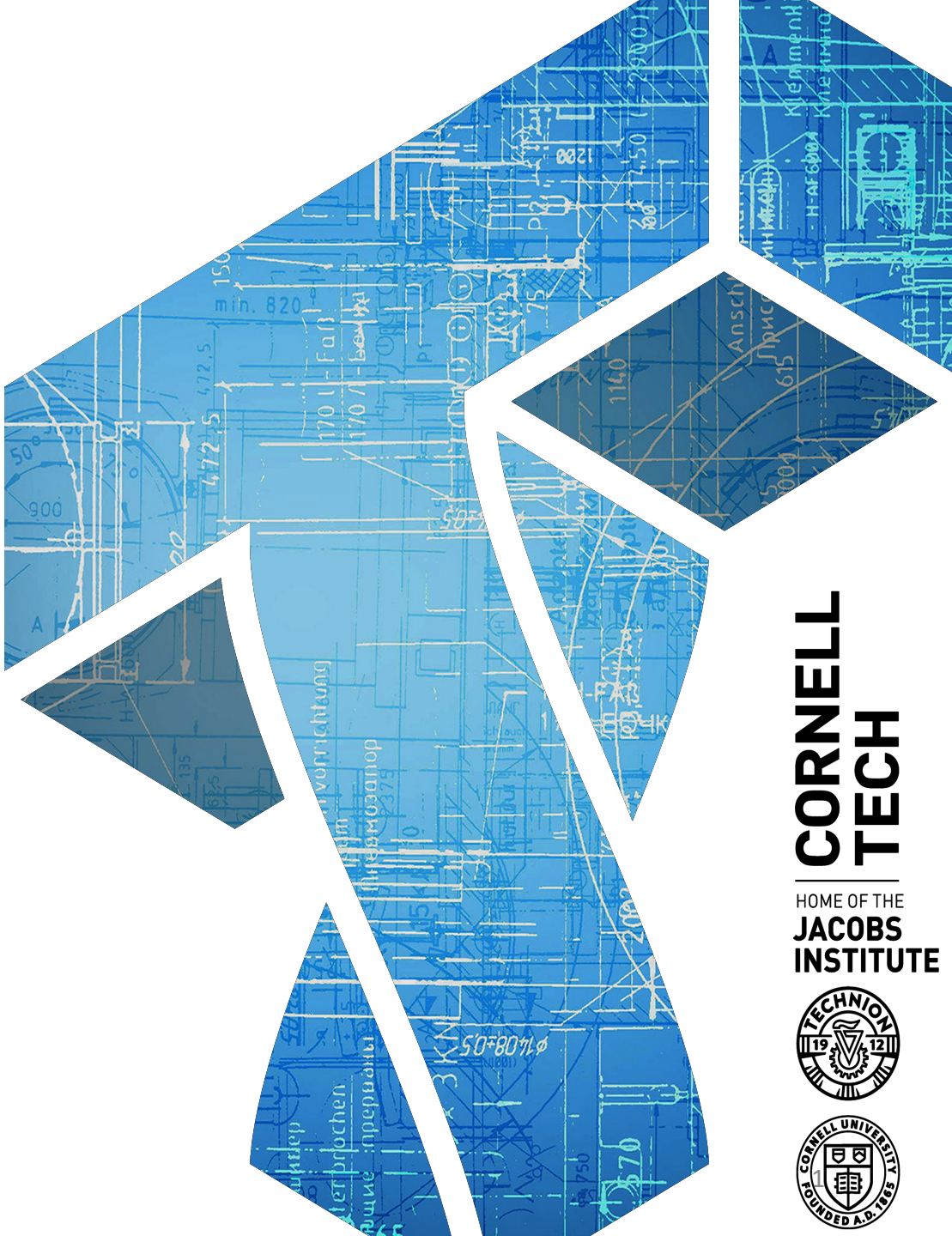
CS 5435
Computer Security
aka
“Security and Privacy in the Wild”

Instructor: Tom Ristenpart

https://github.com/tomrist/cs5435-spring2024



CORNELL TECH

HOME OF THE JACOBS INSTITUTE

So far in 2024…

North Korea's ScarCruft APT group targets infosec pros

News Analysis

Jan 22, 2024 • 6 mins

Advanced Persistent Threats | Phishing

Top U.S. cybersecurity watchdog issues emergency directive to federal agencies about popular software

The directive ordered agencies to patch the software that allows for remote work.

What Microsoft's hack means for its $20 billion cybersecurity franchise and its rivals

PUBLISHED MON, JAN 22 2024•2:30 PM EST | UPDATED MON, JAN 22 2024•2:34 PM EST

Computer security

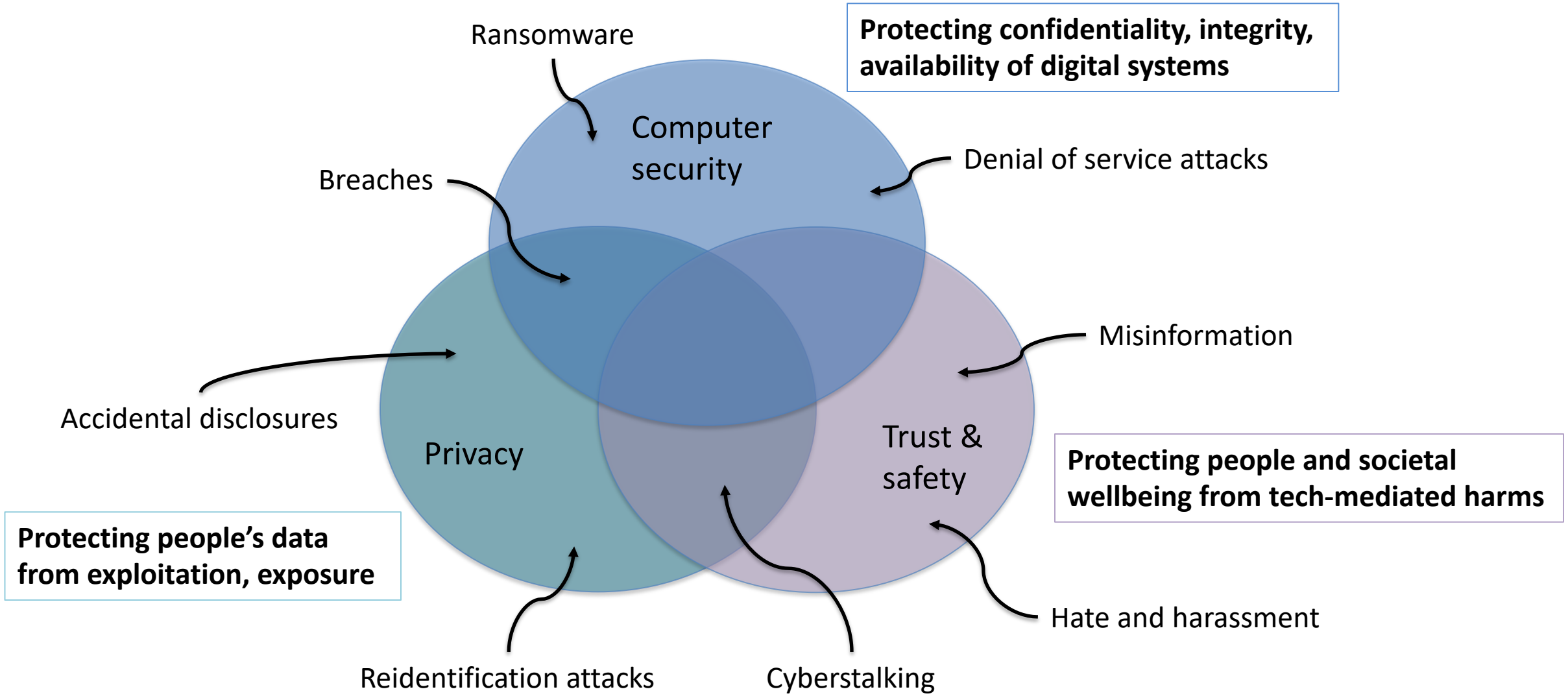
understanding and improving the behavior of computing technologies in the presence of adversaries

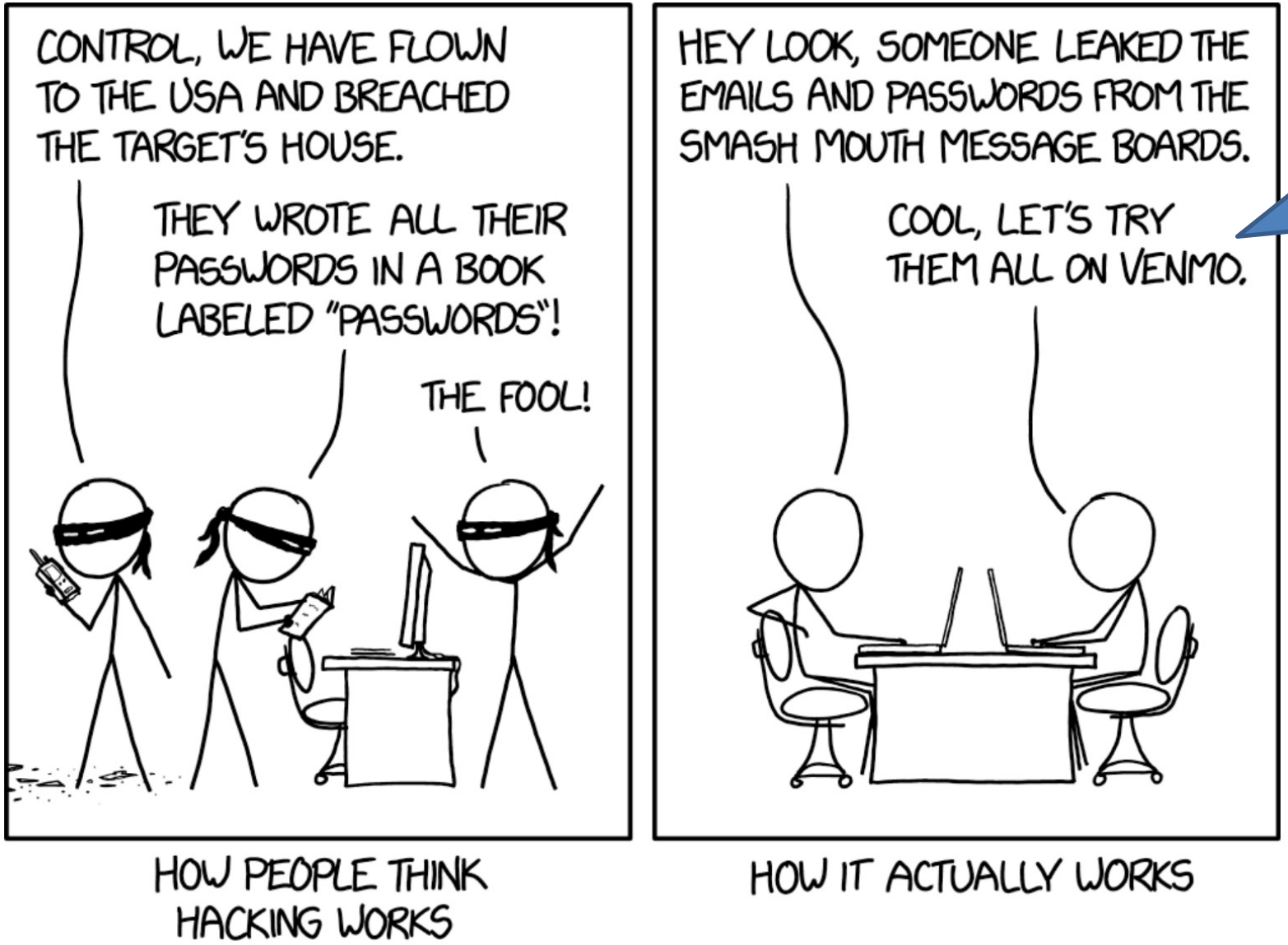
Attackers

Target/victim computing systems

Defenders (designers, engineers, lawyers, etc.)

The expanding world of computer security





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

2010: “Highly sophisticated and targeted attack”

2011:
“Advanced persistent threat”

2011:
Bad crypto = cracked PS3
Play station network down

Entity	Year	Records
Yahoo	2013	3,000,000,000
Verifications.io (total leaks)	2019	2,000,000,000
First American Corporation	2019	885,000,000
India Government Aadhar data breach	2023	810,000,000+
Verifications.io (first leak)	2019	809,000,000
Collection No. 1	2019	773,000,000
Facebook	2019	540,000,000
Marriott International	2018	500,000,000
Yahoo	2014	500,000,000
Friend Finder Networks	2016	412,214,295
Exactis	2018	340,000,000
Airtel	2019	320,000,000
Truecaller	2019	299,055,000
MongoDB	2019	275,000,000
Wattpad	2020	270,000,000
Facebook	2019	267,000,000
Microsoft	2019	250,000,000

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

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

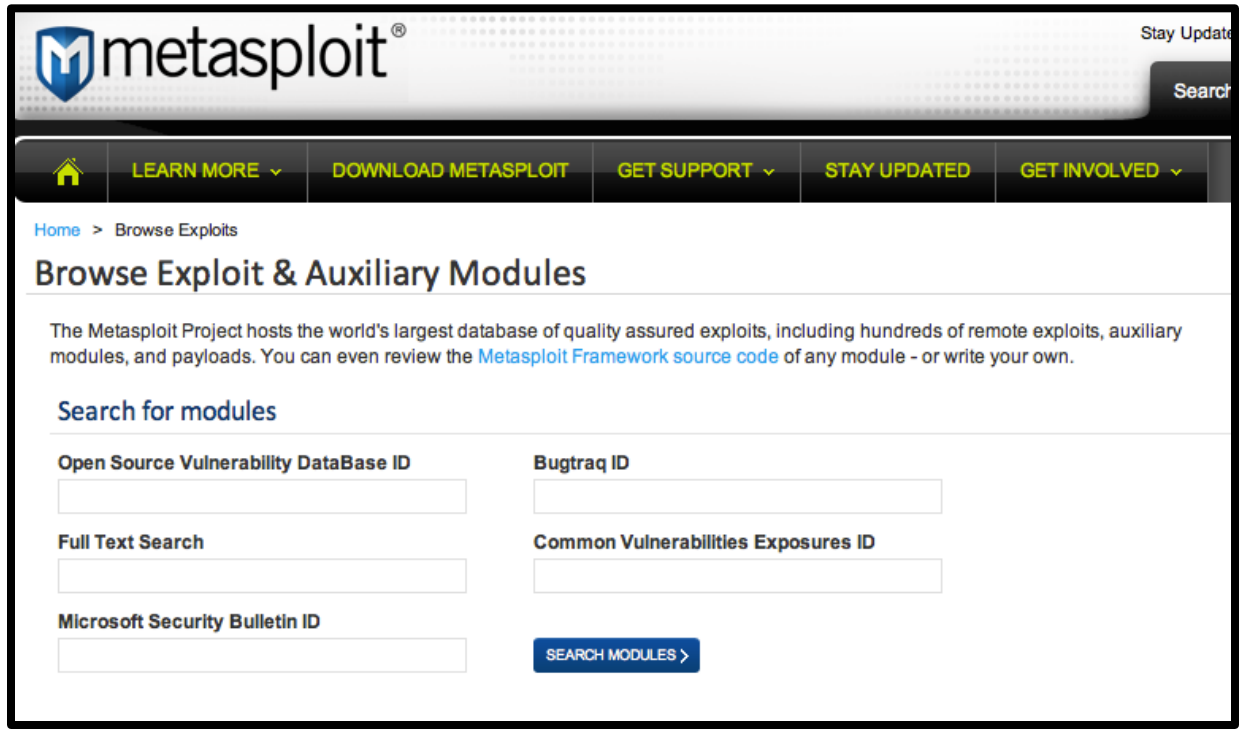
Who are the adversaries?
What are their goals?
What are their capabilities?

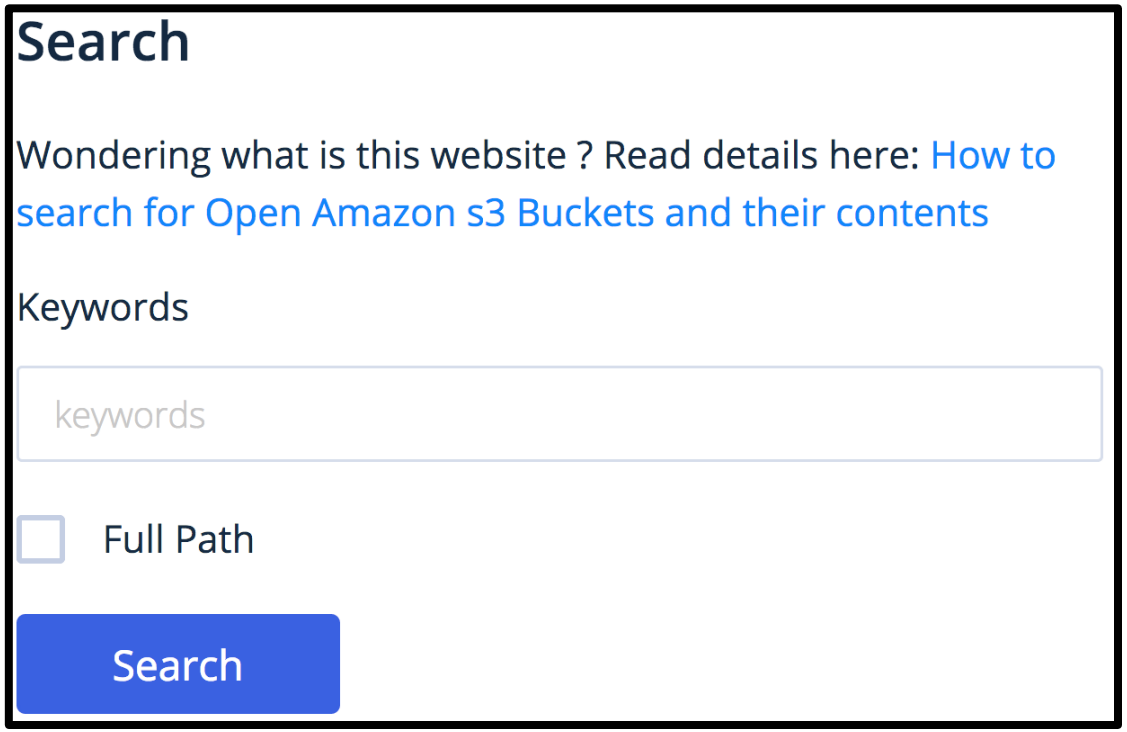
Who are the adversaries?

- “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





About S3: The Story of a Hack

https://slate.com/technology/2020/08/uber-joseph-sullivan-charged-data-breach.html

- **2014**: Uber's source code on GitHub accessed using stolen credentials… in the source code, keys to all Uber's S3 databases
- Mistake #1: hardcoded access credentials ← Solution: rotate keys
- **2016**: Uber's driver database stolen using the same credentials

> In the document that Uber used to track the progress of its investigation of the 2016 breach, one team member commented on Nov. 14, "access key has not be rotated [sic] since [it was created in 2013]. None of the people are at the company any longer. Task was to rotate keys within S3 to ensure this could not happen in the future but there are thousands of tasks. Joe was just deposed on this specific topic and what the best or minimum practices that any company should follow in this area."

How Not to Handle a Data Breach

https://slate.com/technology/2020/08/uber-joseph-sullivan-charged-data-breach.html

- **2016**: Uber pays hackers $100,000 via Bitcoin as a “bug bounty”, covers up the hack
- **2019**: hackers plead guilty to trying to extort Uber and LinkedIn in exchange for promise to delete data they stole from S3
- **2020**: US Dept of Justice charges Uber’s former Chief Security Officer with obstruction of justice

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

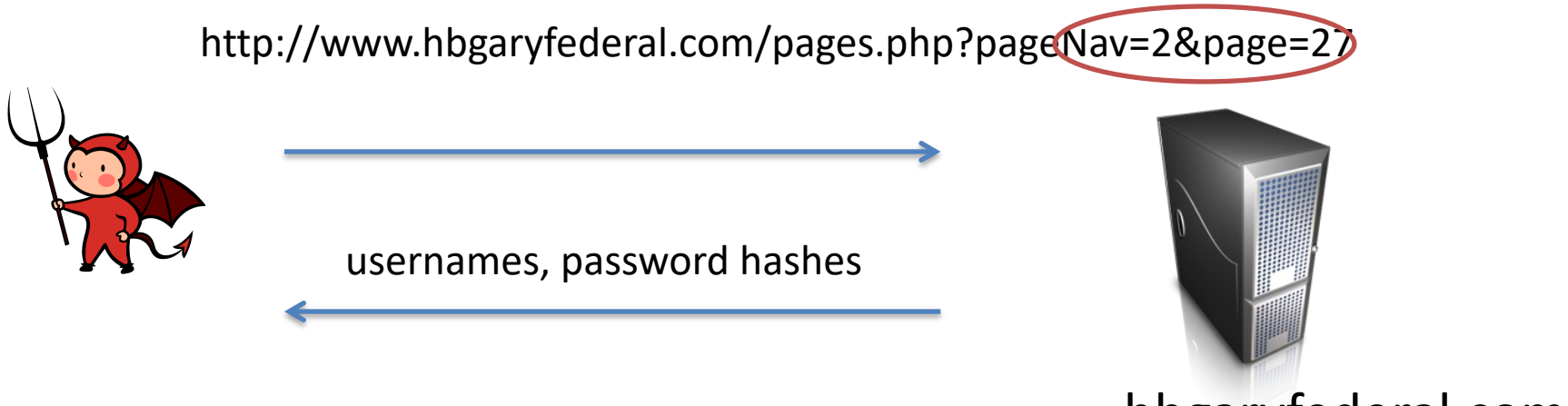
hbgaryfederal.com

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

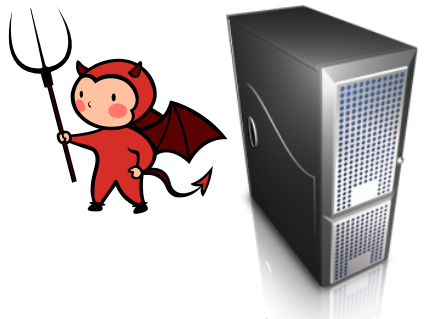
Aaron was administrator for companies' email on Google apps

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

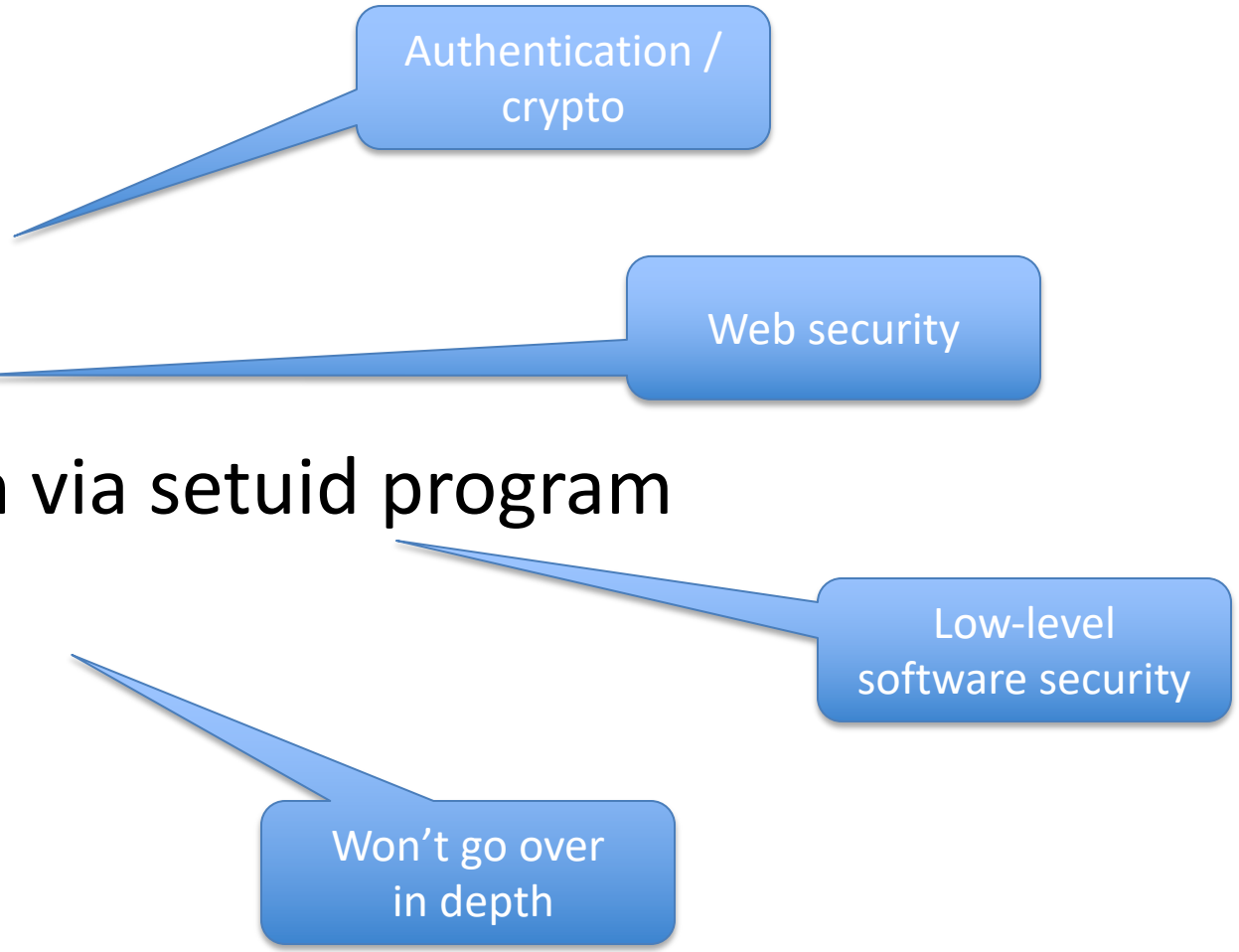
"social engineering"



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

Colonial Pipeline paid 75 Bitcoin, or roughly $5 million, to hackers.

Marketplace for Vulnerabilities

Bug bounty programs

- Google, Facebook, Microsoft: up to $20-100K per bug
- Uber breach

Vulnerability brokers

Gray and black markets

- Over $1,000,000 for iOS and Android zero-days

Payouts Changelog

Changes as of Sep. 13, 2018:

Bounties for both Desktops/Servers and Mobile exploits were updated with new entries and increased payouts.

Modification	Details
New Entries (**Servers/Desktops**)	**$100,000** - nginx RCE i.e. remote exploits via HTTP(S) requests or related protocols **$100,000** - Exim RCE i.e. remote exploits via a malicious email or related vectors **$80,000** - cPanel, Webmin, Plesk RCE i.e. remote pre-auth exploits for major control panels **$50,000** - BSD LPE i.e. privilege escalation for NetBSD, OpenBSD, or FreeBSD **$30,000** - WinRAR, 7-Zip, WinZip, tar RCE i.e. code execution via a malicious archive file
Increased Payouts (**Servers/Desktops**)	**$500,000** - Windows RCE (Zero Click) e.g. via SMB or RDP packets (previously: **$300,000**) **$250,000** - Apache or MS IIS RCE i.e. remote exploits via HTTP(S) requests (previously: **$150,000**) **$250,000** - Chrome RCE + SBX (Windows) including a sandbox escape (previously: **$150,000**) **$150,000** - Outlook RCE i.e. remote exploits via a malicious email (previously: **$100,000**) **$150,000** - PHP or OpenSSL RCE (previously: **$100,000**) **$150,000** - MS Exchange Server RCE (previously: **$100,000**) **$100,000** - Dovecot, Postfix, Sendmail RCE (previously: **$50,000**) **$100,000** - VMWare ESXi VM Escape i.e. guest-to-host escape (previously: **$80,000**) **$100,000** - Chrome RCE without a sandbox escape (previously: **$50,000**) **$100,000** - Egde RCE + SBX including a sandbox escape (previously: **$80,000**) **$100,000** - MS Word/Excel RCE i.e. exploit via a malicious Office document (previously: **$50,000**) **$100,000** - Thunderbird RCE i.e. remote exploits via a malicious email (previously: **$80,000**) **$80,000** - WordPress (Core) RCE i.e. remote pre-auth exploits (previously: **$50,000**) **$50,000** - Edge, Safari, Firefox RCE without a sandbox escape (previously: **$30,000**) **$50,000** - Windows or Linux LPE (previously: **$30,000**)
New Entries (**Mobiles**)	None
Increased Payouts (**Mobiles**)	**$200,000** - Chrome RCE + SBX (Android) including a sandbox escape (previously: **$150,000**) **$200,000** - Safari + SBX (iOS) including a sandbox escape (previously: **$150,000**) **$200,000** - Baseband RCE + LPE (iOS or Android) including a privilege escalation (previously: **$150,000**) **$100,000** - Chrome RCE (Android) without a sandbox escape (previously: **$50,000**) **$100,000** - Safari RCE (iOS) without a sandbox escape (previously: **$50,000**)
Deleted Entries	- (Desktop) Adobe Flash RCE (previously: **$80,000**) - (Mobiles) SS7 Protocol Exploits (previously: **$100,000**)

Source: Zerodium

Marketplace for Stolen Data

Source: Dell SecureWorks 2013

Single credit card number: $4-15

Single card with magnetic track data: $12-30

"Fullz": $25-40

- Full name, address, phone, email addresses (with passwords), date of birth, SSN, bank account and routing numbers, online banking credentials, credit cards with magnetic track data and PINs

Online credentials for a bank account with $70-150K balance: under $300

Prices dropped in the last 10 years, indicating supply glut

Marketplace for Victims

Source: Trend Micro, "Russian Underground 2.0", 2015

Pay-per-install on compromised machines

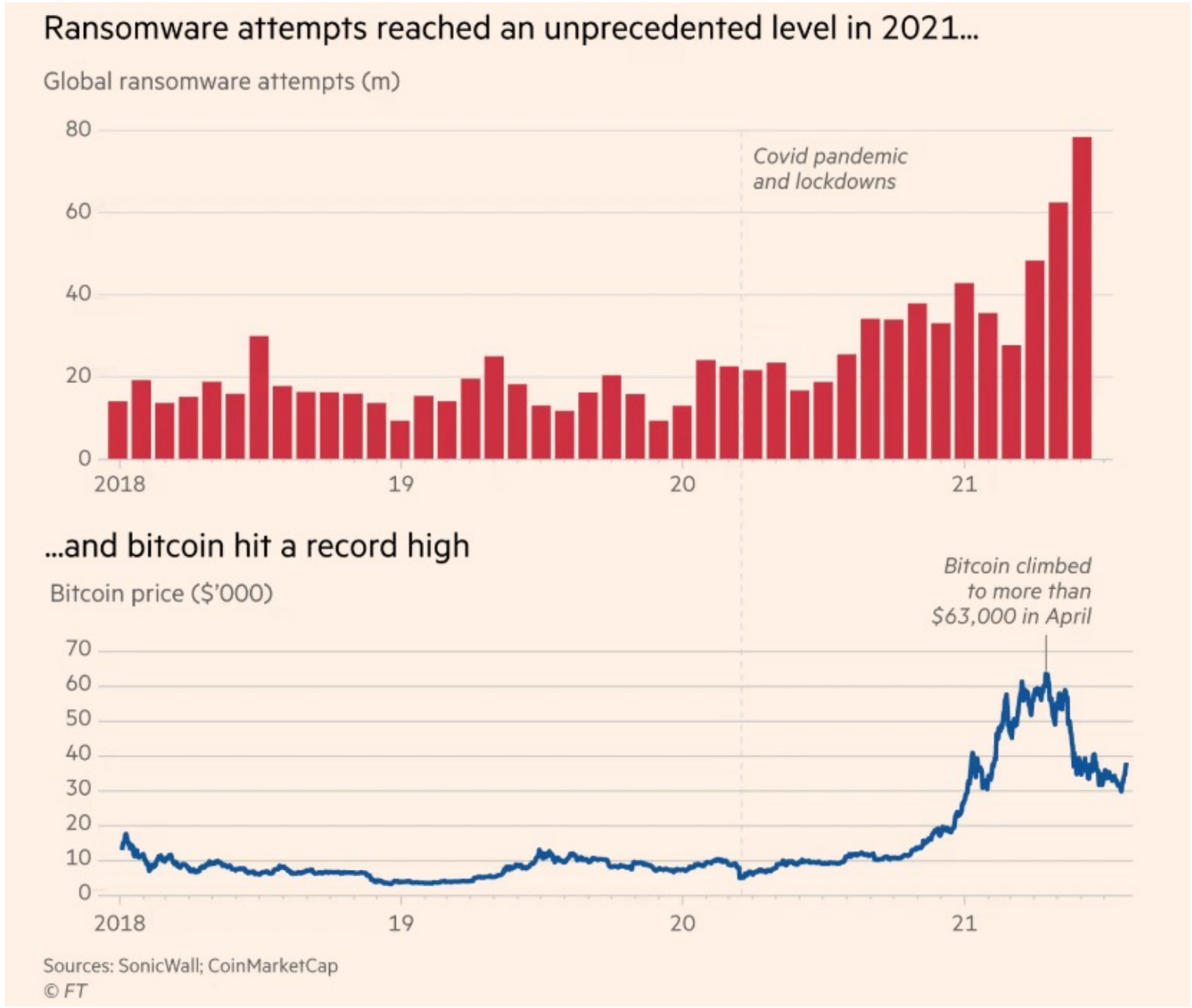
- US: $40-120 / 1000 downloads, "global mix": $10-12
- Can be used to send spam, stage denial of service attacks, perform click fraud, host scam websites

Botnets for rent

- DDoS: up to $100/hour
- Spam: from $1/10,000 emails

Tools and services

- Basic Trojans ($3-10), Windows rootkits ($300), email, SMS, botnet setup and support ($200/month)

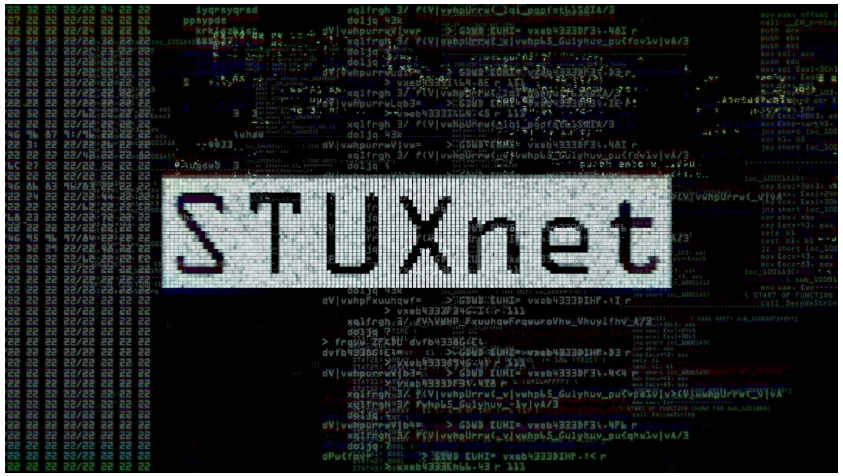


Key enabling technology:

Removed the main obstacle to cybercrime: how to monetize?

Source: Financial Times

Nation-States



Sabotage of Iranian nuclear program

2016 hack of Democratic National Committee

China accused of cyber-attack on Microsoft Exchange servers

North Korean bank heists

A Brief History of WannaCry and NotPetya (2017)

EternalBlue Windows exploit

- Discovered by NSA, stolen and released by ”The Shadow Brokers”

WannaCry cryptoworm/ransomware used exploit to infect over 230,000 machines

- Origin unclear, attributed to North Korea
- Disrupted service at 16 hospitals in the UK, also affected FedEx, Telefonica, Russian Interior Ministry, Honda, …

NotPetya worm released as part of the Russia-Ukraine conflict

- $10 billion in damages (e.g., took Maersk - a major shipping company - offline)
- Cyber insurers refused to cover, claiming it was an act of war

Pegasus: commercialization of intelligence tools

- Pegasus is spyware tool built by NSO, company based in Israel
- Remote compromise of iOS devices
- Sold to law enforcement and government intelligence


Tech > Mobile

Pegasus Spyware and Citizen Surveillance: Here's What You Should Know

NSO Group's software targeted activists, journalists, politicians and executives. Apple's new Lockdown Mode is designed to thwart it.

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

- 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

Administrative details

- https://github.com/tomrist/cs5435-spring2024
- Canvas for homeworks, zoom

- 4 homework assignments (90%)
- Participation (10%)
- Extra credit opportunities along the way

Teaching team

- Instructor: Tom Ristenpart
- TAs:
  - Alaa Daffalla
  - Marina Sanusi

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 / LLM-ing 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

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