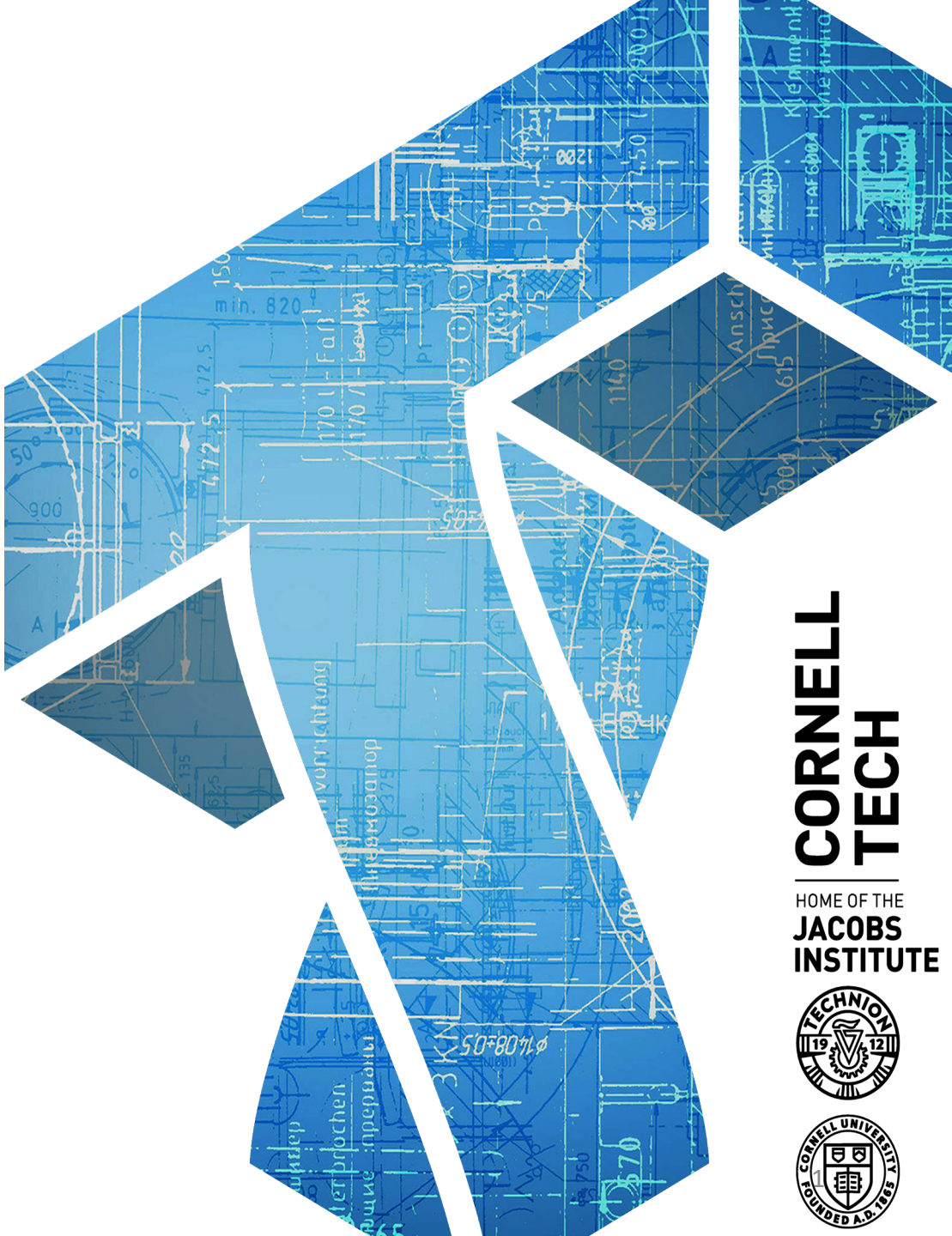
CS 5435
Computer Security
aka
“Security and Privacy in the Wild”

Instructor: Tom Ristenpart

https://github.com/tomrist/cs5435-fall2019



CORNELL TECH

HOME OF THE JACOBS INSTITUTE

Who am I? https://rist.tech.cornell.edu

- Academic computer security researcher
  - ~7 years of grad school at UC Davis & UC San Diego
  - 4.5 years as professor at University of Wisconsin-Madison
  - 4+ years as professor at Cornell Tech

- Applied & theoretical cryptography, cloud computing security, machine learning privacy, user authentication

- Recently: technology privacy and safety in intimate partner violence settings
  - https://ipvtechresearch.org

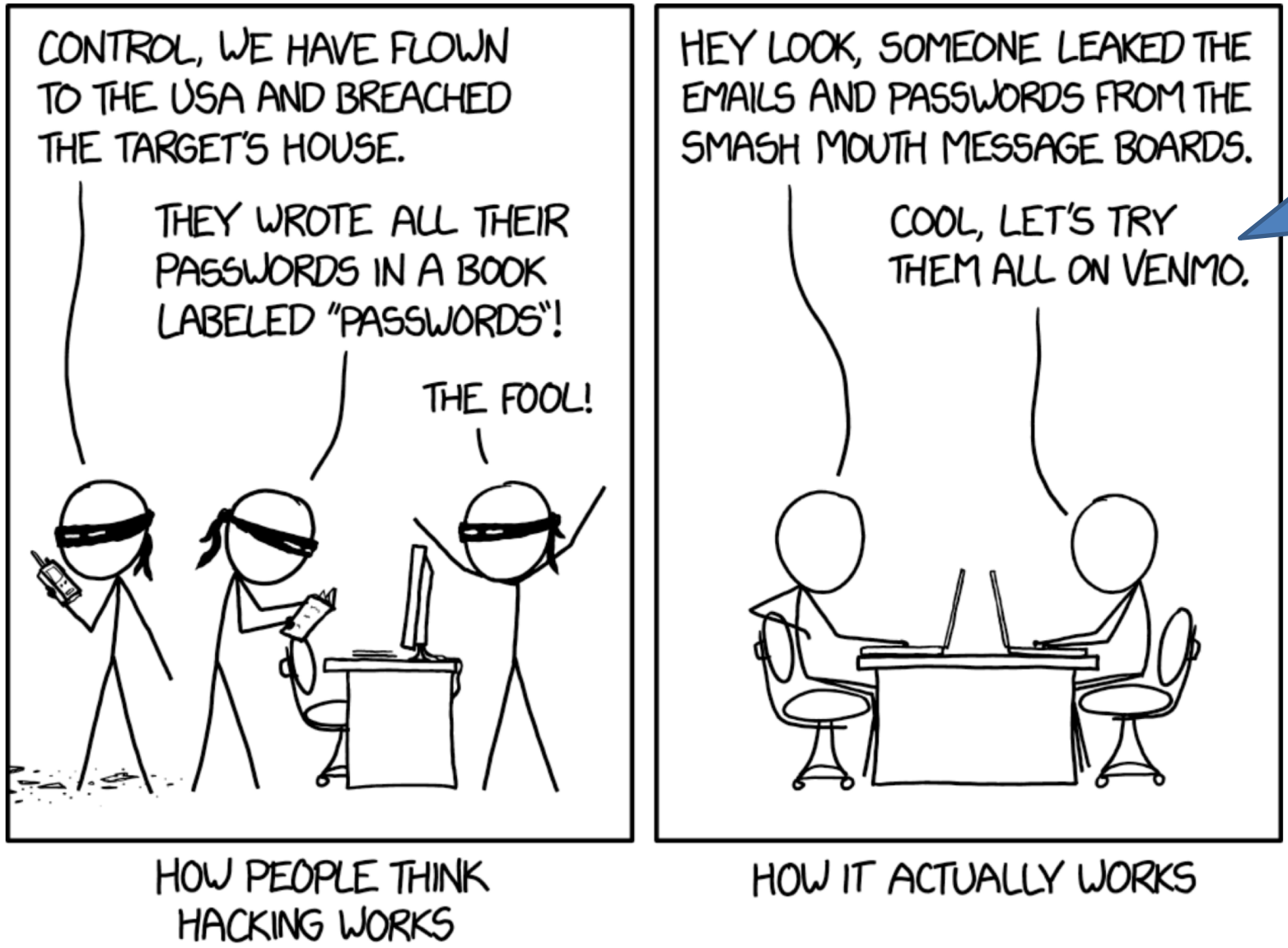
Computer security

understanding and improving the behavior of computing technologies in the presence of adversaries

Attackers

Target/victim computing systems

Defenders (designers, engineers, lawyers, etc.)



Credential stuffing attack

https://xkcd.com/2176/

MOTHERBOARD
TECH BY VICE

Hackers Breach Forum Of Popular Webcomic 'XKCD'

The data breach affected 560,000 users.

By **Lorenzo Franceschi-Bicchierai**

Sep 3 2019, 10:35am Share Tweet

Entity	Year	Records	Organization type	Method	Sources
Yahoo	2013	3,000,000,000	web	hacked	[318][319]
First American Corporation	2019	885,000,000	financial service company	poor security	[124]
Facebook	2019	540,000,000	social network	poor security	[121]
Marriott International	2018	500,000,000	hotel	hacked	[187][188]
Yahoo	2014	500,000,000	web	hacked	[320][321] [322][323][324]
Friend Finder Networks	2016	412,214,295	web	poor security / hacked	[125][126]
Truecaller	2019	299,055,819	Telephone directory	unknown	[277][278]
Massive American business hack including 7-Eleven and Nasdaq	2012	160,000,000	financial	hacked	[189]
Adobe Systems	2013	152,000,000	tech	hacked	[9][10]
Under Armour	2018	150,000,000	Consumer Goods	hacked	[292]

https://en.wikipedia.org/wiki/List_of_data_breaches

2010: “Highly sophisticated and targeted attack”

2011:
“Advanced persistent threat”

2011:
Bad crypto = cracked PS3
Play station network down

How do we approach computer security?

1. Understand what are a system's ***security goals***

2. Learn to spot security ***vulnerabilities***

3. Think through how ***attacks*** would play out

4. Understand and deploy ***countermeasures***

Security goals

Confidentiality	Data not leaked
Integrity	Data/service not modified
Authenticity	Data/action comes from who we think it does
Availability	Service available when needed

Threat modeling

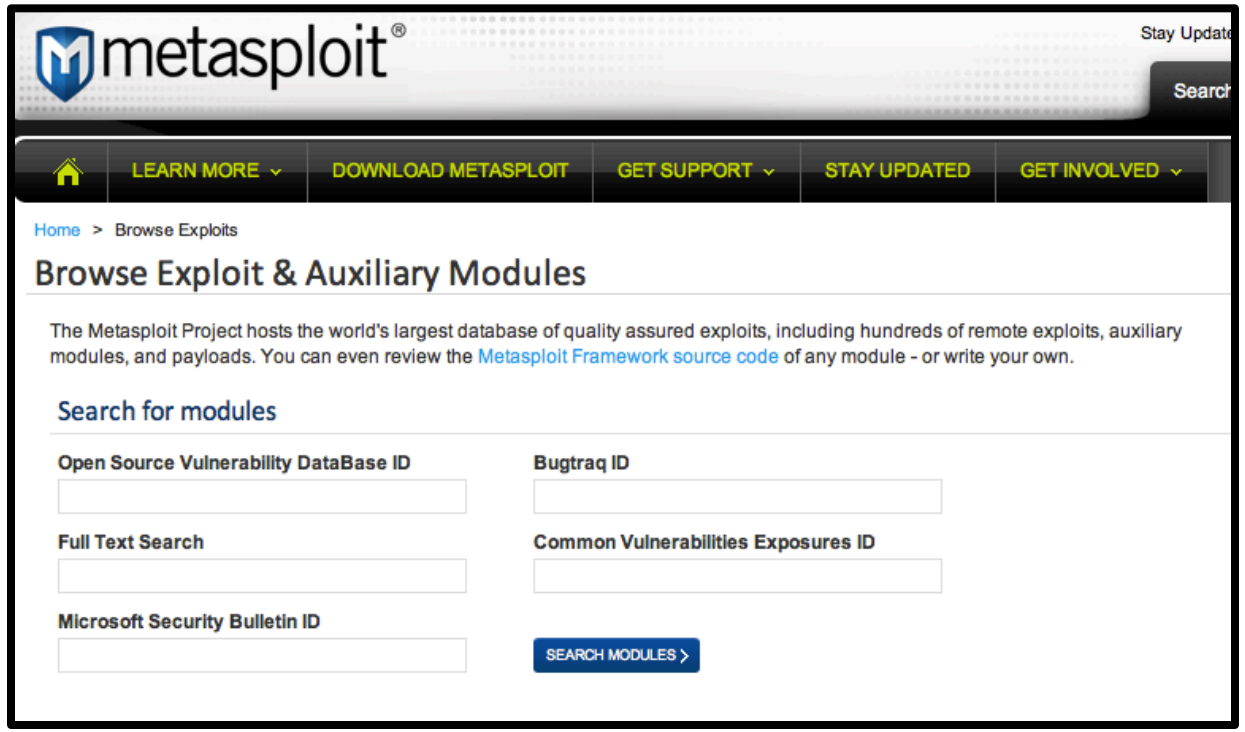
Who are the adversaries?
What are their goals?
What are their capabilities?

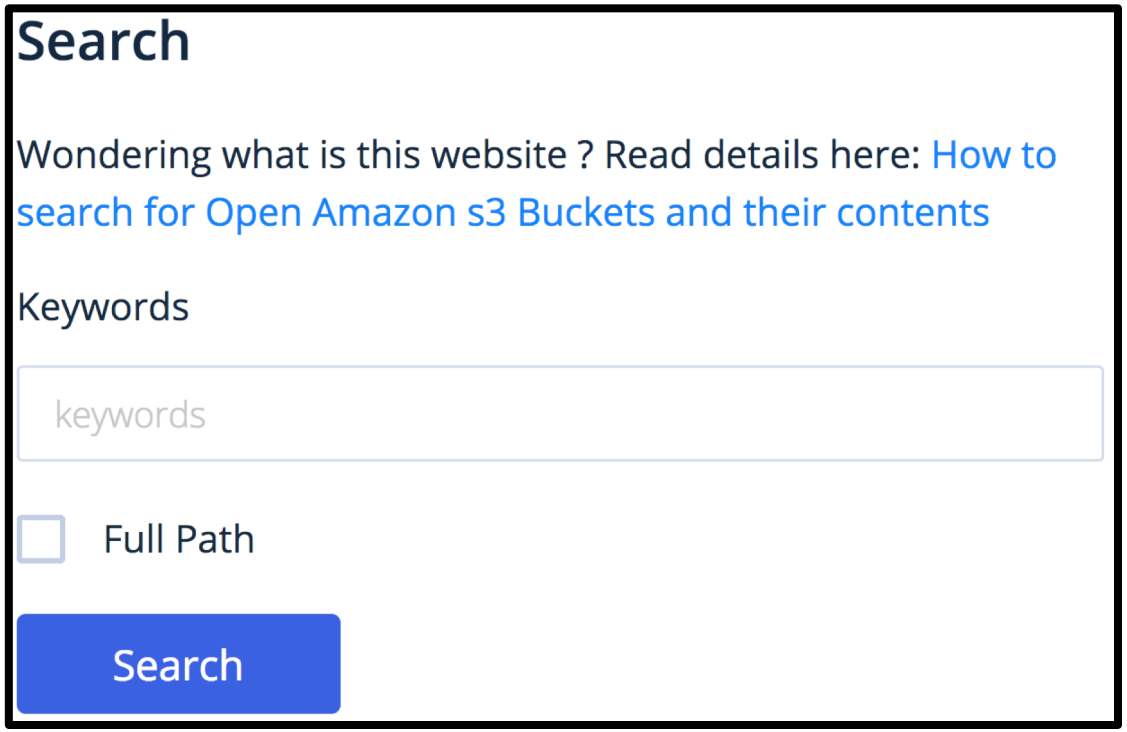
Who are the adversaries?

- “31337” script kiddies
- Abusers / harassers / cyberstalkers
- “Hacktivists”
- Criminals (often economically motivated)
- Nation states

“Hacking” commoditized in tool form

- Metasploit
  - All-in-one penetration testing tool
  - Easy-to-use exploit libraries
- Amazon S3 buckets public
  - Source of many data breaches of late





Abusers / harassers / stalkers

- “Cyberbullying”
- Online stalkers, remote access trojan (RATs)
- Intimate partner violence (IPV) widespread issue
  - 1 out of 4 women, 1 out of 9 men suffer at some point in lives
  - Tech abuse rampant:
    - Account compromise
    - Spyware
    - Social media harassment
    - …

Technologically simple-to-mount attacks, ***very*** hard to mitigate

“Hacktivists”:
Anatomy of an example attack in 2011

http://arstechnica.com/tech-policy/news/2011/02/anonymous-speaks-the-inside-story-of-the-hbgary-hack.ars/1

Anonymous vs HBGary

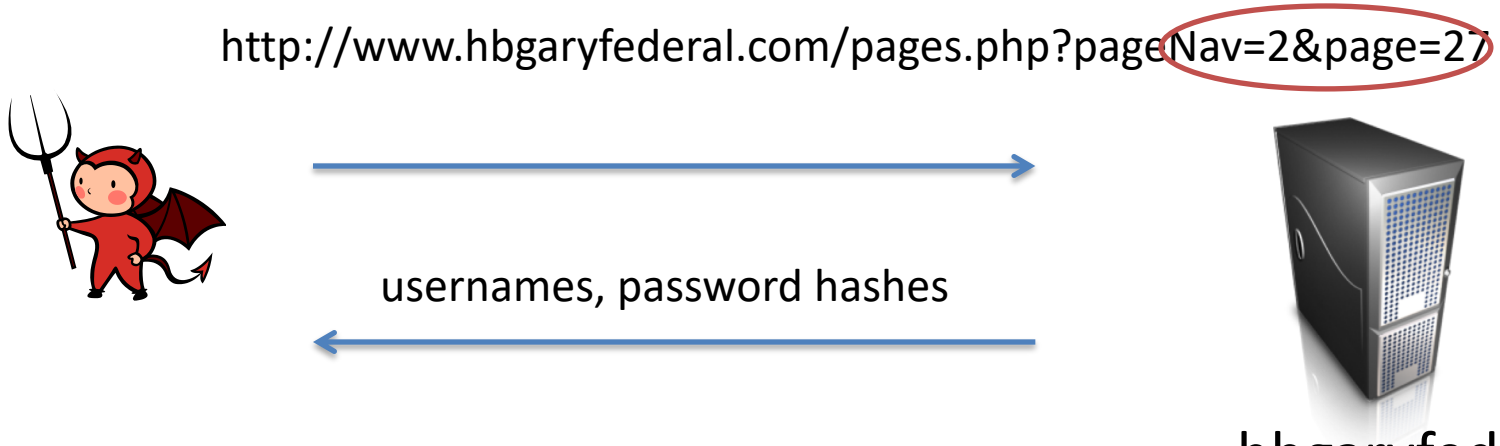
hbgaryfederal.com

Gmail

rootkit.com

Ran by Greg Hoglund,
owner of HBGary / HBGary Federal

Anonymous vs HBGary



SQL injection attack

h = Hash(pw)

Given hash h, recover pw by brute force attack if pw is “simple” enough & Hash function weak (CMS used MD5, no salts! Exceedingly weak)

Used vulnerable content-management system (CMS) (like Wordpress, Joomla, Drupal)

Ted Vera (COO) and Aaron Barr (CEO of HBGary) had passwords only 6 digits, lower case letters and numbers

JohntheRipper easily inverts hashes of such passwords

http://www.openwall.com/john/

Using Ted's access credential: SSH access

login: ted
password: tedv12

hbgaryfederal.com

COO Ted used same password for SSH,
gave user level access to Linux system

Exploited privilege escalation vulnerability
in the glibc linker on Linux

http://seclists.org/fulldisclosure/2010/Oct/257

Attack in 2011:
System not up-to-date on patches

Now have root access on hbgaryfederal.com
Delete gigabytes of data, grab emails, take down phone system

Using Aaron's access credential: Gmail control

login: aaron
password: aaro34

CEO Aaron used same password for gmail account

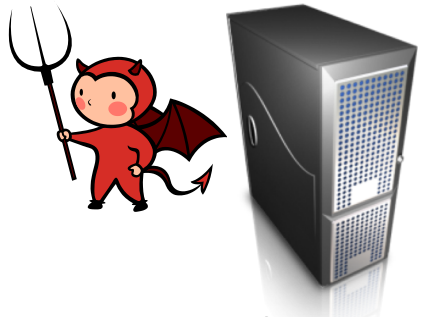
Aaron was administrator for companies' email on Google apps

Full control over Owner Greg's email account

Using Gary's email: access to rootkit.com

From: Greg
To: Jussi
Subject: need to ssh into rootkit
im in europe and need to ssh into the server. can you drop open up firewall and allow ssh through port 59022 or something vague?
and is our root password still 88j4bb3rw0cky88 or did we change to 88Scr3am3r88 ?
thanks

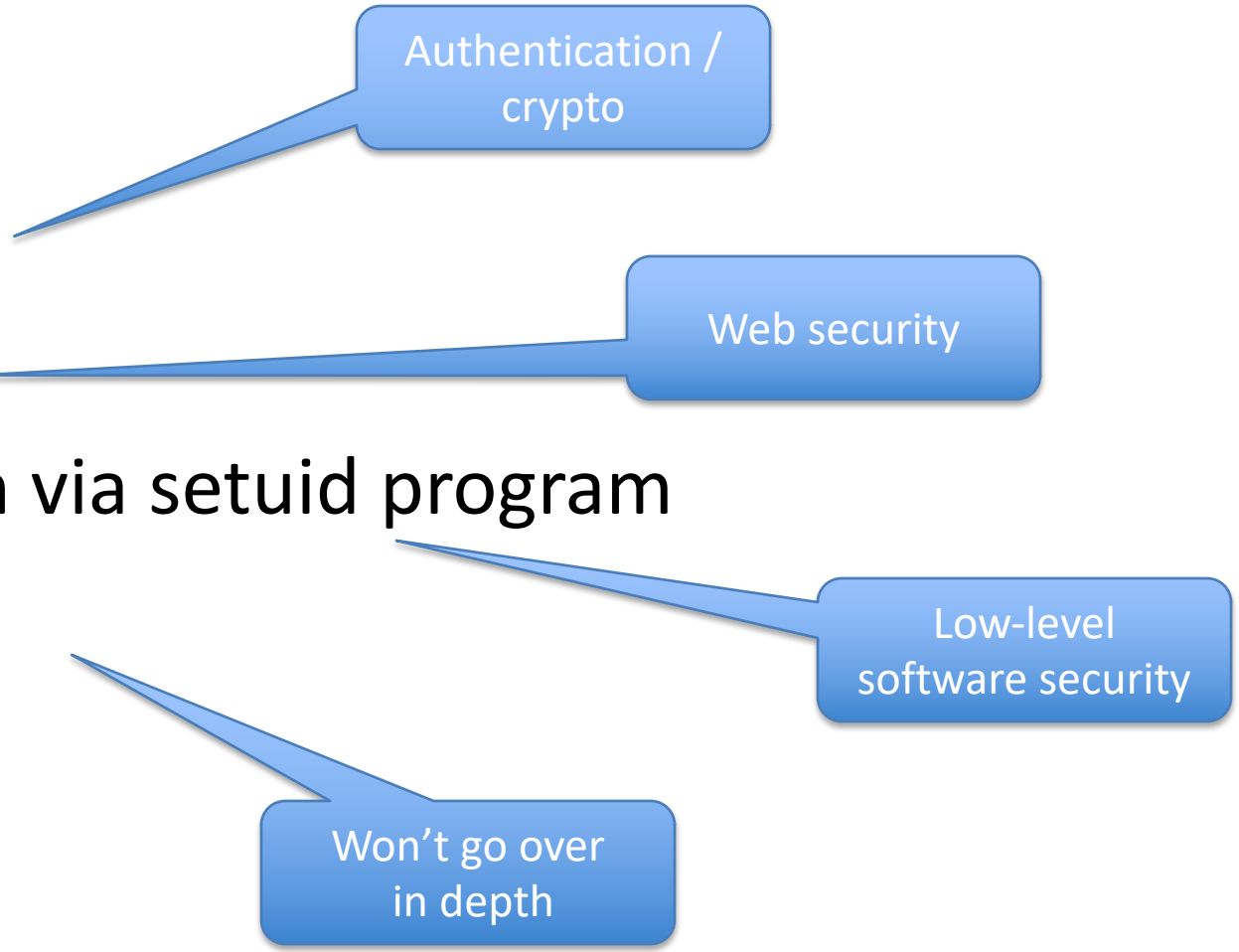
"social engineering"



rootkit.com

Recap:

- Password cracking
- SQL injection
- Privilege escalation via setuid program
- Social engineering



Who are the adversaries?

- “31337” script kiddies
- Abusers / harassers / cyberstalkers
- “Hacktivists”
- Criminals (often economically motivated)
- Nation states

Economically motivated criminals

Economically motivated criminals

- WannaCry Infected >230,000 machines in 150 countries
- Disrupted service at 16 hospitals in United Kingdom, also affected FedEx, Telefonica, Russian Interior Ministry, Honda, ...

- Attribution and provenance complicated:
  - Used EternalBlue exploit against Windows, attributed to USA's National Security Agency
  - Part of USA zero day exploits stolen and leaked onto pastebin by ***The Shadow Brokers*** (Russians?)
  - USA, UK, and Australia officially claim North Korea behind WannaCry

Economically motivated criminals

Android exploits are now worth more than iOS exploits for the first time

Exploit broker Zerodium increases zero-day prices for Android, now worth more than iOS.

By Catalin Cimpanu for Zero Day | September 3, 2019 -- 15:56 GMT (08:56 PDT) | Topic: Security

Computer security & international conflict

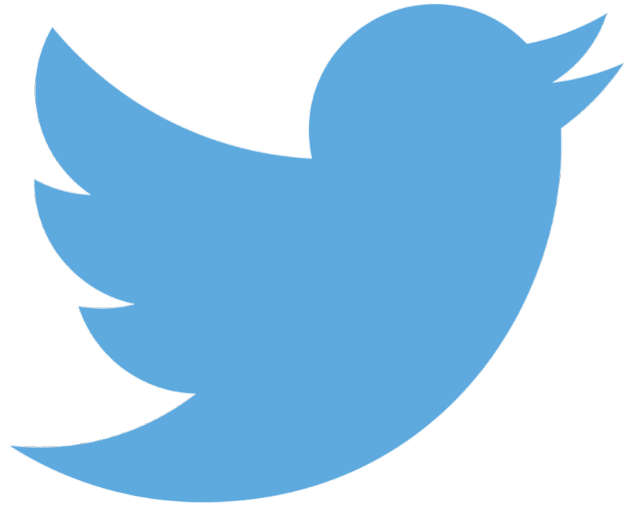
Photo credit: Magnolia Pictures

U.S. Air Force photo by Bobbi Zapka

Computer security & international conflict

- Internet Research Agency
  - St. Petersburg firm ran online influence operations during 2016 presidential election in USA
  - Uses fake accounts (“sockpuppets”)

- Hack of Democratic National Committee
  - Email leaks via Guccifer 2.0, WikiLeaks, etc.



- Hong Kong protests misinformation campaign by accounts emanating from China about

https://en.wikipedia.org/wiki/Russian_interference_in_the_2016_United_States_elections

Themes in this course

- Understanding threats
- Security evaluations (thinking like an attacker)
- Defense approaches
- Advancing our technical skills
  - Web technologies
  - Networking
  - x86 assembly, low-level programming
  - …

Running example: a simple web service

Client devices
with web browser
or app

Network
(the internet)

Virtual machine (VM)

Web backend
(Python scripts)

Support utilities
(Shell scripts,
programs)

Network or
local

Database
(e.g., SQL)

Course organization: Web Service Example

- Authentication, passwords
- Abuse
- Web security
- Network security
- Brief intro to cryptography
- Operating systems security
- Memory corruption vulnerabilities (e.g., buffer overflows)
- Database security, virtualization & cloud security

Ethics and computer security

We will be learning how attackers break into computer systems

Black hat: criminal

Grey hat: sometimes criminal, or at least “bending the law”

White hat: ethical hacker, working within legal framework to perform security evaluations

Rules of thumb

- When in doubt … don't
  - Find someone to talk to (me or a TA)

- You must have explicit (written) permission from a system owner before performing any penetration testing
  - Homework assignments will generally be on your own system
  - We will give explicit permission to hand us exploits for us to test

Responsible disclosure

- **Full disclosure** means revealing everything about a vulnerability including an example exploit

- **Responsible disclosure** (generally) refers to ensuring potential victims are aware of vulnerabilities before going public

Security Update for Gray GoPayment Card Reader

We recently learned from the University of Wisconsin, Madison about a security vulnerability with the gray GoPayment credit card reader made by our partner ID TECH. As soon as we learned about this vulnerability, we immediately started working with the university and ID TECH to test it and ensure that our GoPayment customers were not at risk.

http://security.intuit.com/alert.php?a=51

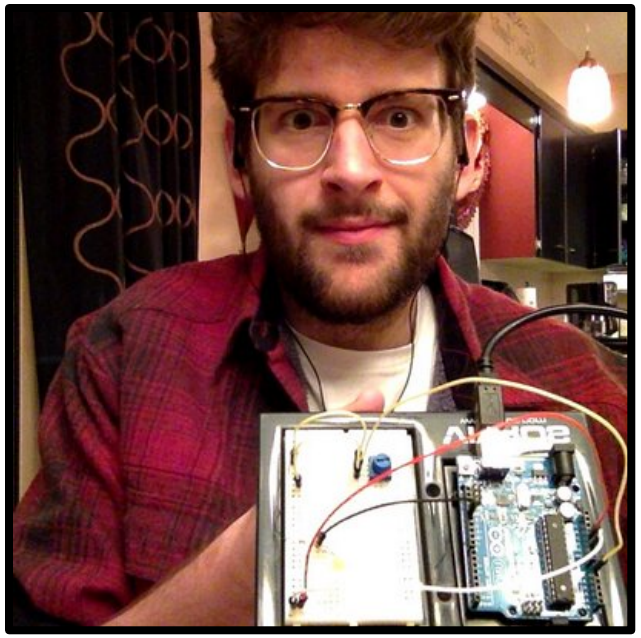
- Notified companies when we had a draft of paper finished
- Worked with them to ensure they could fix vulnerabilities
- Full disclosure at presentation at workshop

Administrative stuff

- https://github.com/tomrist/cs5435-fall2019
- Piazza instance setup
- CMS for turning in homeworks

- 4 homework assignments (60%)
- Prelim/midterm (20%)
- Final (20%)

Teaching team



Paul Grubbs

Bijeeta Pal

Nirvan Tyagi

Graders: Kaveesha Shah, Andy Zhang, Vignesh Rao, Larissa Pereir

Homeworks

- Can work with one partner, if you want to
- Collaboration policy:
  - no collaboration with people outside team
  - using the web for general information is encouraged
  - Googling for answers to questions is not
- Need access to virtualization software (e.g., VirtualBox), will help you setup in Homework 1
- Cheating such as plagiarizing homework answers or copying code will trigger disciplinary actions

Exams

- One in-class midterm
- One in-class final
- Short answer questions

Next time:

- Account security and authentication
- Passwords
- Password guessing attacks

A warm up: security principles

Saltzer and Schroeder.
The protection of information in computer systems.
Proceedings of the IEEE, 1975

1) Economy of mechanism
2) Fail-safe defaults
3) Complete mediation
4) Open design
5) Separation of privilege
6) Least privilege
7) Least common mechanism
8) Psychological acceptability