SECURITY AND PRIVACY CONCEPTS IN THE WILD

VITALY SHMATIKOV

Some 2024 News

National Public Data breach: What you need to know

In early 2024, National Public Data, an online background check and fraud prevention service, experienced a significant data breach. This breach allegedly exposed up to 2.9 billion records with highly sensitive personal data of up to 170M people in the US, UK, and Canada (Bloomberg Law).

2.9 billion records with highly sensitive information on 170M people in the US, UK, and Canada leaked from a data broker that performed background checks (filed for bankruptcy in October)

China Hack Enabled Vast Spying on U.S. Officials, Likely Ensnaring Thousands of Contacts

Hackers scooped up call logs, unencrypted texts and some audio, piercing America's communications infrastructure

Full compromise of nine major telecom providers:
complete metadata for all calls,
complete data DoJ wiretapping operations

AT&T says hackers stole records of nearly all cellular customers' calls and texts

https://support.microsoft.com/en-us/topic/national-public-data-breach-what-you-need-to-know-843686f7-06e2-4e91-8a3f-ae30b7213535
https://www.nbcnews.com/news/us-news/t-says-hackers-stole-records-nearly-cell-customers-calls-texts-rcna161507
https://www.wsj.com/politics/national-security/china-hack-enabled-vast-spying-on-u-s-officials-likely-ensnaring-thousands-of-contacts-1340ba4a

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

Major Data Breaches

List of data breaches involving a government or public entity [edit]

Government	Agency	Year	Records	Organization type	Method	Sources
Shanghai, China	Shanghai National Police Database	2022	1,[illegible]00,000,000, including name, address, birthplace, national ID number, mobile number, all crime/case details	government	unsecured database	[73][74]
India	Indian Council of Medical Research	2023	81[illegible],000,000+, including Aadhaar ID[illegible], passport details, names, phone numbers, addresses	government	hacked by pwn0001	[15]
Unknown	Unknown	2020	20[illegible],000,000	personal and demographic data about residents and their properties of US	Poor security	[57]
?	Unknown agency (believed to be tied to United States Census Bureau)	2020	20[illegible],000,000	financial	accidentally published	[142]
United States	National Archives and Records Administration (U.S. military veterans records)	2009	76[illegible],000,000	military	lost / stolen media	[134]
United States	United States Postal Service	2018	60[illegible],000,000	government	poor security	[124]
Philippines	Commission on Elections	2016	55[illegible],000,000	government	hacked	
Bangladesh	Office of the Registrar General, Birth & Death Registration	2023	50[illegible],000,000+	government	data leak due to security vulnerabilities	[20]

List of data breaches involving companies [edit]

Entity	Year	Records	Organization type	Method	Sources
Yahoo	2013	[illegible],000,000,000	web	hacked	[642][643]
National Public Data	2024	[illegible],900,000,000+ (claimed), including names, email addresses, phone numbers, Social Security numbers, and mailing addresses	data broker	hacked	[473]
Verifications.io (total leaks)	2019	[illegible],000,000,000	online marketing	poor security	[622]
First American Corporation	2019	85,000,000	financial	poor security	[345]
Verifications.io (first leak)	2019	09,000,000	online marketing	poor security	[621]
Collection No. 1	2019	73,000,000	various	compilation of multiple data breaches	[258]
Ticketmaster	2024	60,000,000	ticket distribution	hacked third party service	[581][582]
Facebook	2019	40,000,000	social network	poor security	[335][336]
Marriott International	2018	00,000,000	hotel/casino	hacked	[446]
Yahoo	2014	00,000,000	web	hacked	[644][645][646][647][648]
Friend Finder Networ	2016	12,214,295	web	poor security / hacked	[349][350]
Myspace	2016	60,000,000+, including usernames, passwords email addresses	social network	poor security/account recovery	[469][470][471]
Exactis	2018	40,000,000	data broker	poor security	[322]
Airtel	2019	20,000,000	telecommunications	poor security	[162]
Truecaller	2019	99,055,000	telephone directory	unknown	[595][596]
MongoDB	2019	75,000,000	tech	poor security	[459]
Wattpad	2020	70,000,000	web	hacked	[630]
Facebook	2019	67,000,000	social network	poor security	[338][339]
Microsoft	2019	50,000,000	tech	data exposed by misconfiguration	[454]

What Is Computer Security?

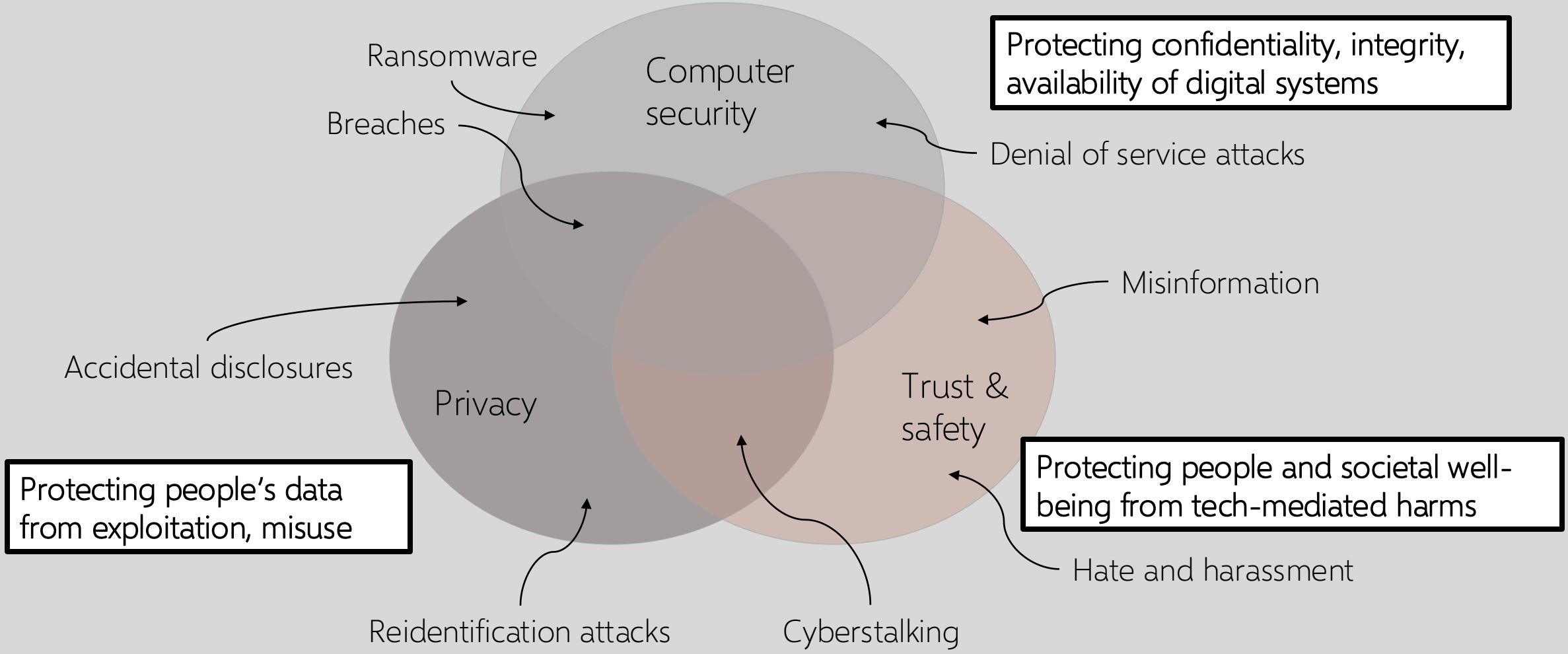
Understanding and improving the behavior of computing technologies in the presence of adversaries

Attackers

Target (victim) computing systems

Defenders: designers, developers, engineers, lawyers, etc.

The World of Computer Security



Course Personnel

Instructor: Vitaly Shmatikov

TAs: Rishi Jha and Collin Zhang

- Office hours: TBD

Course website: **https://cs5435.github.io/**

- Reading materials, lecture notes

Slack for discussions and Q&A -- see Canvas for the link

Canvas for assignments

Prerequisites

Required: working knowledge of C and JavaScript

- Security is a contact sport!
- Homeworks will involve Web security and writing buffer overflow attacks in C

Required: detailed understanding of x86 architecture and memory management (stack layout, calling conventions, etc.)

Recommended:
Operating Systems; Compilers; Computer Networks; Cryptography

- Not much overlap with this course, but will help gain deeper understanding of security mechanisms and where they fit in the big picture

DO NOT TAKE THIS COURSE
IF YOU ARE NOT COMFORTABLE
PROGRAMMING IN C AND JAVASCRIPT

Consider an Alternative!

TECH 5270 studio module in the spring (four 3-hour sessions)

Just the basics

- Dos and don'ts of computer security and privacy
- Human factors in security
- Basics of user authentication
- Basics of network and mobile security
- Cybercrime and ransomware
- Ethical data collection and data privacy
- Security and privacy by design
- Industry perspectives

Not very technical!

Grading

Four programming projects (15% each)

Two take-home exams (15% each)

Attendance and participation (10%)

Cornell University **Code of Academic Integrity** will be strictly enforced

Homeworks / Projects

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

Homeworks need to be done in a virtual environment, will help you setup in Homework 1

Cheating such as plagiarizing homework answers or copying code will trigger disciplinary actions

Late Submission Policy

Each assignment is due at 11:59p ET on the due date

You have 3 late days to use any way you want

- You can submit one assignment 3 days late, 3 assignments 1 day late, etc.
- After you use up your days, you get 0 points for each late assignment
- Partial days are rounded up to the next full day

Course Materials

No textbook

Occasional readings (see course website)

Lectures will cover some material that is not in the notes or readings – and you will be tested on it!

Learning Objectives

Understand the system's security goals

Learn to spot security vulnerabilities

Think through how attacks would play out

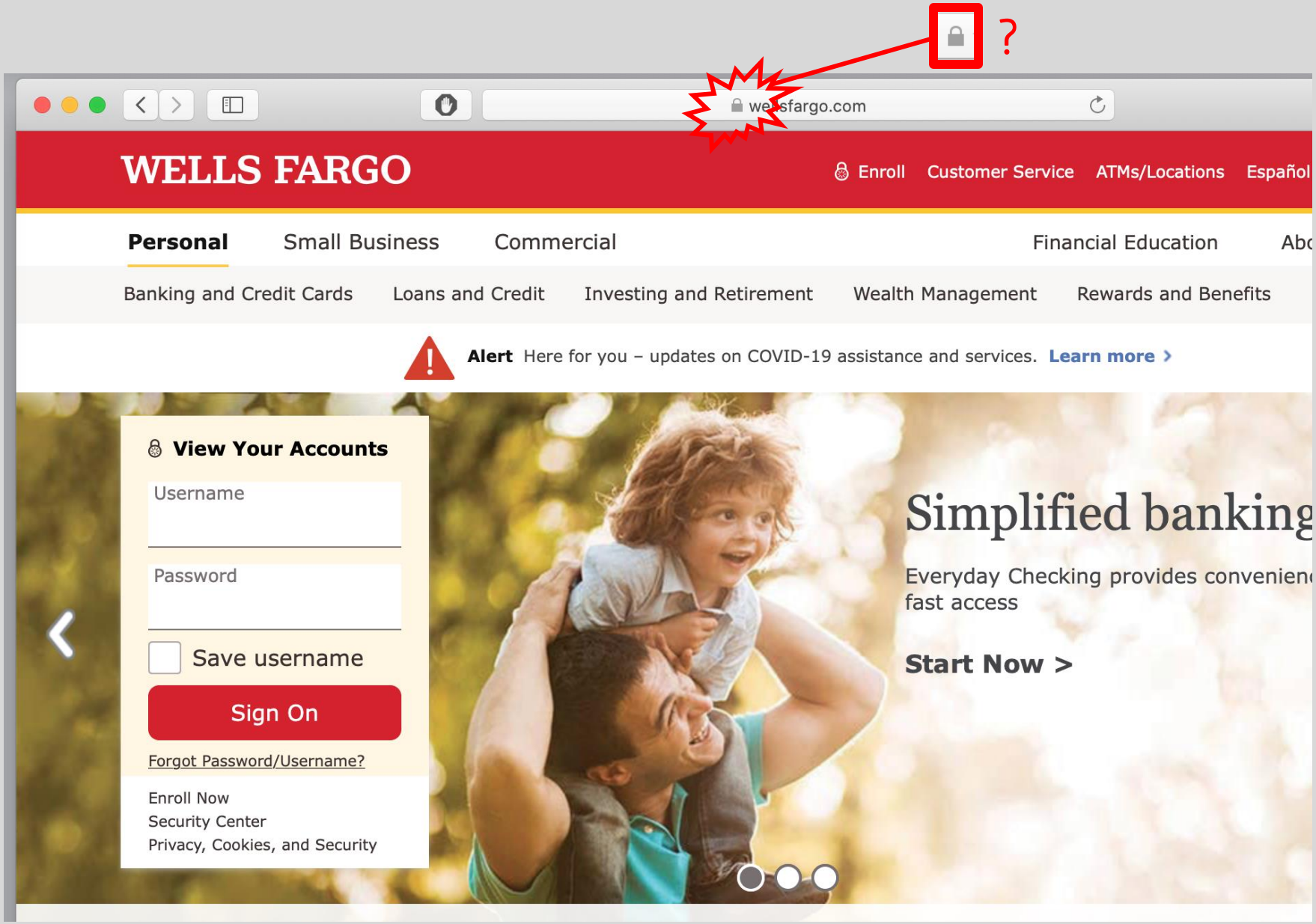
Understand and deploy countermeasures

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?


?
wellsfargo.com
WELLS FARGO
Enroll
Customer Service
ATMs/Locations
Español
Personal
Small Business
Commercial
Financial Education
Banking and Credit Cards
Loans and Credit
Investing and Retirement
Wealth Management
Rewards and Benefits
Alert Here for you – updates on COVID-19 assistance and services. Learn more
View Your Accounts
Username
Password
Save username
Sign On
Forgot Password/Username?
Enroll Now
Security Center
Privacy, Cookies, and Security
Simplified banking
Everyday Checking provides convenien
fast access
Start Now >

U.S. Privacy Policies and Notices

- Wells Fargo U.S. Consumer Privacy Notice
- California Consumer Privacy Act Notice
- Digital Privacy and Cookies Policy
- Wells Fargo Retail Services Privacy Notice (PDF)
- Wells Fargo Bank, N.A. Dillard's Privacy Notice (PDF)
- Health Information Notice
- Social Security Number Protection Policy

Legal Terms

- ESIGN Consent
- General Terms of Use
- Online Access Agreement

International Privacy Notice

+ **special sets of notices** for Australia, Canada, EU, New Zealand, South Korea

International Non-Employee Privacy Notices

+ **special notices** for Canada, EU, South Korea

Global Data Access

What Do You Think Should Be Included in "Privacy and Security" for an E-commerce website?

Desirable Properties

- Authenticity
- Confidentiality
- Integrity
- Availability
- Accountability and non-repudiation
- Access control
- Privacy of collected information
- ...

Correctness vs. Security

Modular design may increase vulnerability!
Abstraction is difficult to achieve in security: what if the adversary operates below your level of abstraction?
... but also increase security (small TCB)

Correctness

System satisfies specification

For reasonable input, get reasonable output

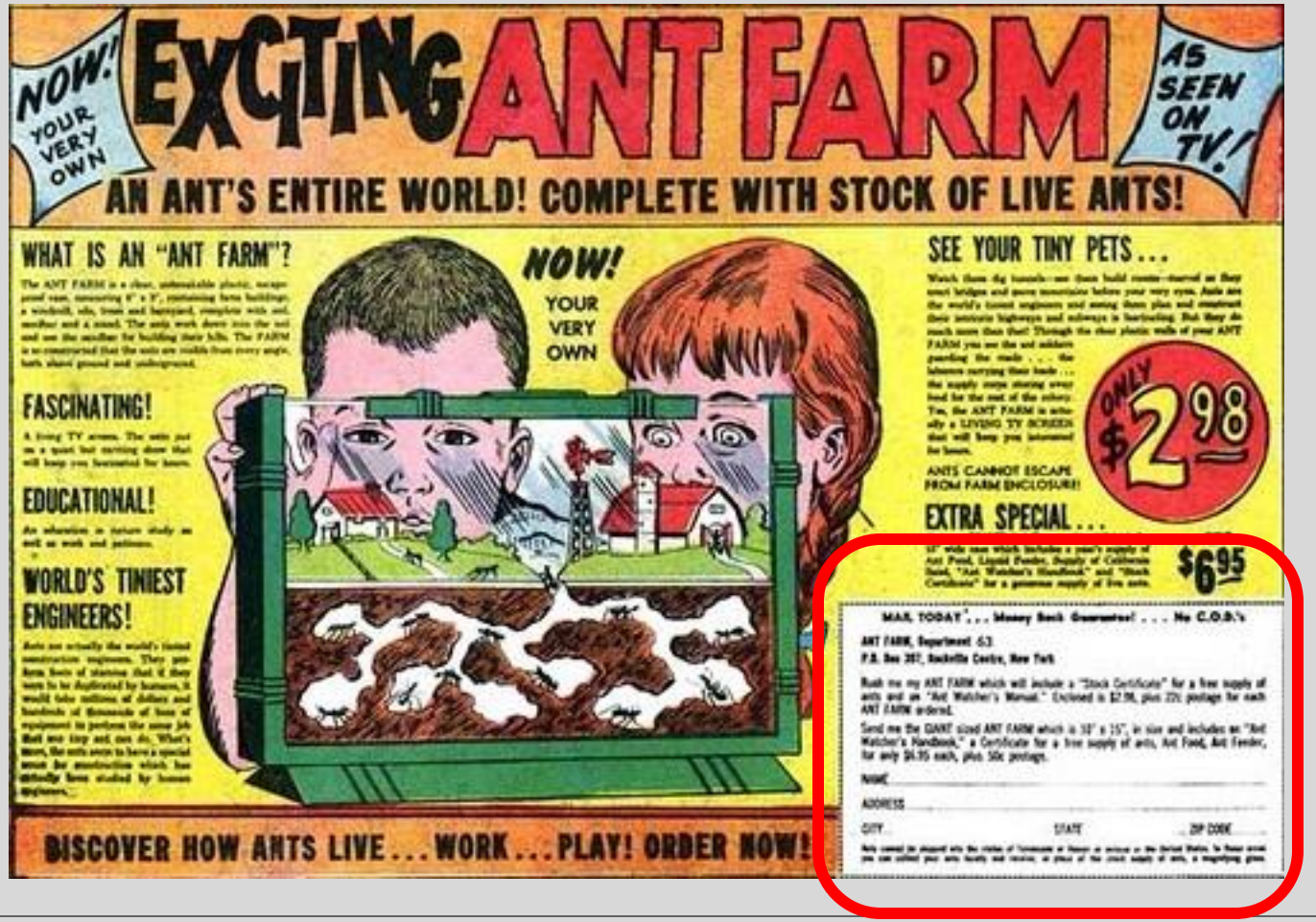
Security

System properties preserved in face of attack

For unreasonable input, output not completely disastrous

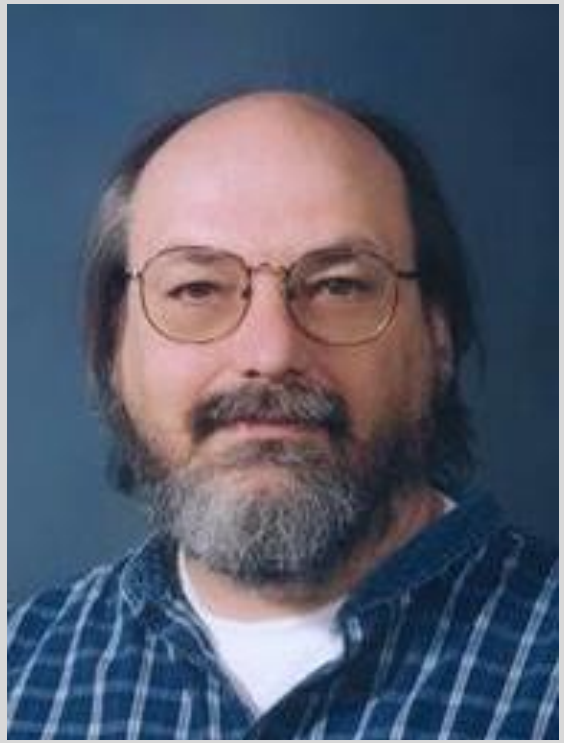
Main difference:
active interference from an adversary

A Security Engineer's Mindset



Credit:
Bruce Schneier

Ken Thompson



ACM Turing Award, 1983

Reflections on Trusting Trust

What code can we trust?

Consider "login" or "su" in Unix

- Is Ubuntu binary reliable? RedHat?
- Does it send your password to someone?
- Does it have backdoor for a “special” remote user?

Can't trust the binary, so check source code or write your own, recompile

Does this solve problem?

http://www.acm.org/classics/sep95

Reflections on Trusting Trust

Who wrote the compiler?

Compiler looks for source code that looks the login process, inserts backdoor into it

Ok, inspect the source code of the compiler… Looks good? Recompile the compiler!

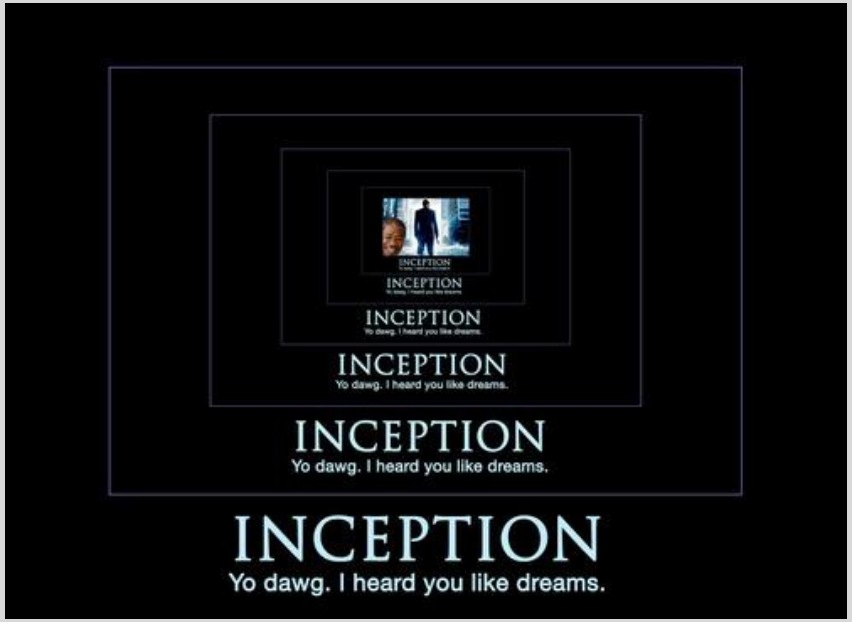
Does this solve the problem?

http://www.acm.org/classics/sep95

Reflections on Trusting Trust

The compiler is written in C …

```
compiler(S) {
    if (match(S, "login-pattern")) {
        compile (login-backdoor)
        return }
    if (match(S, "compiler-pattern")) {
        compile (compiler-backdoor)
        return }
    .... /* compile as usual */ }
```



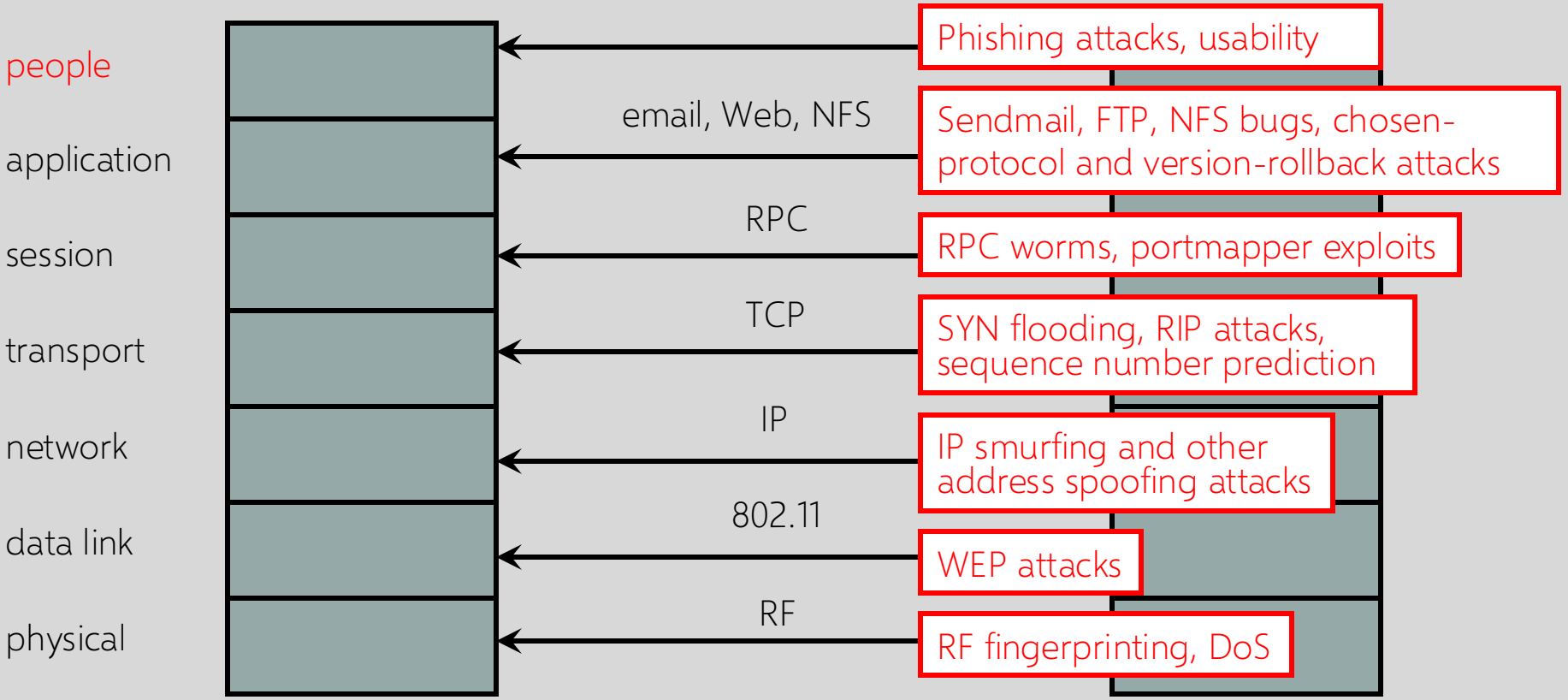
http://www.acm.org/classics/sep95

Reflections on Trusting Trust

"The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)"

http://www.acm.org/classics/sep95

Network Stack

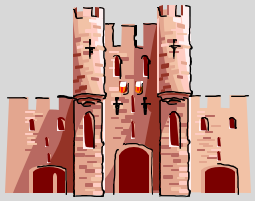


Only as secure as the single weakest layer… or interconnection between the layers

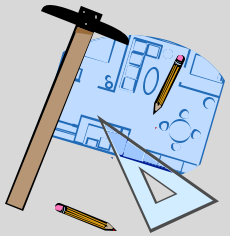
Network Defenses

All defense mechanisms must work correctly and securely

People



Systems



Blueprints

Building blocks

End uses — Password managers, company policies…

Implementations — Firewalls, intrusion detection…

Protocols and policies — TLS, VPN, access control…

Cryptographic primitives — RSA, DSS, SHA…

Bad News

- Security often not a primary consideration
  - Performance and usability take precedence
- Feature-rich systems may be poorly understood
- Implementations are buggy
  - Buffer overflows are the “vulnerability of the decade”
  - Cross-site scripting and other Web attacks
  - Emerging classes of attacks: SSRF, others
- Networks are more open and accessible than ever
  - Increased exposure, easier to cover tracks
- Many attacks are not even technical in nature
  - Phishing, social engineering, etc.

Better News

There are a lot of defense mechanisms

It's important to understand their limitations

- "If you think cryptography will solve your problem, then you don't understand cryptography… and you don't understand your problem"
- Many security holes are based on a misunderstanding

Security awareness and user "buy-in" help

Other important factors: usability and economics

Main Themes of the Course

Vulnerabilities of modern systems and networks

- Phishing, credential theft, denial of service, attacks on Web applications, attacks on system software, attacks on infrastructure

Defensive technologies

- Authentication
- Web and mobile security
- Basic cryptography, application- and transport-layer security protocols
- Protection of software: memory integrity, code analysis, intrusion detection

Running Example: 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

Securing a Web Service

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

What This Course Is Not About

Not a comprehensive course on computer security

Not a course on ethical, legal, or economic issues

- No file sharing, DMCA, piracy, free speech issues
- Little about surveillance

Only a cursory overview of cryptography

Only some issues in systems security

- Very little about OS access control, secure hardware, security of embedded devices, physical security…

Consider an Alternative!

TECH 5270 studio module in the spring (four 3-hour sessions)

Just the basics

- Dos and don'ts of computer security and privacy
- Human factors in security
- Basics of user authentication
- Basics of network and mobile security
- Cybercrime and ransomware
- Ethical data collection and data privacy
- Security and privacy by design
- Industry perspectives

Not very technical!

Peek at the Dark Side

The only reason we will be learning about attack techniques is to build better defenses

Do not even think about using this knowledge to attack anyone

CULT OF THE DEAD COW®
PARAMEDIA • est. 1984 v.666

BlackHat®
USA • EUROPE • ASIA
Training

Rules of Thumb

When in doubt … don’t

- Find someone to talk to (instructor or TA)

You must have explicit written permission from the system owner before performing any penetration testing

- Homework assignments will generally be in an isolated virtual environment
- We will give explicit permission to hand us exploits 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

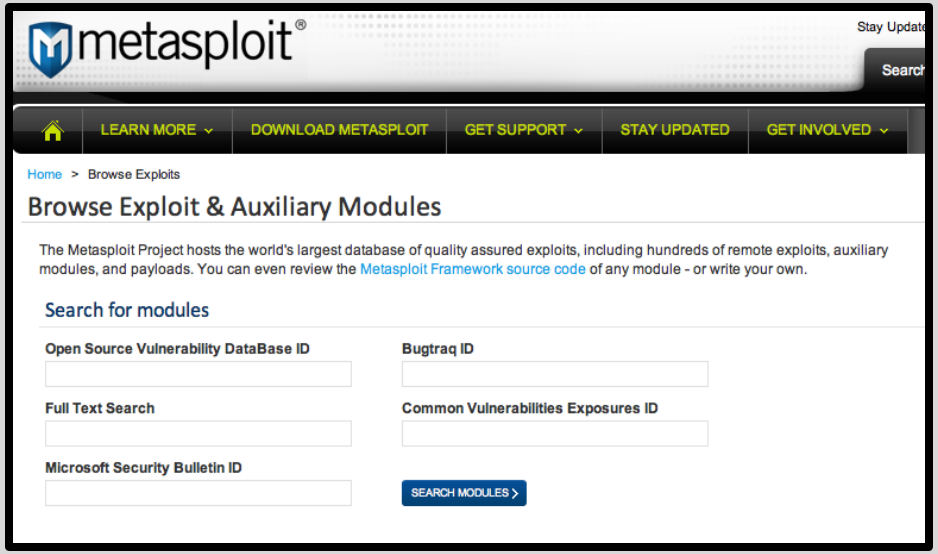
Who Are the Adversaries?

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

Hacking Commoditized

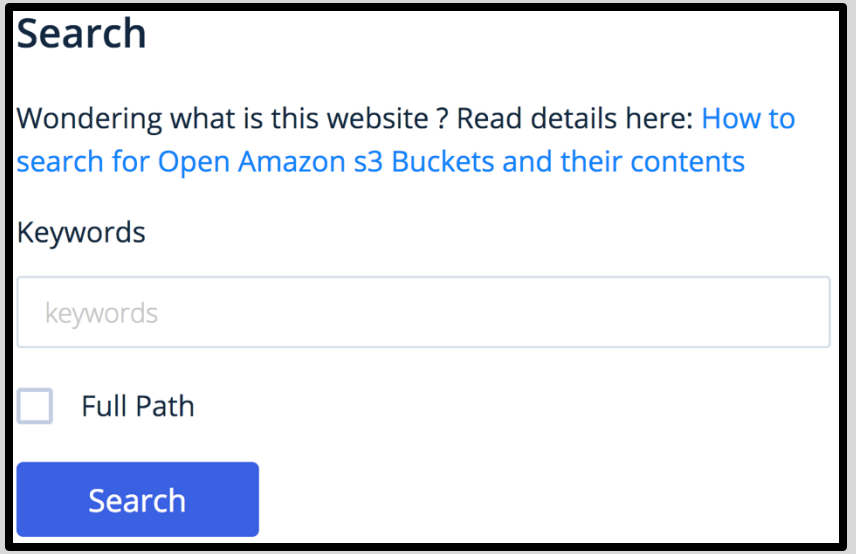
Metasploit

- All-in-one penetration testing tool
- Easy-to-use exploit libraries



Public Amazon credentials for AWS, S3 buckets, …

- Source of many recent breaches



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

About S3: The Story of a Hack

Did not protect essential credentials

- 2014: Uber's source code on GitHub accessed using stolen credentials
- In the source code, keys to all Uber's S3 databases
- 2016: Uber's driver database stolen using same credentials

Cloud keys hardcoded in source code

rotate your keys!

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."

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

How Not to Handle a Data Breach

- 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 Joe Sullivan, Uber’s former Chief Security Officer
- 2022: Sullivan convicted of obstruction of justice and misprision (failure to report knowledge of a felony)

First federal prosecution of a corporate executive for the handling of a data breach

Review of the Summer 2023 Microsoft Exchange Online Intrusion

Compromise of the email accounts of senior US government representatives working on national security matters using a compromised Microsoft signing key (enabling creation of forged authentication tokens)

Top companies ground Microsoft Copilot over data governance concerns

"... bigger companies that have complex permissions around their SharePoint or their Office 365 or things like that, where the Copilots are basically aggressively summarizing information that maybe people technically have access to but shouldn't have access to"

https://www.cisa.gov/sites/default/files/2024-04/CSRB_Review_of_the_Summer_2023_MEO_Intrusion_Final_508c.pdf
https://www.theregister.com/2024/08/21/microsoft_ai_copilots/

Abusers

- "Cyberbullying"
- Online stalkers, remote access trojan (RATs)
- Intimate partner violence (IPV)
  - Widespread: 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…

“Hacktivists”

Anonymous vs HBGary (2011)

hbgaryfederal.com

Gmail

rootkit.com

Ran by Greg Hoglund,
owner of HBGary / HBGary Federal

Anonymous vs HBGary

http://www.hbgaryfederal.com/pages.php?pageNav=2&page=27

usernames, password hashes

hbgaryfederal.com

SQL injection attack

h = hash(pw)

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

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

Ted Vera (COO) and Aaron Barr (CEO) of HBGary had passwords with 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

"social engineering"

```
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
```

rootkit.com

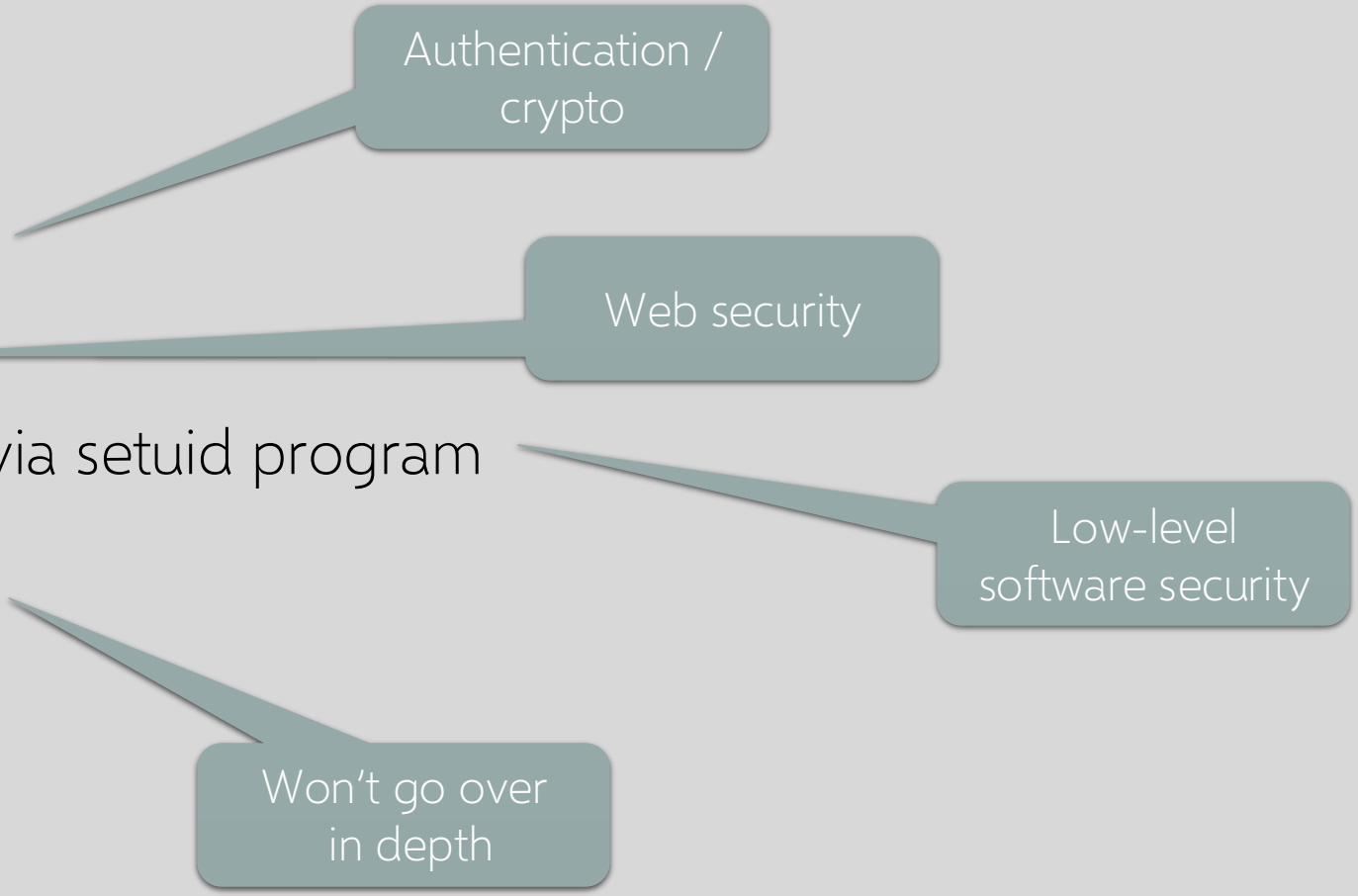
Recap

Password cracking

SQL injection

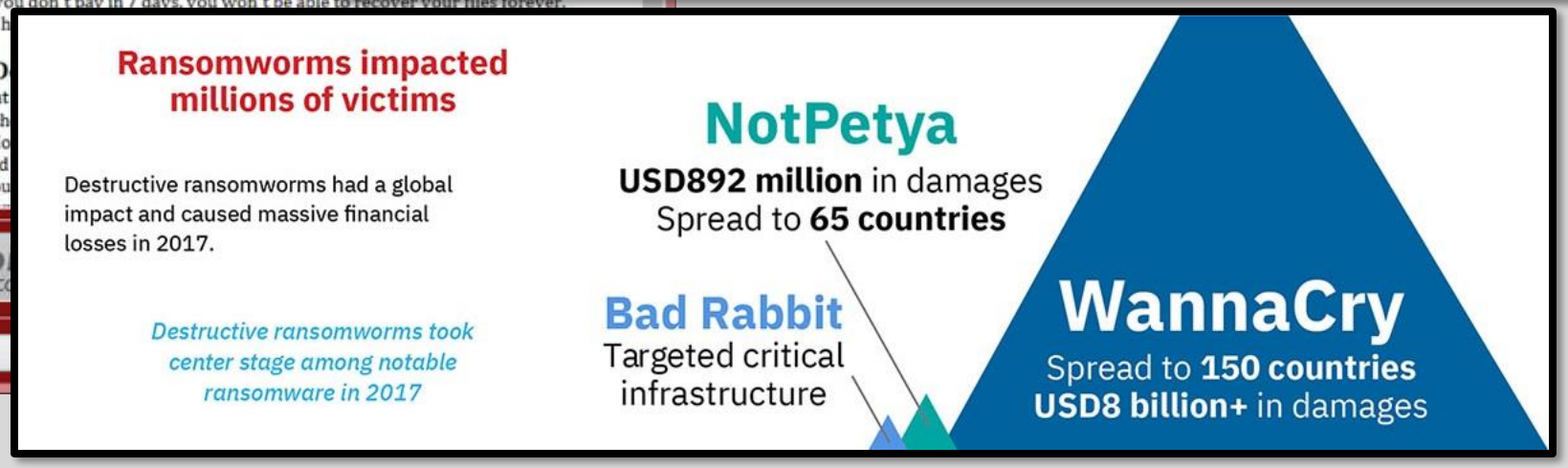
Privilege escalation via setuid program

Social engineering



Economically Motivated Criminals

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



Marketplace for Vulnerabilities

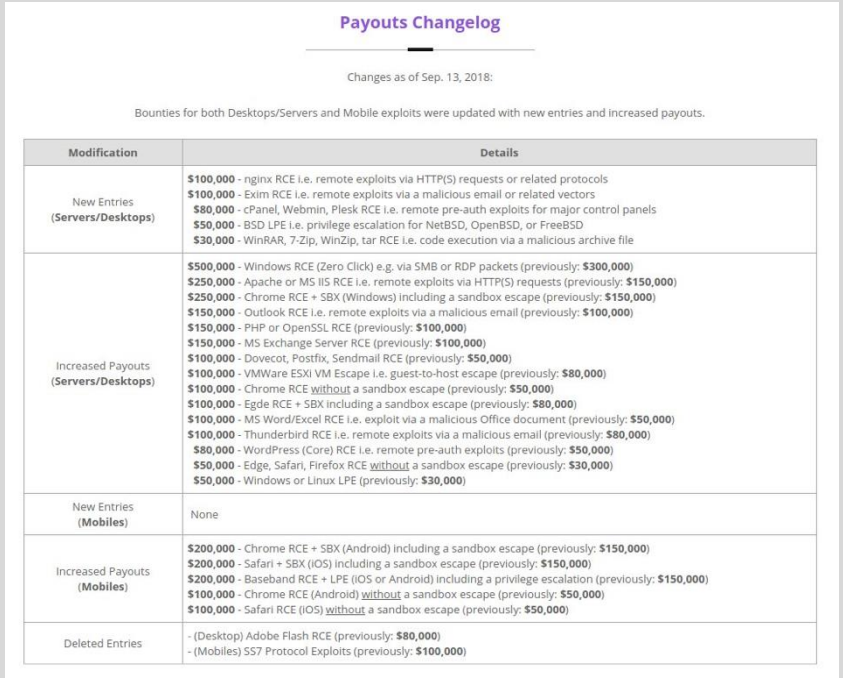
Bug bounty programs

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

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

Source: Dell SecureWorks 2013

Marketplace for Stolen Data

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

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

Marketplace for Victims

Pay-per-install on compromised machines

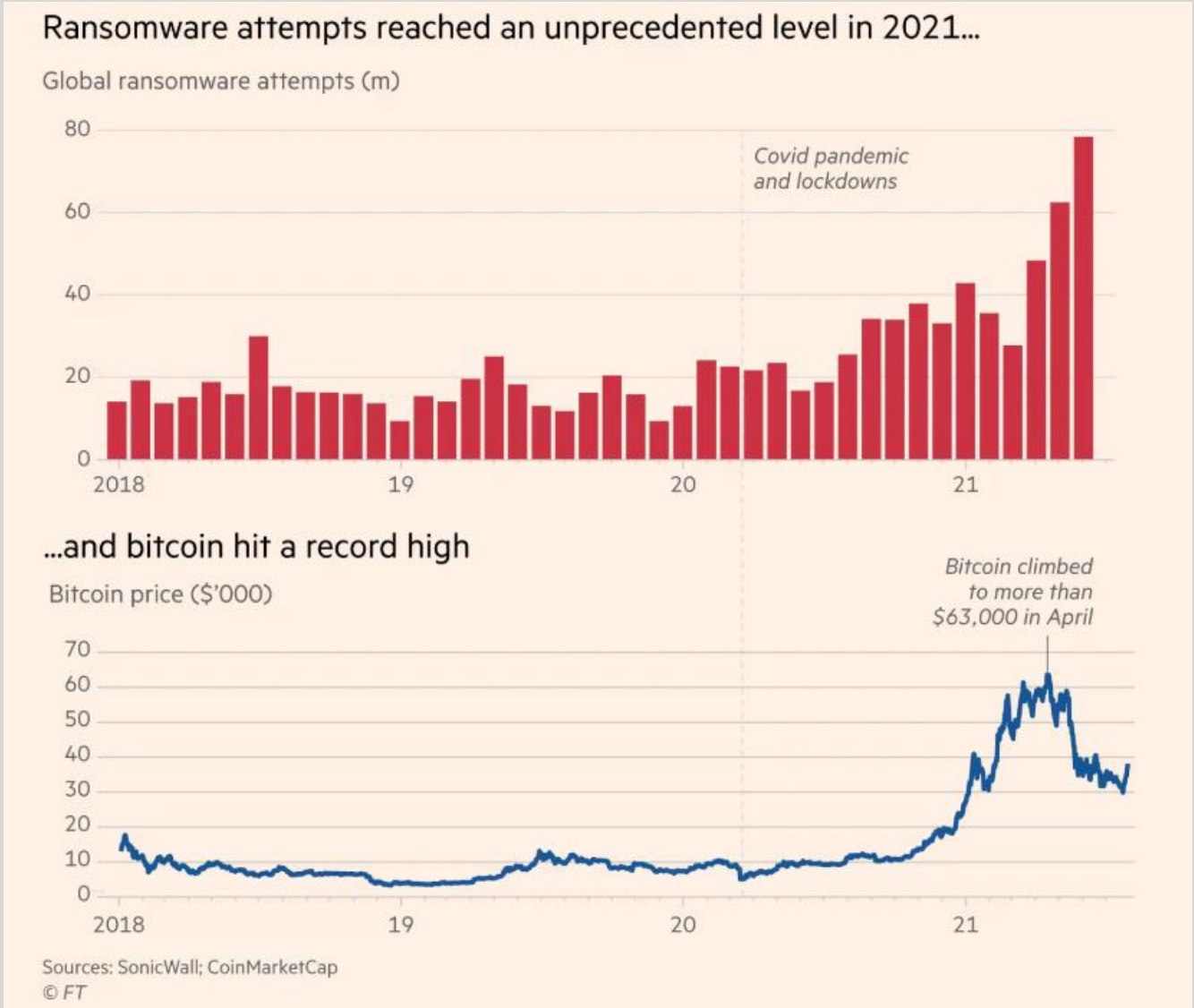
- US: $40-120 / 1000 downloads, "global mix": $10-12
- Can be used to send spam, stage denial of service attacks, perform click fraud, host scam websites

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)

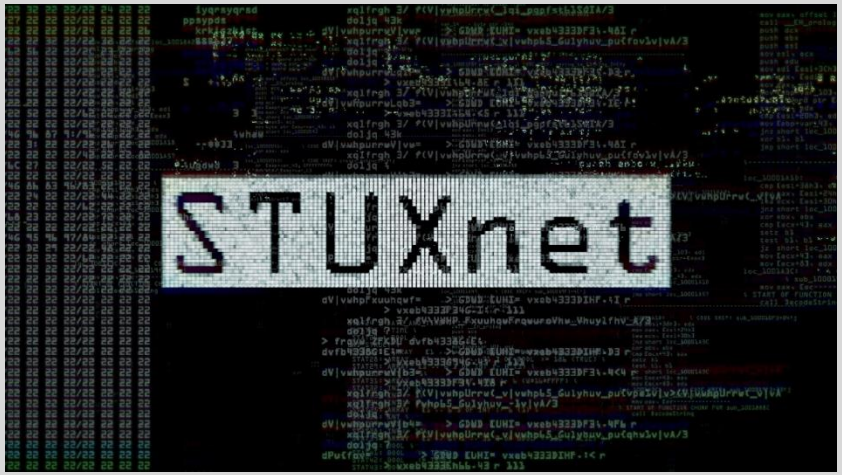


Key enabling technology:

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, a 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.

Stephen Shankland

July 19, 2022 8:49 a.m. PT

9 min read

Security Principles

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

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

See readings on the course website to self-test

DO NOT TAKE THIS COURSE
IF YOU ARE NOT COMFORTABLE
PROGRAMMING IN C AND JAVASCRIPT

Consider an Alternative!

TECH 5270 studio module in the spring (four 3-hour sessions)

Just the basics

- Dos and don'ts of computer security and privacy
- Human factors in security
- Basics of user authentication
- Basics of network and mobile security
- Cybercrime and ransomware
- Ethical data collection and data privacy
- Security and privacy by design
- Industry perspectives

Not very technical!