



SECURITY AND PRIVACY CONCEPTS IN THE WILD

VITALY SHMATIKOV

So Far in 2021



Facebook CEO Mark Zuckerberg. AP Photo/Andrew Harnik

- The personal data of over 500 million Facebook users was posted in a low-level hacking forum.
- It includes phone numbers, full names, locations, email addresses, and biographical information.

At Least 30,000 U.S. Organizations Newly Hacked Via Holes in Microsoft's Email Software

Credits: ZDNet, Krebs on Security, Insider

T-Mobile Investigating Claims of Massive Customer Data Breach

Hackers selling the data are claiming it affects 100 million users.

August 15, 2021

The data includes social security numbers, phone numbers, names, physical addresses, unique IMEI numbers, and driver licenses information, the seller said.

...

On the underground forum the seller is asking for 6 bitcoin, around \$270,000, for a subset of the data containing 30 million social security numbers and driver licenses. The seller said they are privately selling the rest of the data at the moment.

<https://www.vice.com/en/article/akg8wg/tmobile-investigating-customer-data-breach-100-million>

Major Data Breaches

| Entity | ◆ Year ◆ | Records ▼ | Organization type | Method | Sources |
|--|----------|---------------|--|----------------------------------|---|
| Yahoo | 2013 | 3,000,000,000 | web | hacked | [377] [378] |
| First American Corporation | 2019 | 865,000,000 | financial service company | poor security | [148] |
| Facebook | 2019 | 500,000,000 | social network | poor security | [141] [142] |
| Marriott International | 2018 | 500,000,000 | hotel | hacked | [223] |
| Yahoo | 2014 | 500,000,000 | web | hacked | [379] [380] [381] [382] [383] |
| Friend Finder Networks | 2016 | 42,214,295 | web | poor security / hacked | [152] [153] |
| Exactis | 2018 | 30,000,000 | data broker | poor security | [129] |
| Airtel | 2019 | 30,000,000 | telecommunications | poor security | [18] |
| Truecaller | 2019 | 29,055,000 | Telephone directory | unknown | [325] [326] |
| MongoDB | 2019 | 25,000,000 | tech | poor security | [236] |
| Wattpad | 2020 | 20,000,000 | web | hacked | [367] |
| Facebook | 2019 | 20,700,000 | social network | poor security | [144] [145] |
| Microsoft | 2019 | 20,000,000 | tech | data exposed by misconfiguration | [229] |
| MongoDB | 2019 | 20,000,000 | tech | poor security | [235] |
| Unknown | 2020 | 20,100,000 | personal and demographic data about residents and their properties of US | Poor security | [157] |
| Instagram | 2020 | 20,000,000 | social network | poor security | [194] |
| Unknown agency (believed to be tied to United States Census Bureau) | 2020 | 20,000,000 | financial | accidentally published | [392] |

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.

Course Personnel

- Instructor: Vitaly Shmatikov
- TAs: Jialing Pei (full) and Deepak Maram (half)
 - Office hours TBA
- Course website: <https://cs5435.github.io/>
 - Reading materials
 - Slack for discussions and Q&A, lecture notes
 - 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 5260 studio module in the spring (8 lectures)

- 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 homeworks (15% each)
- Two exams (15% each)
 - Format TBD
- Attendance and participation (10%)
- Cornell University **Code of Academic Integrity** will be strictly enforced

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**

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

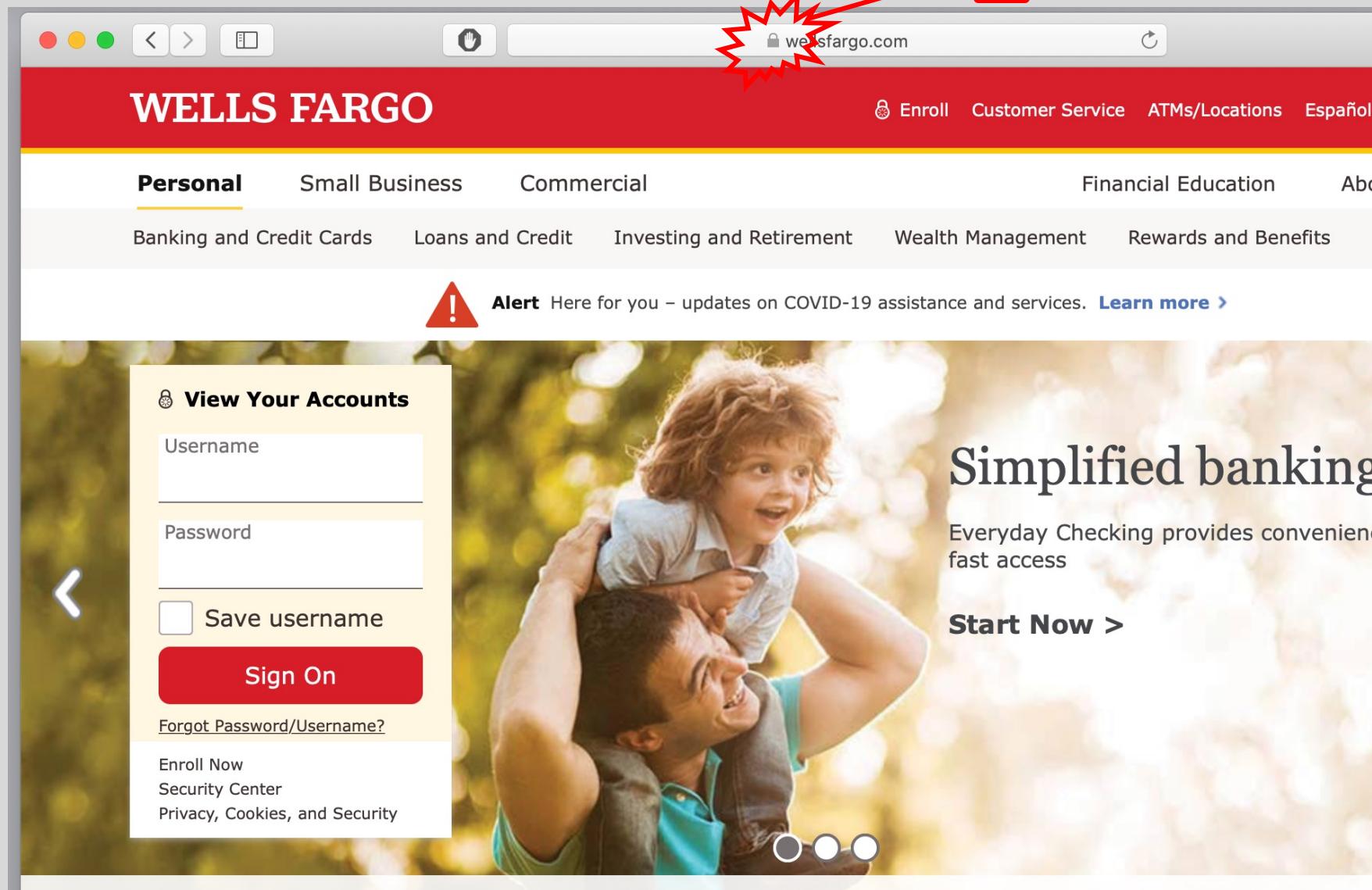
- No textbook
- Occasional readings (see course website)
- Lectures will cover some material that is not in the notes or readings – and **you will be tested on it!**

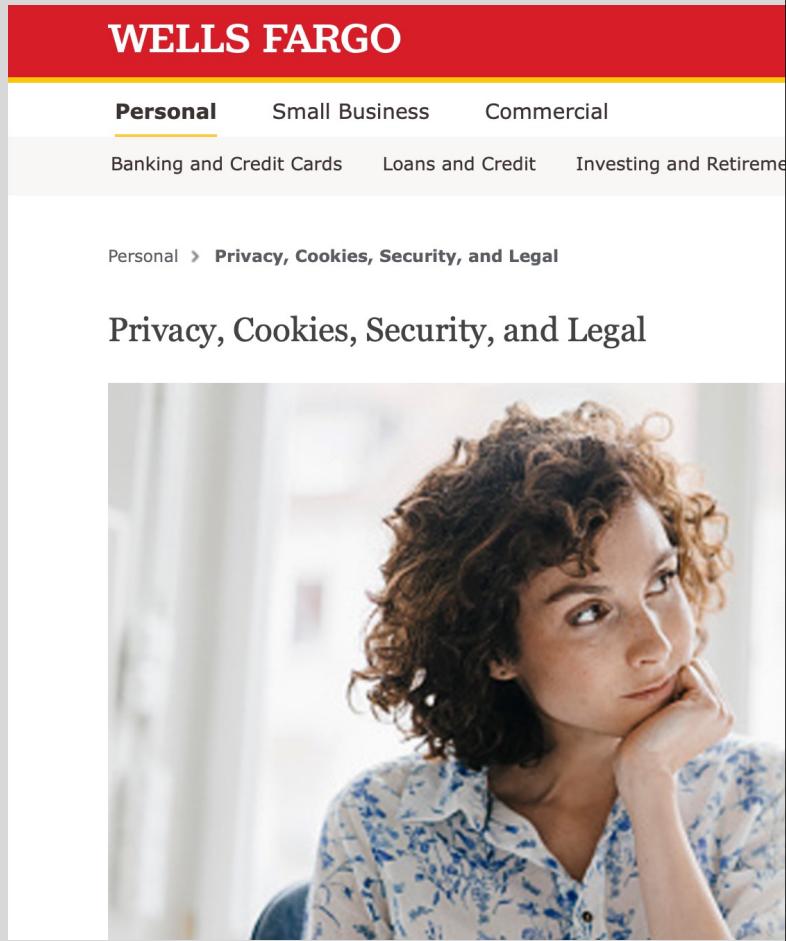
A Few Old (but Still Relevant) Books

- Ross Anderson’s “*Security Engineering*”
 - Focuses on design principles for secure systems
 - Many entertaining examples: banking, nuclear command and control, burglar alarms
- “*The Shellcoder’s Handbook*”
 - Practical how-to manual for hacking attacks (somewhat obsolete)
 - May be useful for the buffer overflow project
- Kevin Mitnick’s “*The Art of Intrusion*”
 - Real-world hacking stories
 - Good illustration for many concepts in this course

Learning Objectives

- Understand the system's security goals
- Learn to spot security vulnerabilities
- Think through how attacks would play out
- Understand and deploy countermeasures





WELLS FARGO

Personal Small Business Commercial

Banking and Credit Cards Loans and Credit Investing and Retirement

Personal > Privacy, Cookies, Security, and Legal

Privacy, Cookies, Security, and Legal

A woman with curly hair, resting her chin on her hand, looking thoughtful.

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

- System **correctness**: system satisfies specification
 - For reasonable input, get reasonable output
- System **security**: system properties preserved in face of attack
 - For unreasonable input, output not completely disastrous
- Main difference: **active interference from an adversary**
- 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)

A Security Engineer's Mindset



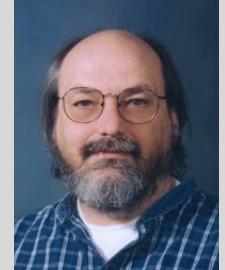
*Credit:
Bruce Schneier*

Ken Thompson



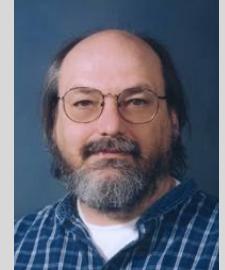
ACM Turing Award, 1983

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?

Reflections on Trusting Trust



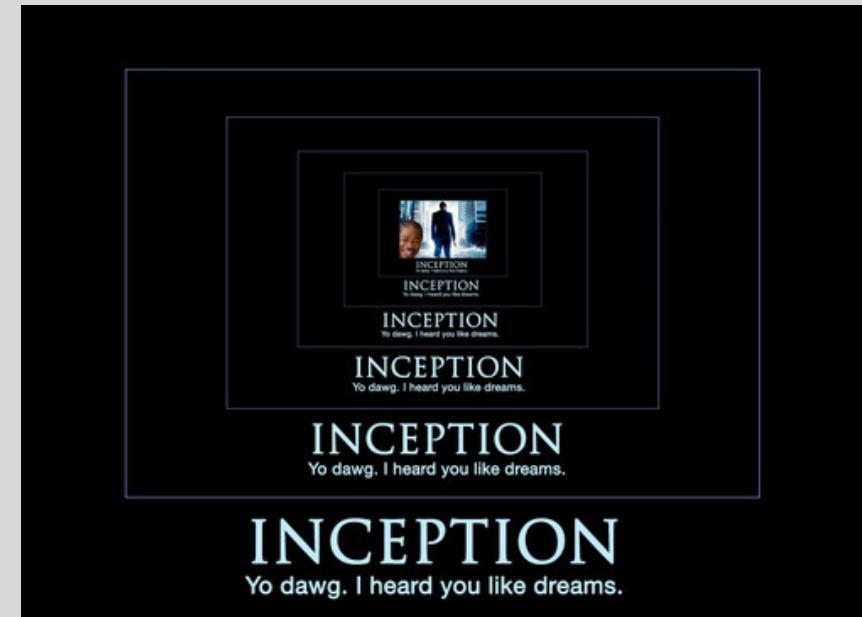
- Who wrote the compiler?
- Compiler looks for source code that looks the login process,
inserts backdoor into it
- Ok, inspect the source code of the compiler... Looks good?
Recompile the compiler!
- Does this solve the problem?

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 */ }
```

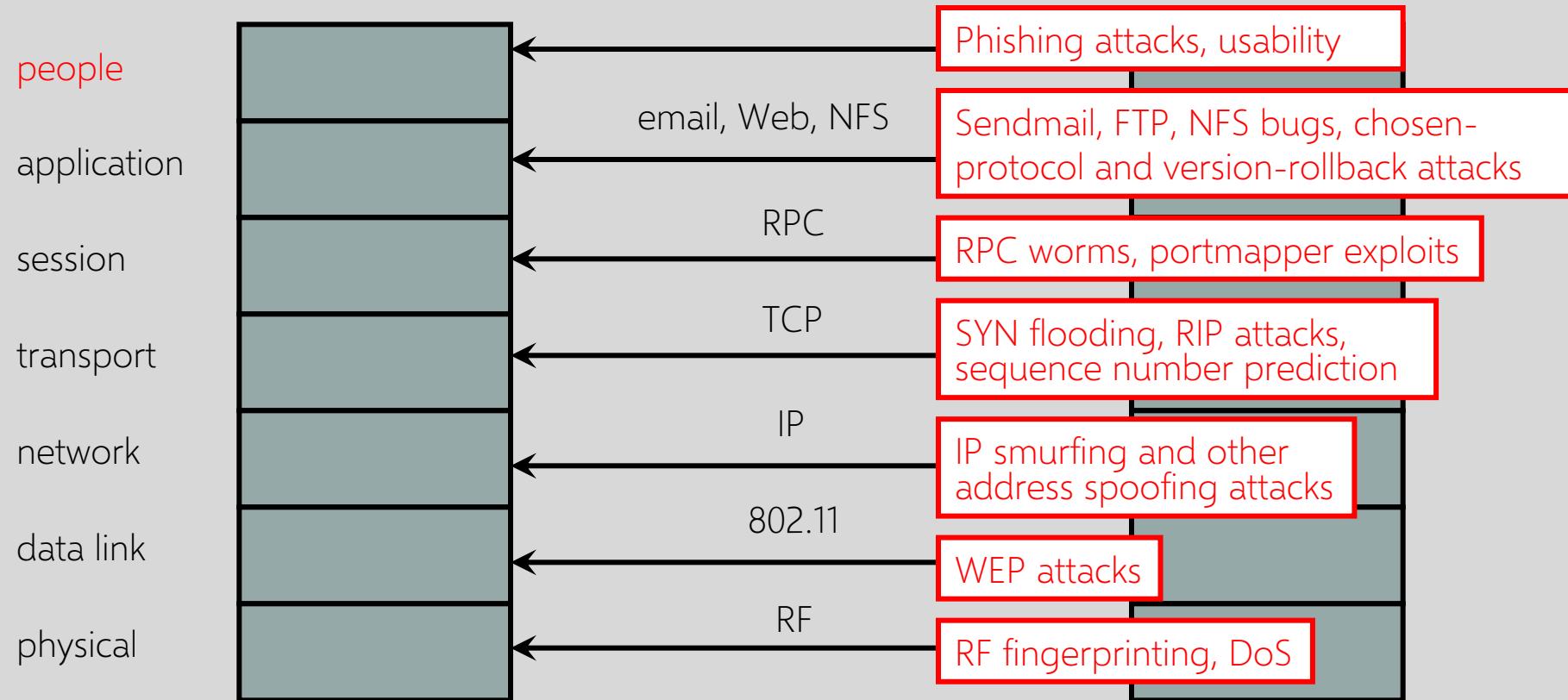


Reflections on Trusting Trust



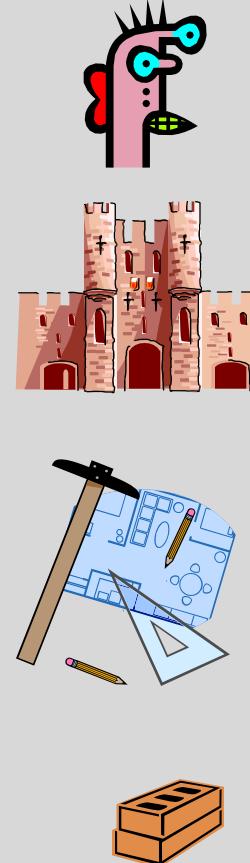
"The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)"

Network Stack



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

Network Defenses

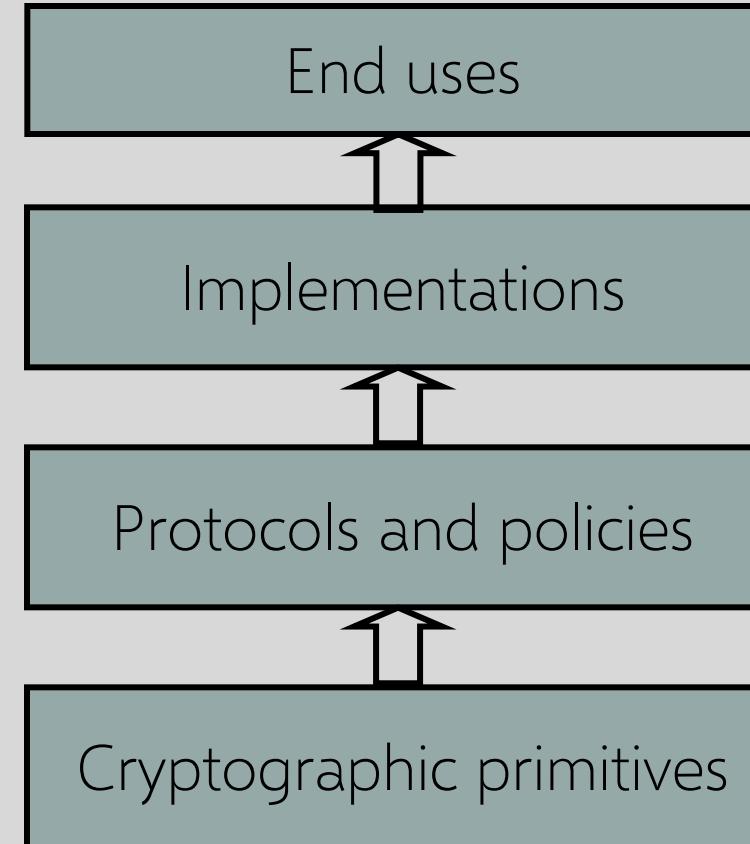


People

Systems

Blueprints

Building
blocks



Password managers,
company policies...

Firewalls, intrusion
detection...

TLS, VPN,
access control...

RSA, DSS, SHA...

All defense mechanisms must work correctly and securely

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

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 5260 studio module in the spring (8 lectures)

- 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



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 on your own system
 - 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

The screenshot shows the Metasploit Project website. At the top, there's a navigation bar with links for 'LEARN MORE', 'DOWNLOAD METASPLOIT', 'GET SUPPORT', 'STAY UPDATED', and 'GET INVOLVED'. Below the navigation is a search bar. The main content area is titled 'Browse Exploit & Auxiliary Modules'. It features a sub-headline about the world's largest database of quality assured exploits. There are several search input fields: 'Open Source Vulnerability DataBase ID', 'Bugtraq ID', 'Full Text Search', 'Common Vulnerabilities Exposures ID', and 'Microsoft Security Bulletin ID'. A 'SEARCH MODULES >' button is located at the bottom right of these fields.

The screenshot shows a search interface with a title 'Search'. Below it, a message reads: 'Wondering what is this website ? Read details here: [How to search for Open Amazon s3 Buckets and their contents](#)'. Underneath is a section titled 'Keywords' with a text input field containing 'keywords'. Below that is a checkbox labeled 'Full Path'. At the bottom is a large blue 'Search' button.

About S3: The Story of a Hack

- 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."

<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 Uber’s former Chief Security Officer with obstruction of justice

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...



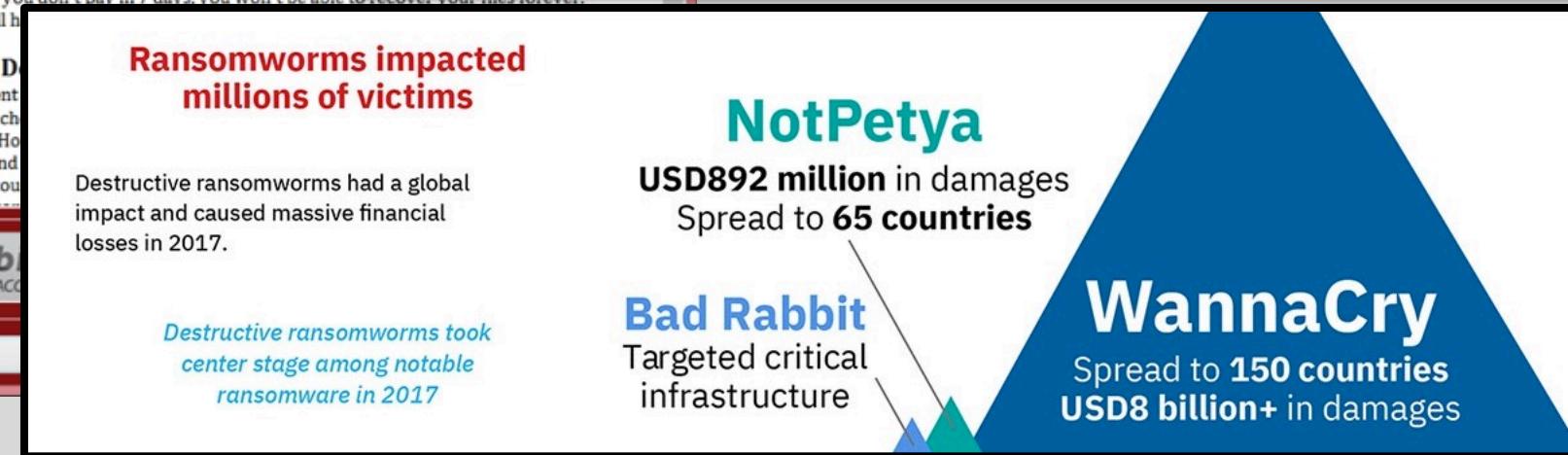
“Hacktivists”



Economically Motivated Criminals



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



A Brief History of WannaCry (2017)

- Used the EternalBlue exploit for propagation
 - A Windows exploit discovered by NSA, stolen and released by "The Shadow Brokers"
- Cryptoworm origin unclear
 - Attributed to North Korea
- Infected over 230,000 machines
 - Disrupted service at 16 hospitals in the UK, also affected FedEx, Telefonica, Russian Interior Ministry, Honda, ...

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 HTTPS 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 HTTPS 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 - Edge 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

- 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 since then, indicating supply glut

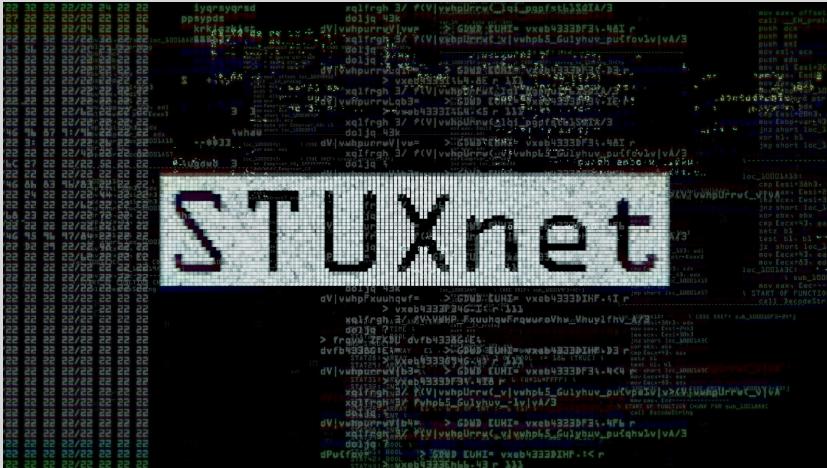
Source: Trend Micro, "Russian Underground 2.0", 2015

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)



Nation-States



Sabotage of Iranian nuclear program

China accused of cyber-attack on Microsoft Exchange servers

2016 hack of Democratic National Committee



North Korean bank heists

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
- 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
 - We'll study some, but by no means all, in this course
- 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

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 5260 studio module in the spring (8 lectures)

- 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!