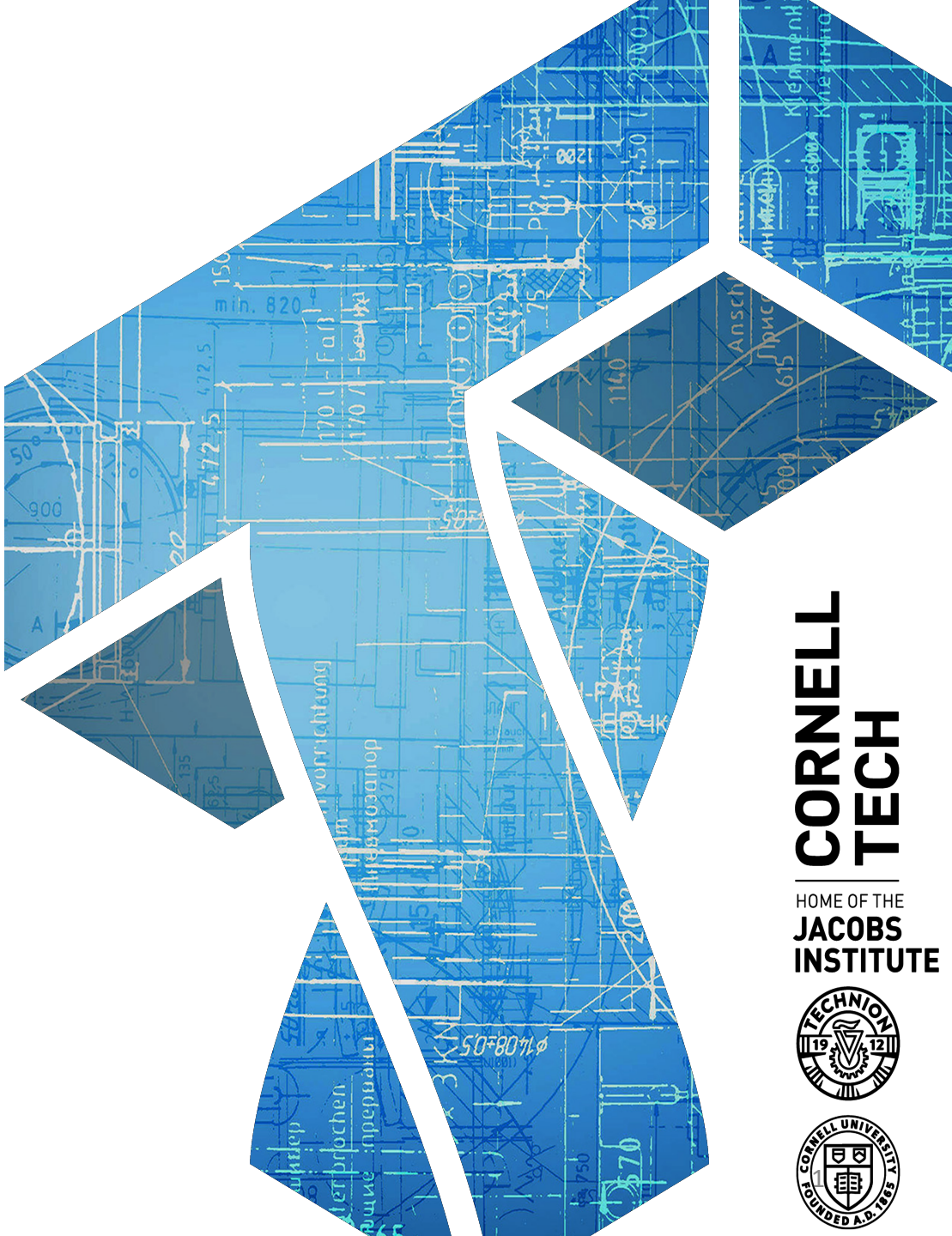
CS 6431
Security & Privacy Technologies



Instructor: Tom Ristenpart

https://github.com/tomrist/cs6431-fall2021

CORNELL TECH

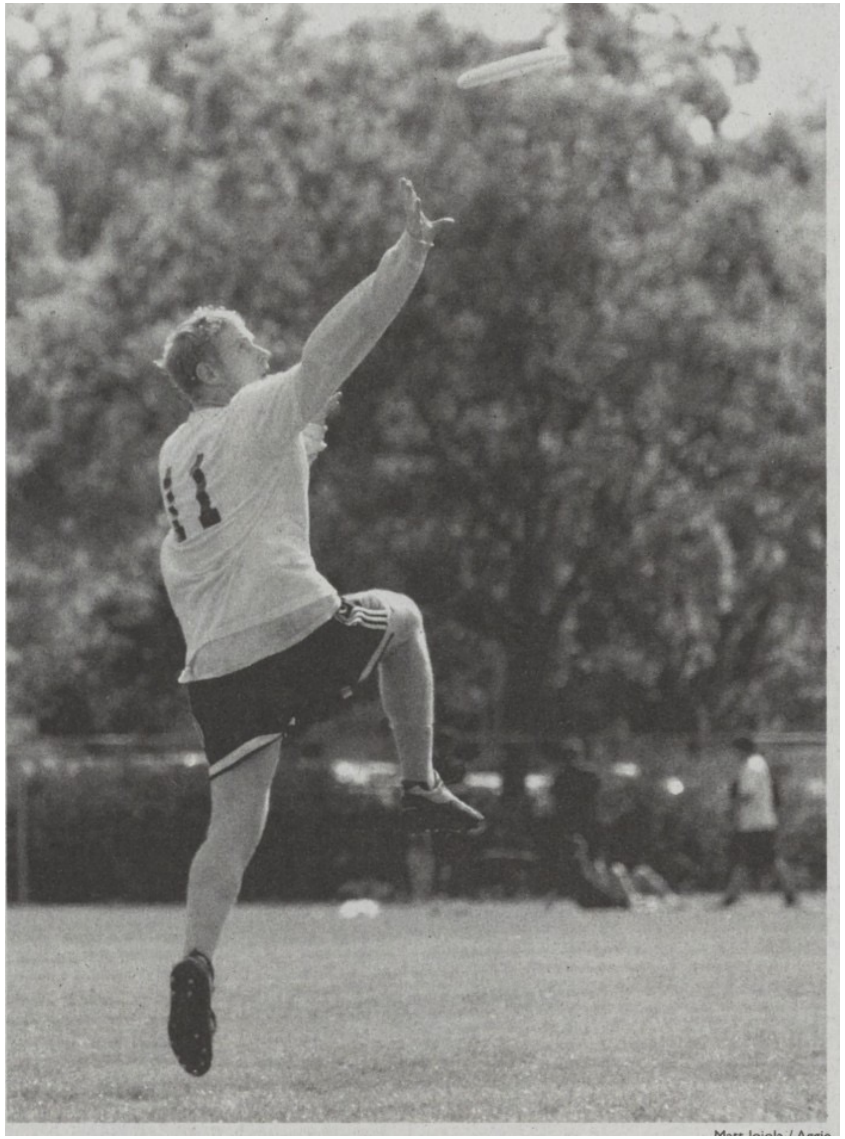
HOME OF THE JACOBS INSTITUTE

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
  - 6+ years as professor at Cornell Tech
  - Some industry experience (most recently: Cloudflare)

- Applied & theoretical cryptography
- Cloud computing security
- Machine learning privacy
- User authentication
- Tech abuse in intimate partner violence

Why did I do a PhD?



Why computer security research?

Security research involves understanding and improving the behavior of computing technologies in the presence of adversaries

- Very broad description
- Every topic in CS has security projection
  - Can jump into large swathe of CS
  - Must balance with need for depth in research
- It is ***really important*** and we are generally kind of ***bad at it***
  - Lots of research problems
  - Real-world impact near at hand
  - But: can sometimes be depressing to live in a world full of villains

How do we approach computer security?

1. Understand what are a system's ***security goals*** (aka, threat modeling)

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

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

4. Understand, design, & 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

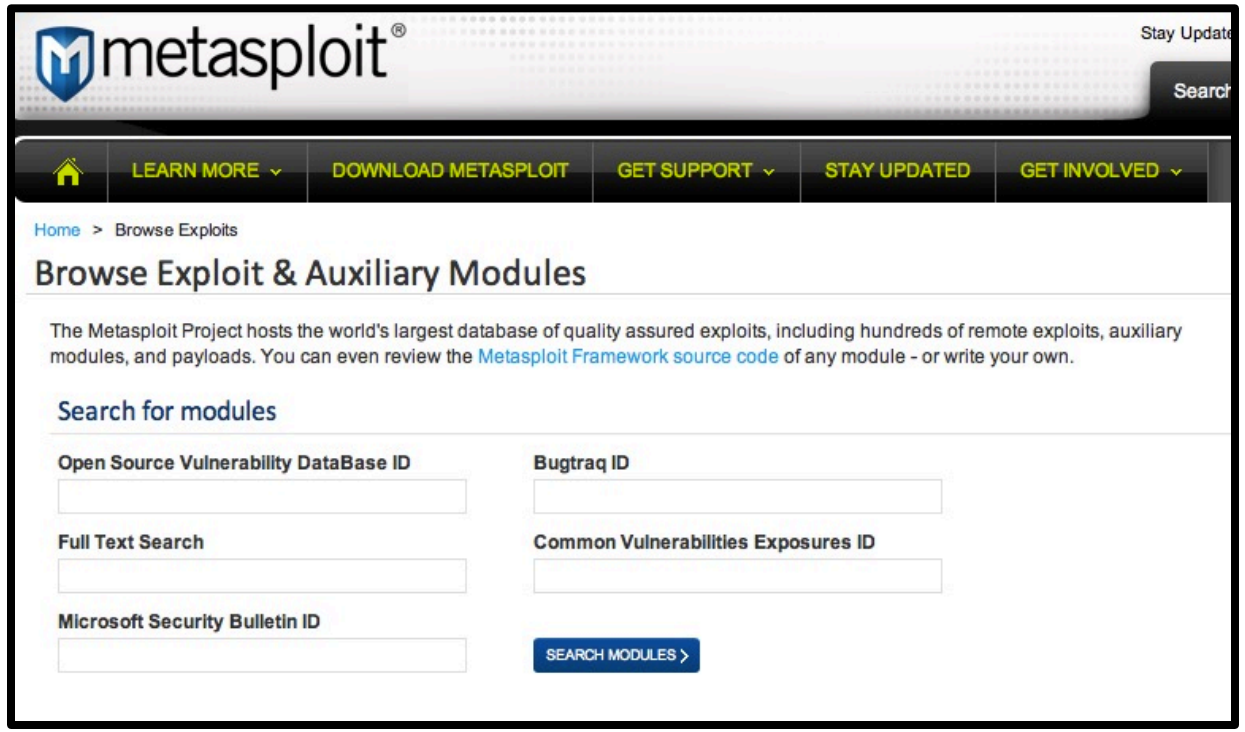
Who/what are the targets?
Who are the adversaries?
What are their goals?
What are their capabilities?

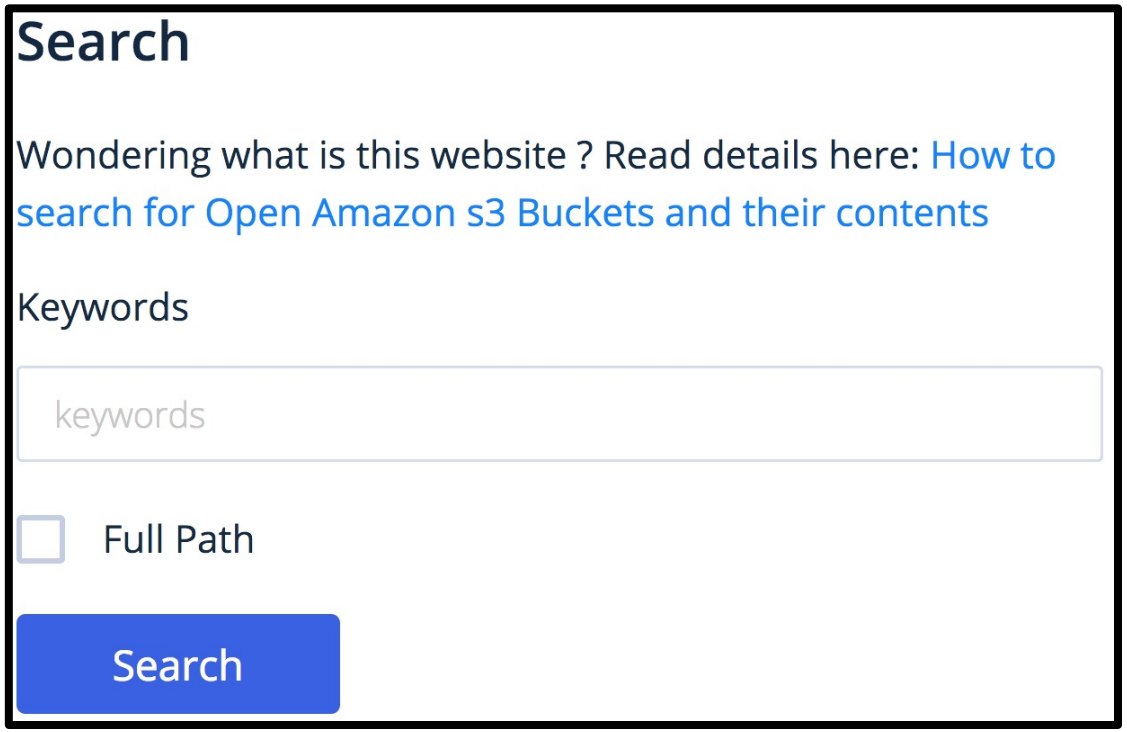
Who are the adversaries?

- “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

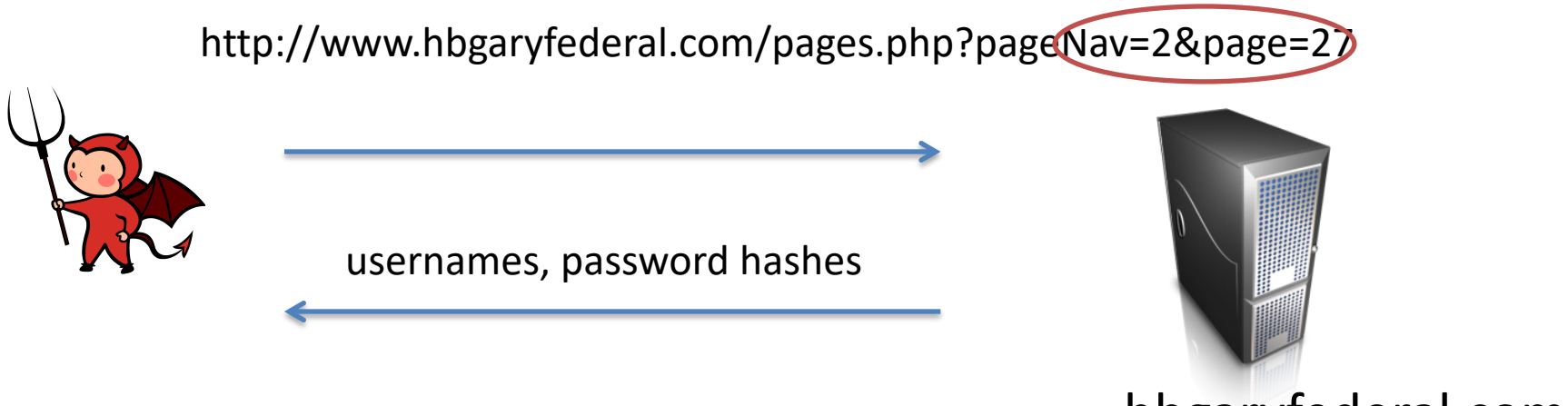
hbgaryfederal.com

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

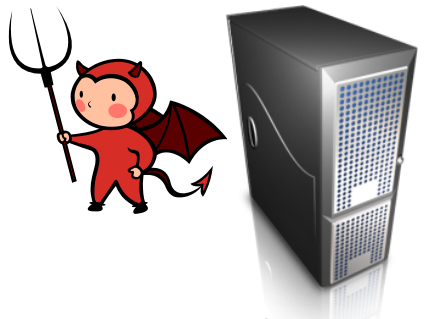
Aaron was administrator for companies' email on Google apps

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

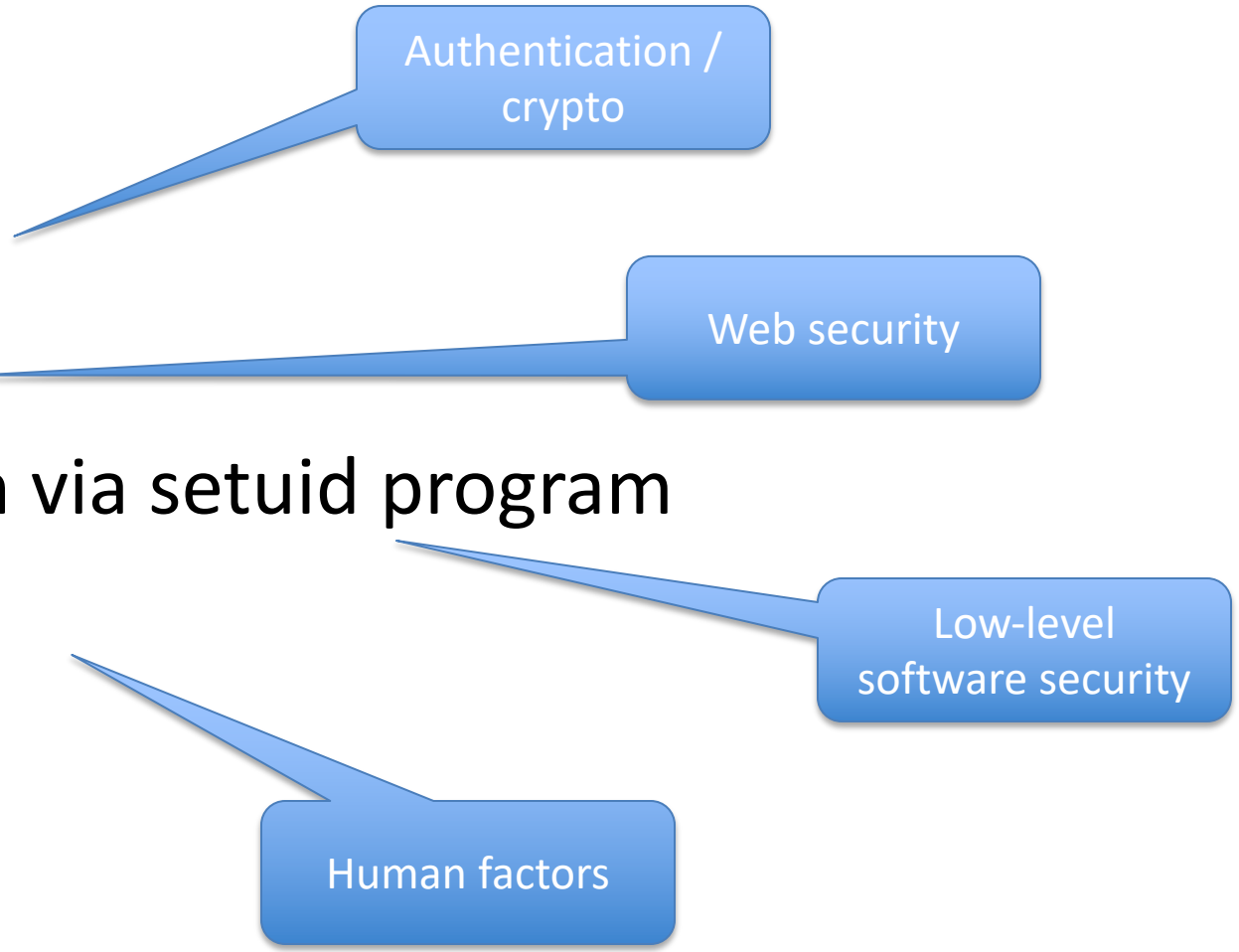
"social engineering"



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

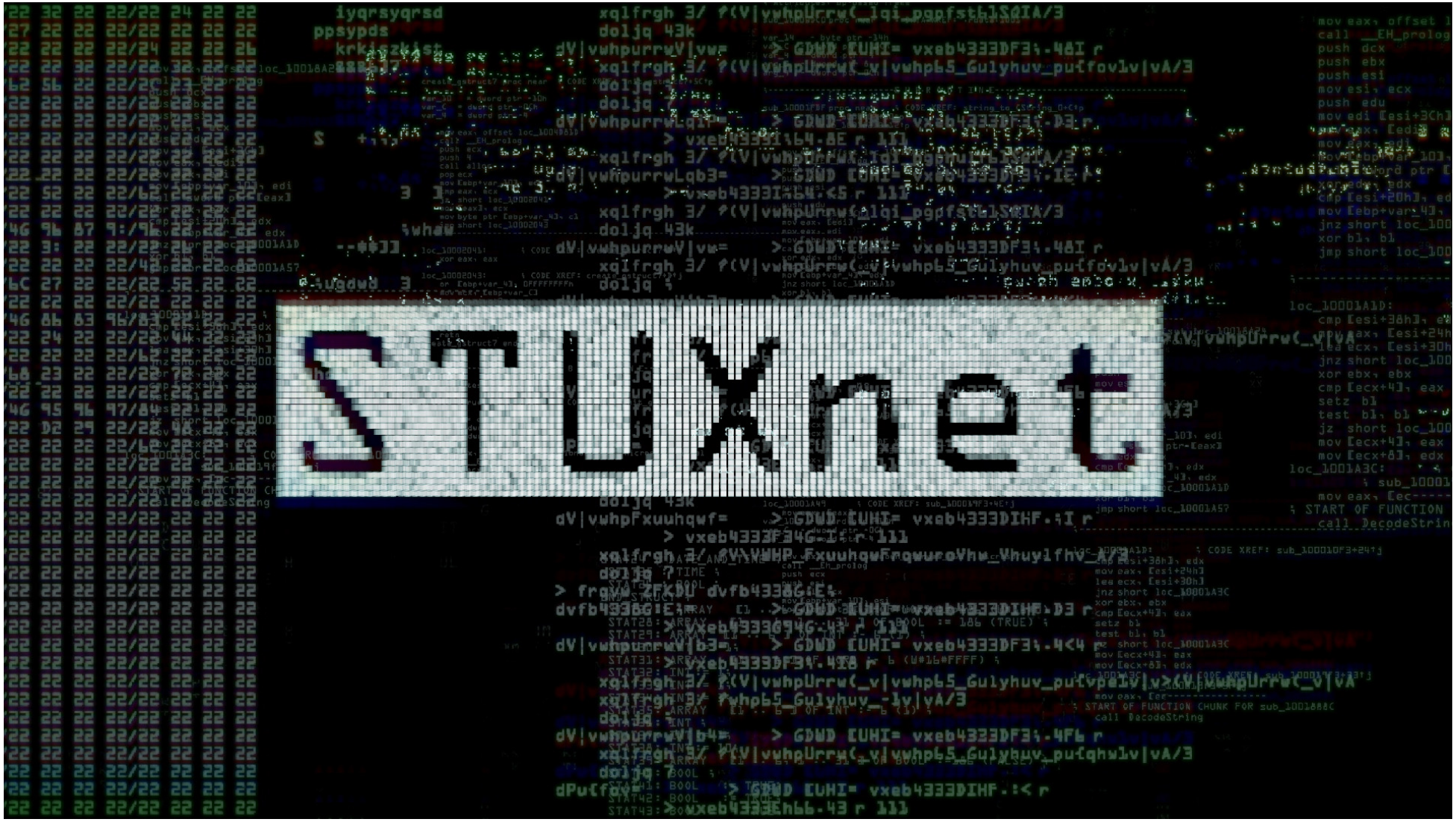
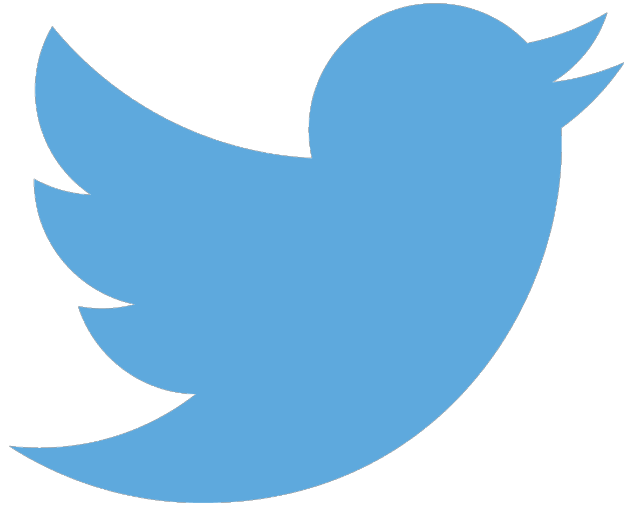


Photo credit: Magnolia Pictures

Computer security & geopolitics

- 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.



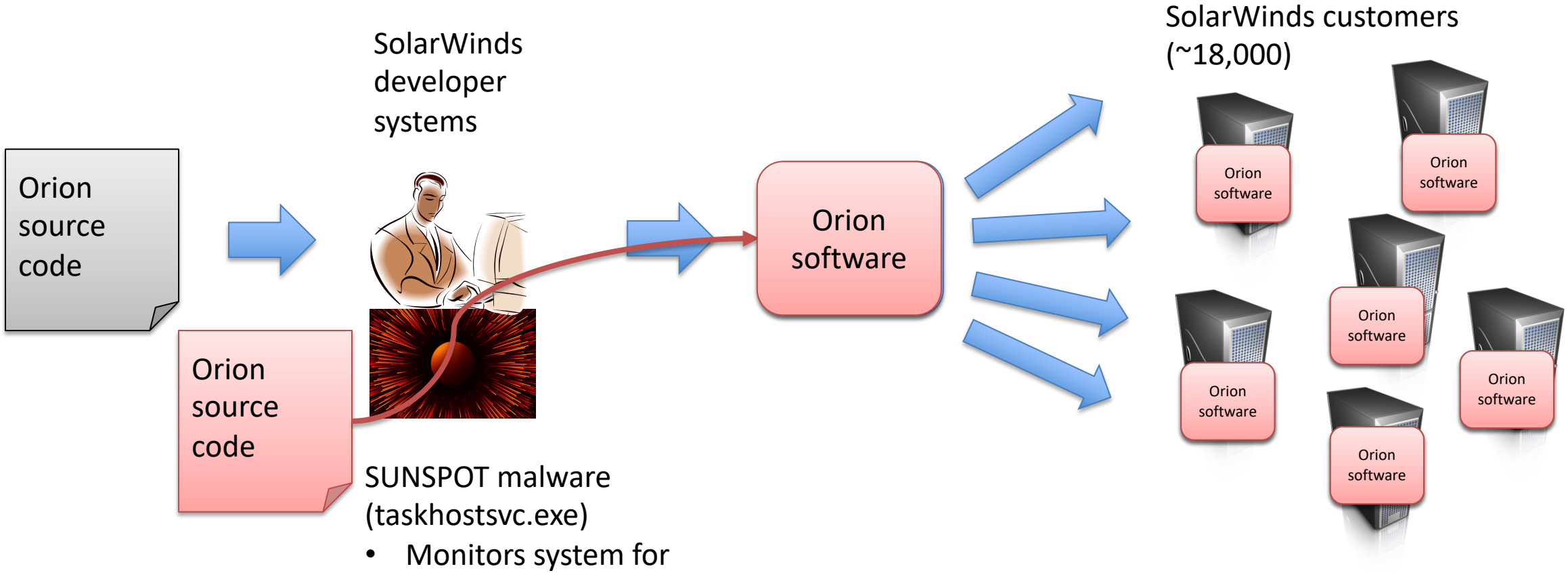
- Hong Kong protests misinformation campaign by accounts emanating from China about

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

Supply chain attacks: SolarWinds (2021)

- Target less-secured upstream suppliers of hardware / software
- SolarWinds hack
  - SolarWinds Orion product is a network monitoring software
  - Most likely Russian APT (SVC or Cozy Bear)
  - Likely one piece of much larger campaign involving other supply chain attacks & targeting US Government & tech companies

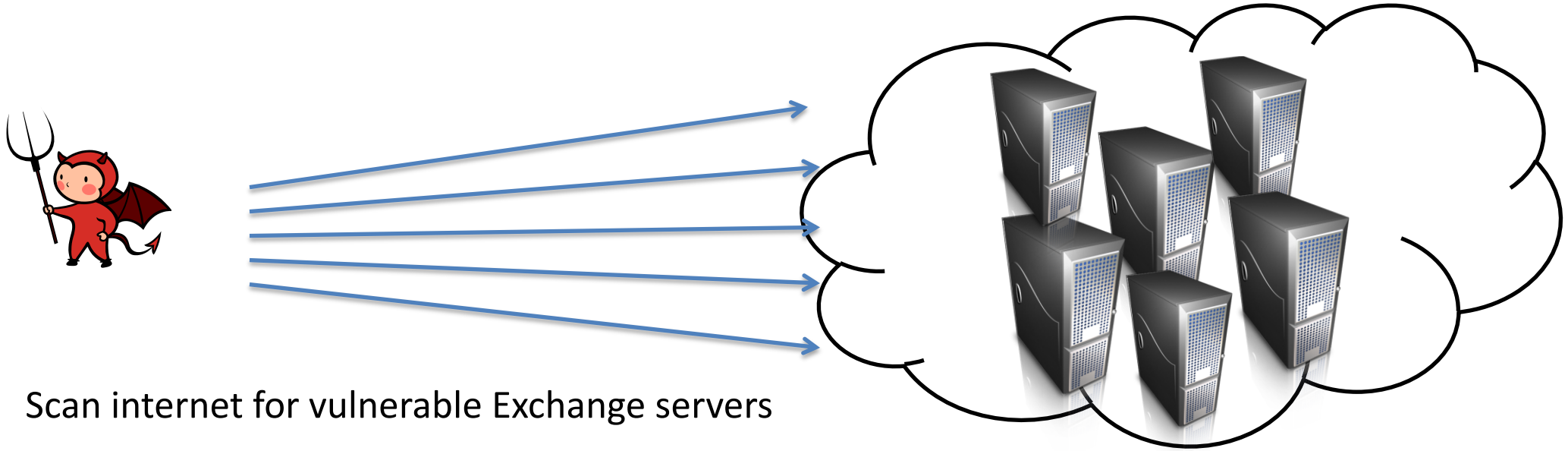
Supply chain attacks: SolarWinds (2021)



Thompson: https://www.cs.cmu.edu/~rdriley/487/papers/Thompson_1984_ReflectionsonTrustingTrust.pdf

Microsoft Exchange vulnerabilities (2021)

4 zero-day vulnerabilities exploited in hacking campaign



1) Scan internet for vulnerable Exchange servers

Microsoft Exchange vulnerabilities (2021)

4 zero-day vulnerabilities exploited in hacking campaign

1) Scan internet for vulnerable Exchange servers
2) Exploit server-side request forgery (SSRF)
   - Tricks web server to make an attacker-controlled authenticated request
   - Allows accessing inboxes for any known email address handled by server
3) Other zero days allow:
   - Remote code execution and writing attacker-controlled files anywhere on server

https://www.volexity.com/blog/2021/03/02/active-exploitation-of-microsoft-exchange-zero-day-vulnerabilities/

Microsoft Exchange vulnerabilities (2021)

- Exploitation first detected by Volexity in January 6, 2021
  - Initial attack campaigns just quietly exfiltrated emails
- Shifted to chaining with remote code execution vulnerabilities:
  - Add webshells for persistent remote access
  - Exfiltrate user credentials (active directory)
  - Add new user accounts
  - Lateral movements to other systems/environments
- Behaviors indicative of Hafnium APT (Chinese espionage group)

From security problems to research

- Need to abstract away from individual security incidents/bugs
  - New classes of vulnerabilities
  - New approaches to defenses
  - New case studies
  - Measurement (including human factors) to improve understanding
- Applied research abstracts from contemporary technology
- Theoretical research driven by research community

Research is community effort

- Learning taste in security problems
- Appreciating style of security papers
  - threat model section, adversarial thinking of readers, etc.
- Understanding landscape of security community
  - IEEE Symposium on Security and Privacy (“Oakland”)
  - USENIX Security
  - ACM Computer and Communications Security (CCS)
  - Network and Distributed System Security (NDSS)
  - Adjacent areas: Crypto/Eurocrypt/Asiacrypt, SOSP/OSDI, Sigcomm, IMC, POPL/PLDI, …

Research is a community effort

- Lone wolf genius trope attractive, but incorrect
  - Even if doing research by yourself, views, taste, incentive structures of research community

- This class will ~~indoctrinate~~ familiarize you with security community, heavily biased by my views/interests

- Highly recommended reading at some point during PhD:
  - Kuhn. Structure of Scientific Revolutions

Consider a simple web service

Client devices
with web browser
or app

Network
(the internet)

Web backend
(Python scripts)

Support utilities
(Shell scripts,
programs)

Virtual machine (VM)

Network or
local

Database
(e.g., SQL)

Research areas relevant to a web service

- Authentication, passwords, authorization
- Abuse / trust & safety
- Web security
- Network security
- Applied cryptography
- Operating systems & mobile security
- Software vulnerabilities (e.g., buffer overflows)
- Database security, virtualization & cloud security
- Privacy
- Ethics

Administrative stuff

- https://github.com/tomrist/cs6431-fall2021
- Canvas instance setup

- Still sorting out details but tentatively:
  - Participation (20%)
  - Problem sets (20%)
  - Project proposal (20%)
  - Project report + presentation (40%)

Main learning goal: conduct security research

- This means being able to produce results of scientific interest
- Project will be geared towards that
  - Target is publishable results, or results that could lead with further work to publishable results
  - Surveys are not really in scope
- We'll do project proposals and help refine projects
- Fine to dovetail with research topic interests or ongoing security research projects

Homework (in addition to readings) for next class:

- Fill out intake survey for class
  - https://forms.gle/gc5vsDx47TiCzJRZA
- Also sent via announcement on Canvas