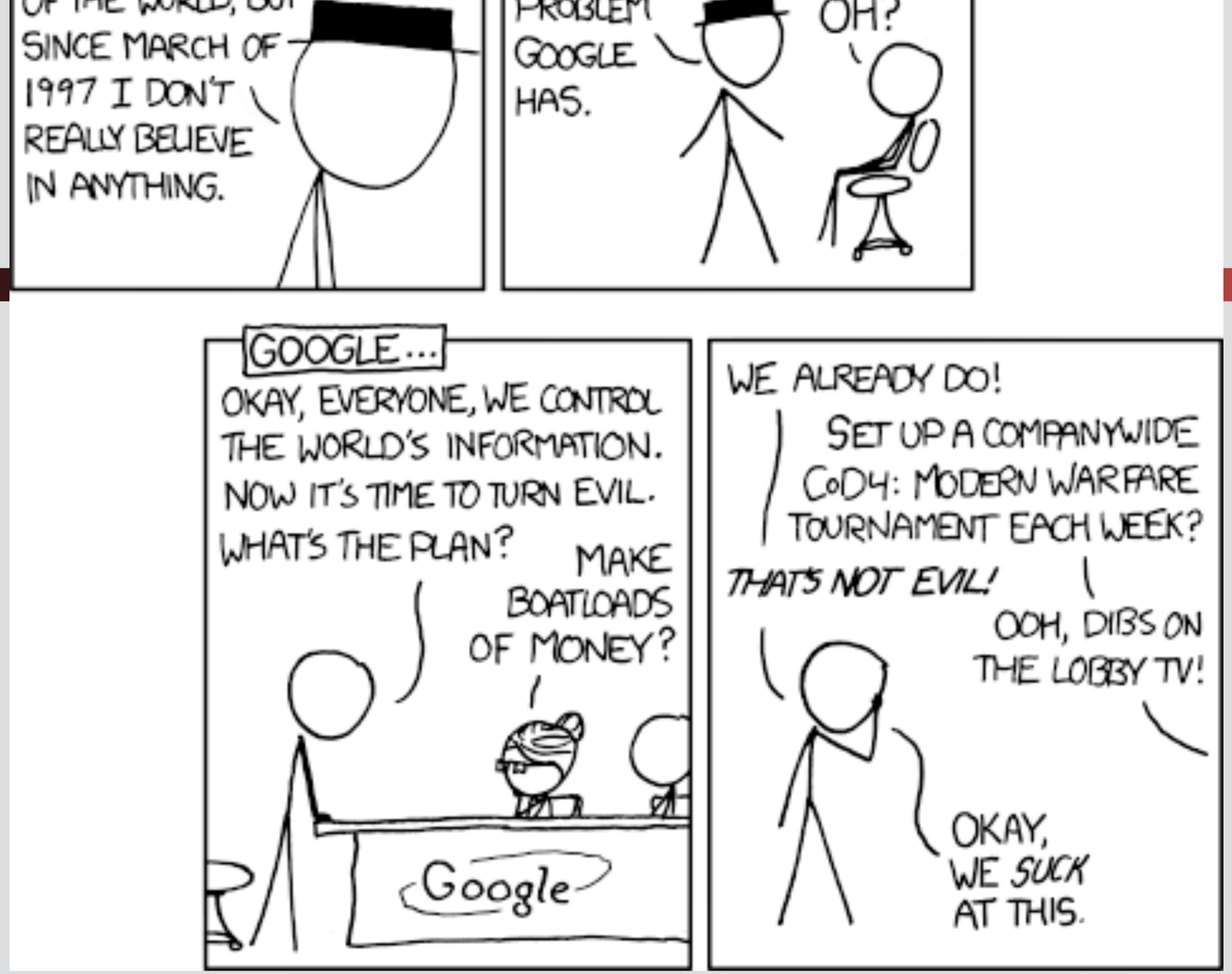

UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4dor&3
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
2^28 = 3 DAYS AT 1000 GUESSES/SEC
(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS SOME SYMBOL...
DIFFICULTY TO REMEMBER:
HARD
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
2^44 = 550 YEARS AT 1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED 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.
PROBLEM 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

And Fido U2F Security Keys/ WebAuthn 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

So For Account Security...

- Use a password manager
  - So you have a unique password for each site and a bad guy can't do "credential stuffing"
- Always enable 2-factor
  - So that even if a bad guy gets your password they have to get the second factor
    - Even SMS is better than nothing!
  - Even if you are successfully phished the bad guy only gets temporary access
- When possible, use a security key
  - Bad guys can't phish it at all!

So Homework -1:
Real World Security...

- Decide on a password manager and get it
  - If your CalNet password is shared with anything else, change it!
- Get yourself a security key
  - I like the Yubico ones, either a basic "security key" for $20
    or a full Yubikey 5 for $50... But anything supporting U2F/FIDO2 will do
- Enable security key authentication on your CalNet and Google accounts
  - And all other key email accounts & social media accounts
- Now silently laugh at phishers and password stuffers!

The Properties We Want in a Safe

- We want the inside to be inaccessible to an attacker
  - But what ***sort*** of attacker?
  - But ***how much time*** does the attacker have?
- We want to ***measure*** how much time & capabilities needed for an attacker
  - For a safe, ratings communicate how much based on experts performing the attack
    - Such security ratings are much harder in the computer security side

Security Rating: A Real Safe

- TL-15:
  - An expert with common tools will take >= 15 minutes to break in
- May even have "relockers"
  - EG, a pane of glass which, if shattered when trying to drill for the combo lock, causes the safe to freeze closed!

Security Rating: A Stronger Safe

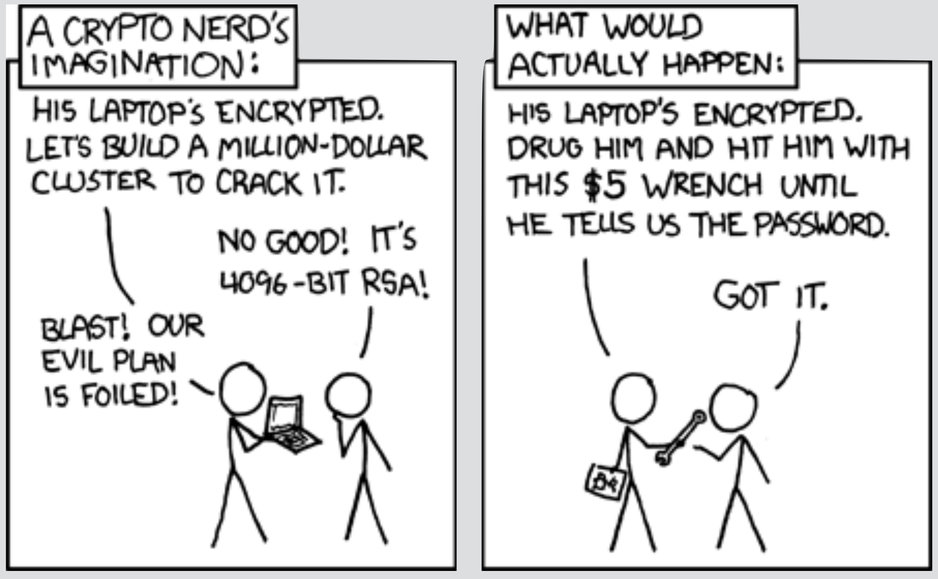
- TL-30:
  - The same expert and tools now takes 30 minutes

Security Rating: Now We Are Talking

- TRTL-30
  - 30 minute to break with tools and/or a cutting torch

Security Rating: Maximum Overkill...

- TXTL-60:
  - 60 minutes with tools, torches, and up to 4 oz of ***explosives!***
  - Far easier to use "Rubber Hose Cryptanalysis" on someone who knows the combination



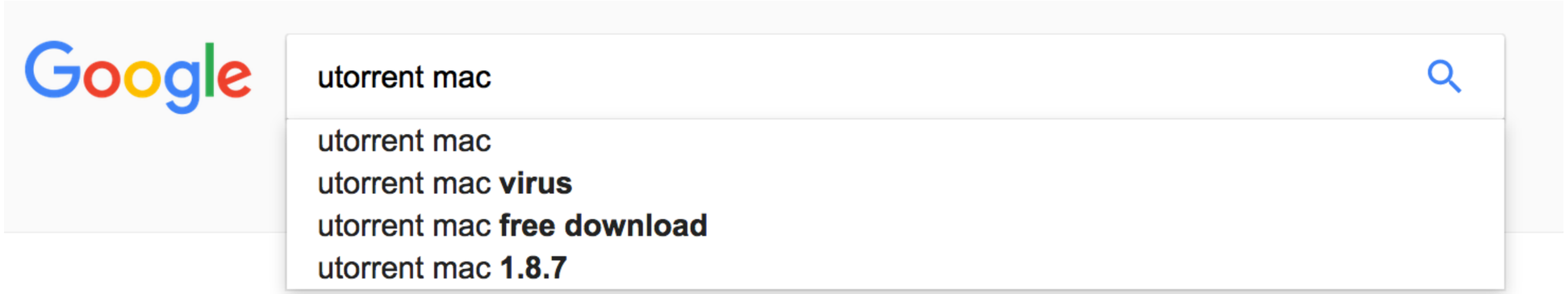
Security Rating:

😂😂😂😂😂😂😂😂😂...

- This is legally a "gun safe"
  - Meets the California requirements for "safe" storage of a handgun
- But it is practically ***snake oil***:
  - Cylindrical locks can often be opened with a Bic pen
  - Some safes like this open if you just ***drop them a foot!***
- So why do people buy this?
  - It creates an ***illusion*** of security
  - It meets the ***legal requirement*** for security

Lesson: Security is economics

- More security (***generally***) costs more
  - If it costs the same or less and doesn't impose other costs, you'd always go with "more security"
- Standards often define security
  - The safe standards from Underwriters Laboratories
    - If you are selling a real safe to a customer who knows what they are buying, you have to meet theses standards
  - The "gun safe" standards from the California Department of Justice
    - Which are a joke
- The more purchasers makes security cheaper...
  - If you need a safe at home, buy a UL listed Residential Security Container ***gun safe!***
    - The gun owners are willing to pay for security, and so have created a market for security!



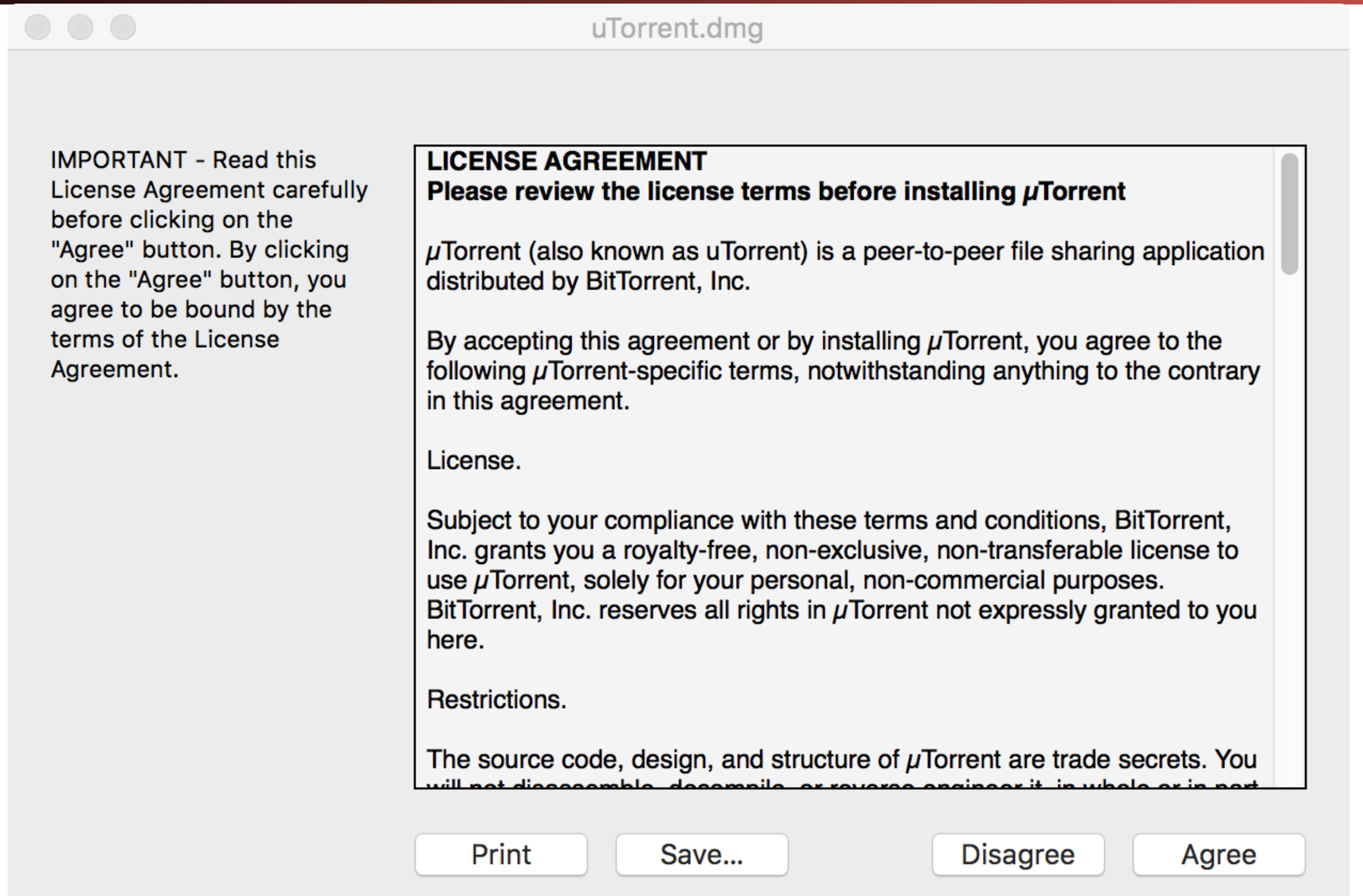
Mac and OSX Downloads - µTorrent® (uTorrent) - a (very) tiny ...
www.utorrent.com/downloads/mac
Download the official µTorrent® (**uTorrent**) torrent client for Windows, **Mac**, Android or Linux-- **uTorrent** ... For **Mac** (1.42 MB); English (US) - November 27, 2016.

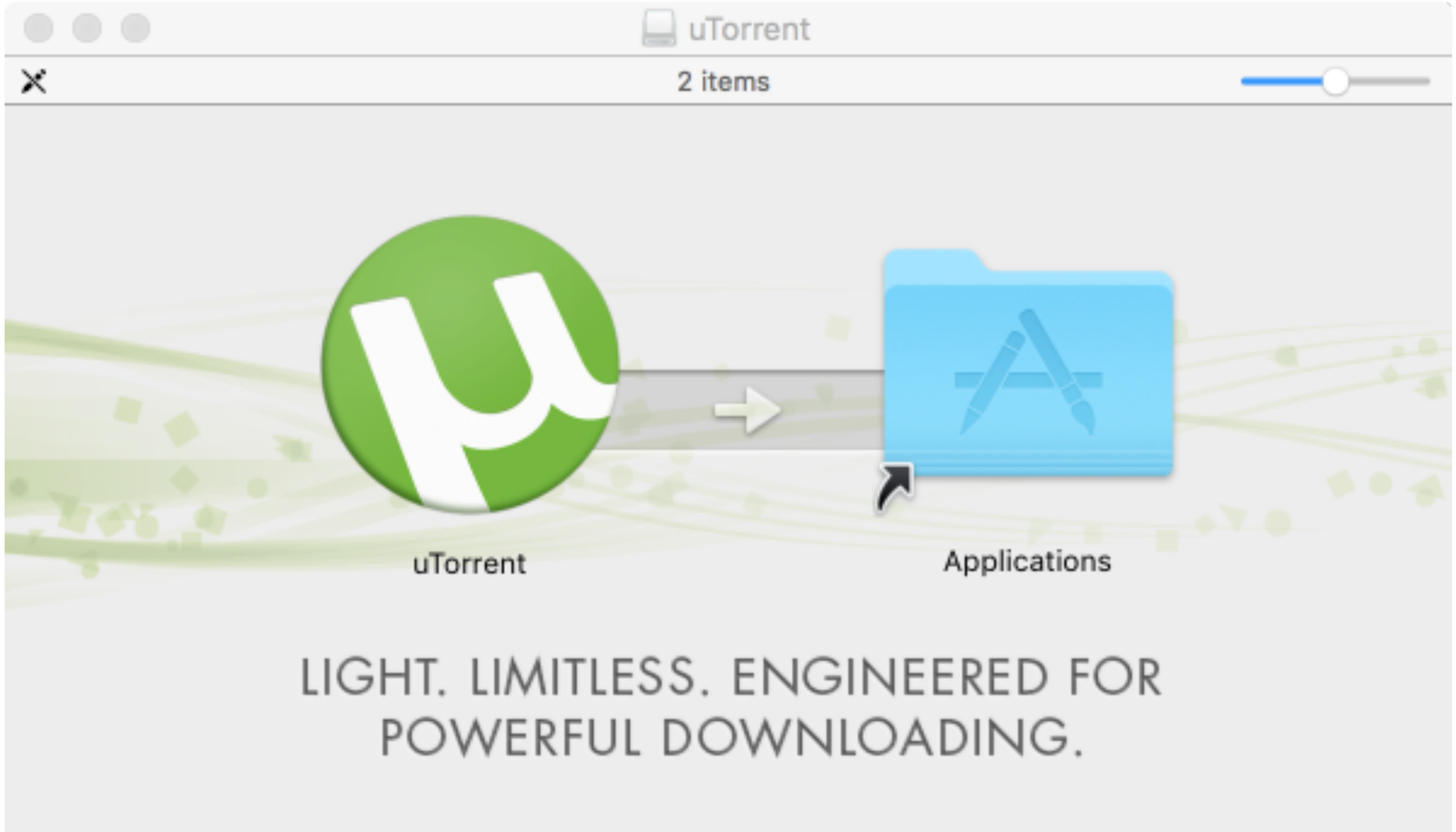
uTorrent (Mac)
µtorrent estable(1.8.7 build 43001).
Para Mac (1.42 MB); Inglés ...

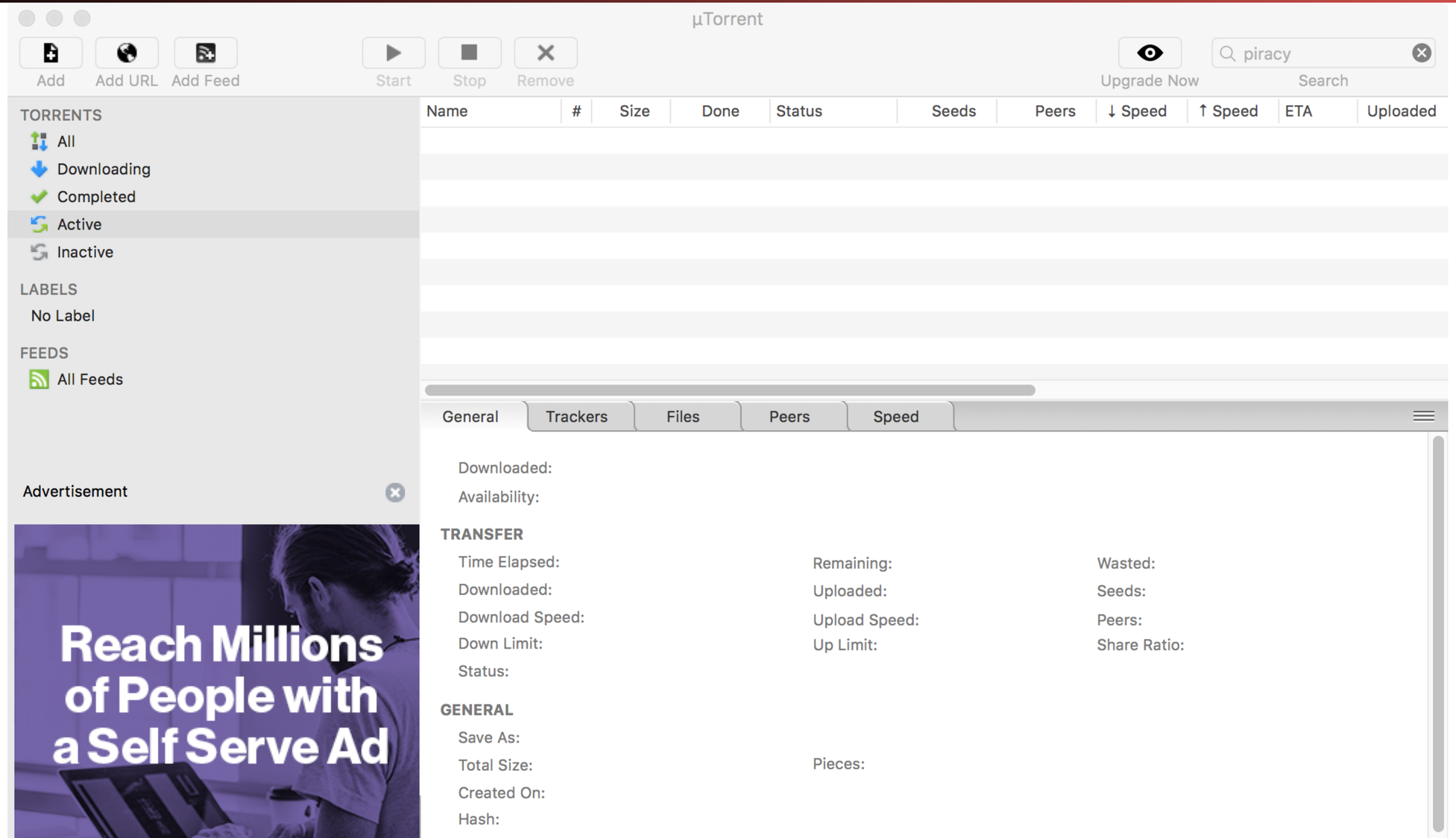
Download
µTorrent Stable(1.8.7 build 43001).
Für Mac (1.42 MB); Englisch ...

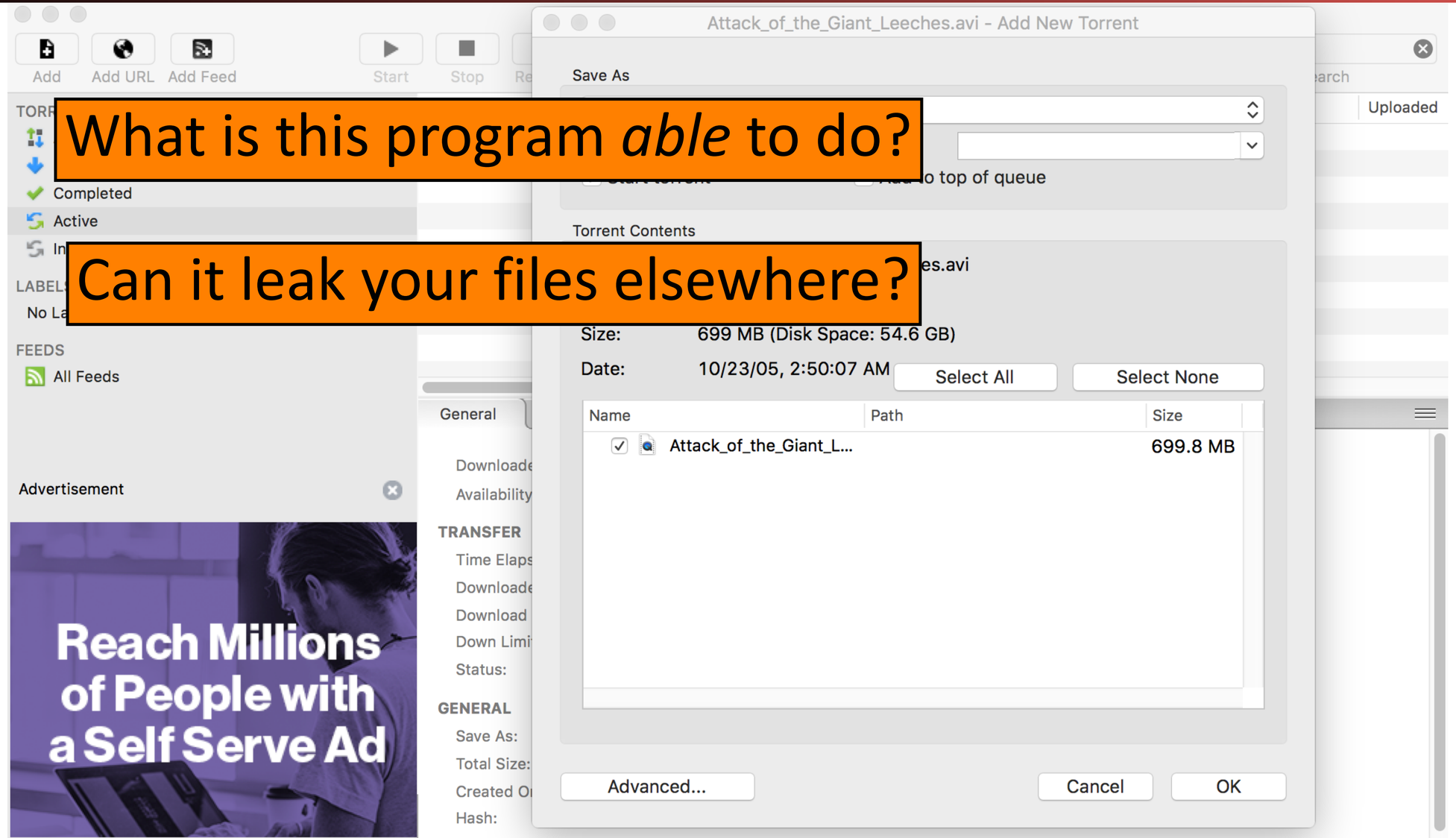
More results from utorrent.com »

uTorrent (Mac) - Free download
https://utorrent.en.softonic.com/mac
★★★☆☆ Rating: 3 - 550 votes - Free - Mac OS - Utilities/Tools
uTorrent, free download. **uTorrent** 1.8.6: Super lightweight torrent client for **Mac**. **uTorrent** for **Mac** is a lightweight and efficient BitTorrent client that allows you to ...


uTorrent.dmg
IMPORTANT - Read this License Agreement carefully before clicking on the "Agree" button. By clicking on the "Agree" button, you agree to be bound by the terms of the License Agreement.
LICENSE AGREEMENT
Please review the license terms before installing µTorrent
µTorrent (also known as uTorrent) is a peer-to-peer file sharing application distributed by BitTorrent, Inc.
By accepting this agreement or by installing µTorrent, you agree to the following µTorrent-specific terms, notwithstanding anything to the contrary in this agreement.
License.
Subject to your compliance with these terms and conditions, BitTorrent, Inc. grants you a royalty-free, non-exclusive, non-transferable license to use µTorrent, solely for your personal, non-commercial purposes. BitTorrent, Inc. reserves all rights in µTorrent not expressly granted to you here.
Restrictions.
The source code, design, and structure of µTorrent are trade secrets. You
Print
Save...
Disagree
Agree

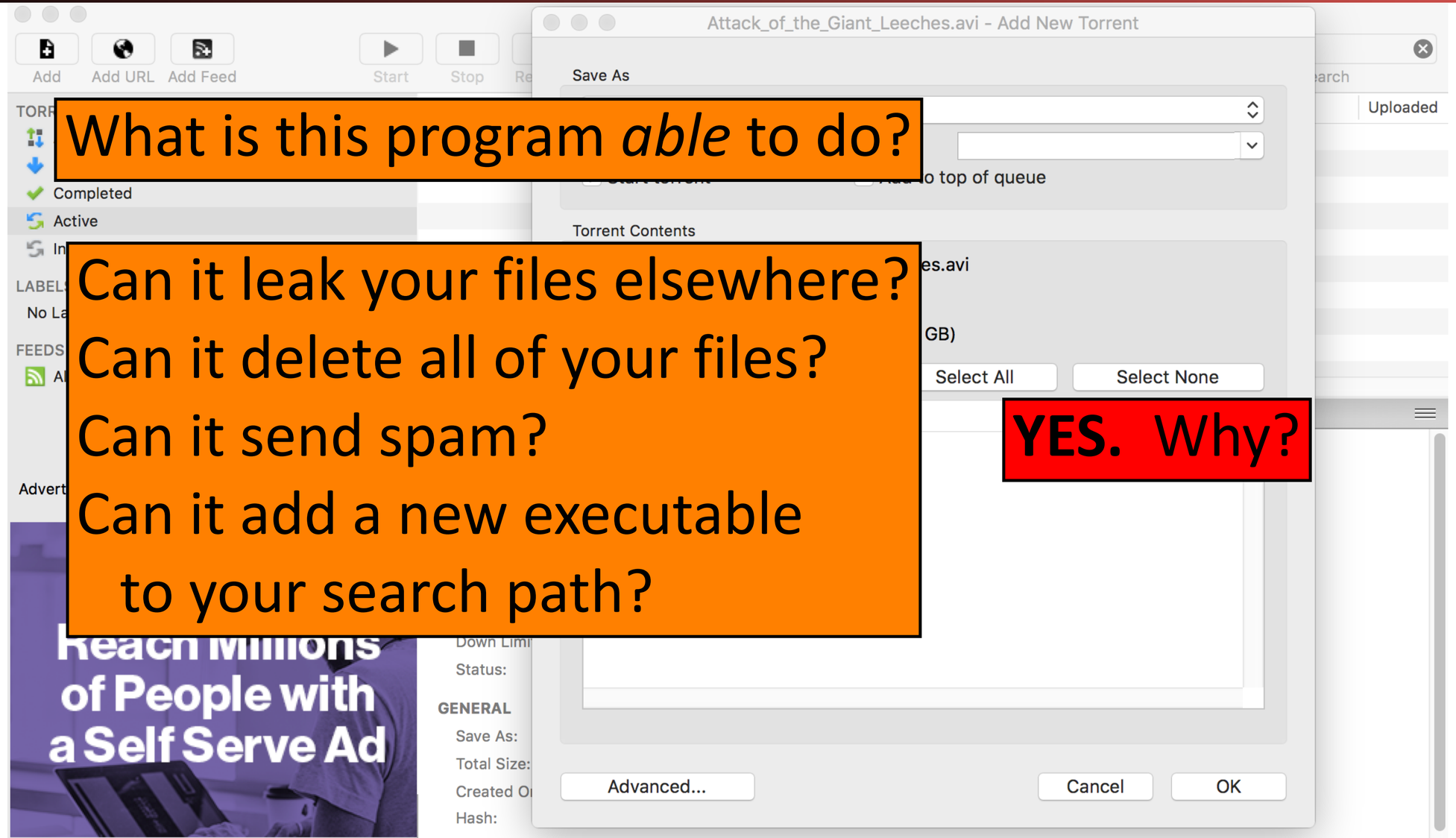

uTorrent
2 items
uTorrent
Applications
LIGHT. LIMITLESS. ENGINEERED FOR
POWERFUL DOWNLOADING.


µTorrent
Add
Add URL
Add Feed
Start
Stop
Remove
Upgrade Now
piracy
Search
TORRENTS
All
Downloading
Completed
Active
Inactive
LABELS
No Label
FEEDS
All Feeds
Name
#
Size
Done
Status
Seeds
Peers
↓ Speed
↑ Speed
ETA
Uploaded
General
Trackers
Files
Peers
Speed
Downloaded:
Availability:
TRANSFER
Time Elapsed:
Remaining:
Wasted:
Downloaded:
Uploaded:
Seeds:
Download Speed:
Upload Speed:
Peers:
Down Limit:
Up Limit:
Share Ratio:
Status:
GENERAL
Save As:
Total Size:
Pieces:
Created On:
Hash:
Advertisement
Reach Millions of People with a Self Serve Ad



What is this program *able* to do?

Can it leak your files elsewhere?



What is this program *able* to do?

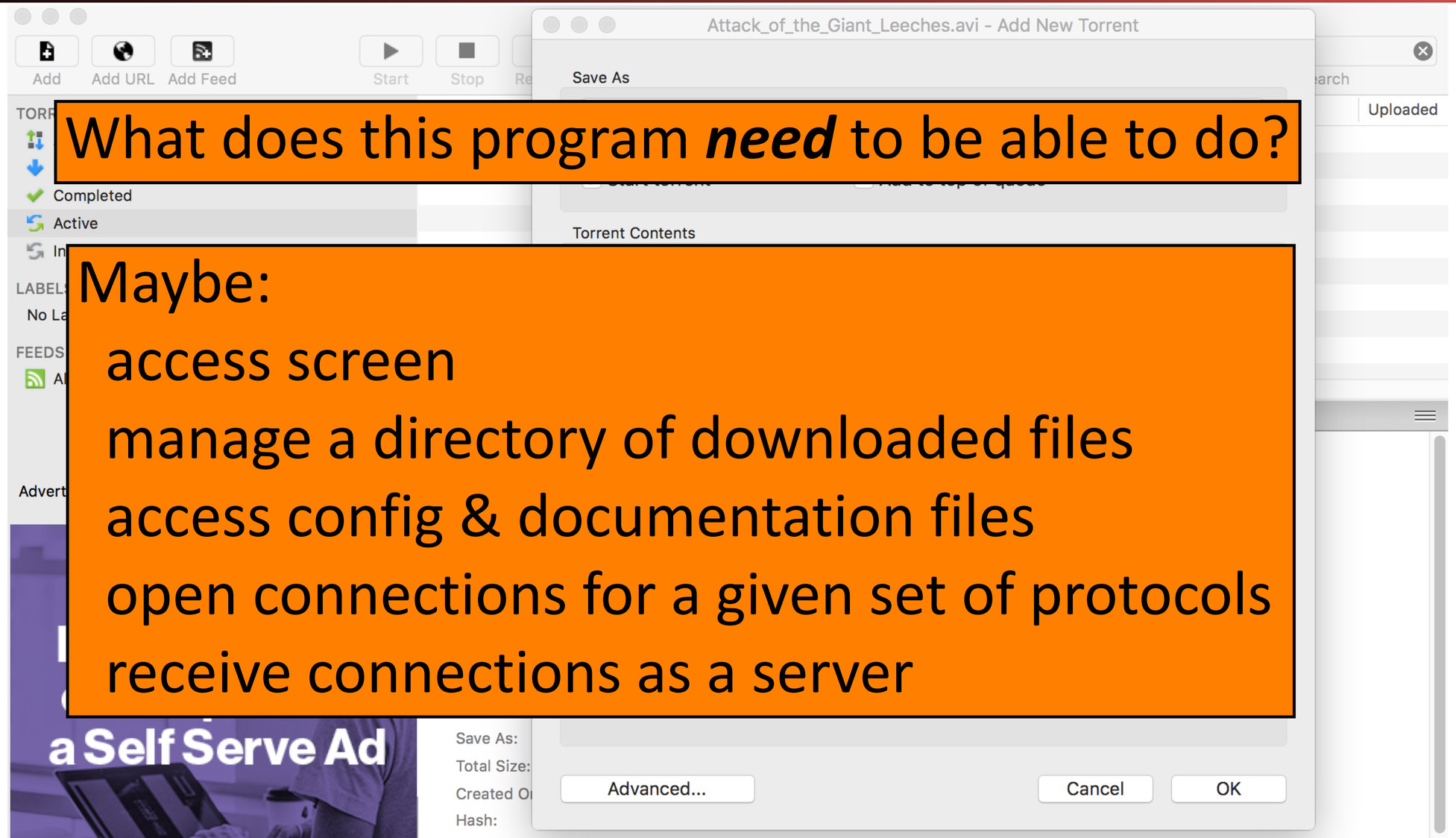
Can it leak your files elsewhere?

Can it delete all of your files?

Can it send spam?

Can it add a new executable to your search path?

YES. Why?



What does this program ***need*** to be able to do?

Maybe:

- access screen
- manage a directory of downloaded files
- access config & documentation files
- open connections for a given set of protocols
- receive connections as a server

Check for Understanding

- We've seen that laptop/desktop platforms grant applications a lot of privileges

- Quiz: Name a platform that does a better job of least privilege

So What Do You Think Here?