

Security and Privacy Concepts in the Wild

Vitaly Shmatikov

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.

Hackers Steal \$10M in “Wonderfully Done” fraud from Norway’s State Investment Fund

 by [Graham Cluley](#) on May 18, 2020

Norfund, the Norwegian state-owned investment fund for developing countries, has [revealed](#) that it has been swindled out of US \$10,000,000 (approximately 100 million Norwegian Krona) intended for an institution in Cambodia.

Garmin reportedly paid millions to resolve its recent ransomware attack

The company is said to have made the payment through a third party.

 Kris Holt, @krisholt
August 3, 2020

9
Comments



A game of 'cat and mouse': Hacking attacks on hospitals for patient data increase during coronavirus pandemic

[Karen Weintraub](#) USA TODAY

Published 6:01 a.m. ET Jul. 12, 2020 | Updated 3:02 p.m. ET Jul. 13, 2020

Bezos, Musk, Gates, Obama and others target of cryptocurrency hack on Twitter

Jefferson Graham, Emre Kelly and Mike Snider USA TODAY

Published 5:42 p.m. ET Jul. 15, 2020 | Updated 9:07 a.m. ET Jul. 16, 2020

The Twitter accounts of prominent figures from the worlds of tech and money, celebrities, a presidential candidate and a former president were all hacked Wednesday in what was the largest breach in the company's history.

Bogus messages soliciting bitcoin appeared on the Twitter accounts for Tesla CEO Elon Musk, Microsoft co-founder Bill Gates, Amazon CEO and founder Jeff Bezos, Berkshire Hathaway CEO and president Warren Buffett, former President Barack Obama, presumptive Democratic candidate Joe Biden, former New York mayor Michael Bloomberg, Israeli Prime Minister Benjamin Netanyahu and the corporate accounts for Apple.

Celebrities were also targeted, including rapper Kanye West and his wife Kim Kardashian and rapper Wiz Khalifa.

Twitter said late Wednesday that it detected what it believes was a "coordinated social engineering attack by people who successfully targeted some of our employees with access to internal systems and tools."

U.S. Warns of Global Bank Heist Campaign by North Korean Hackers

[WSJ], August 27 2020]

WASHINGTON—Hackers tied to the North Korean government are trying to rob banks across the globe by draining ATMs and initiating fraudulent money transfers, in an effort by the cash-strapped Pyongyang regime to [fund its nuclear weapons program](#), multiple federal government agencies warned Wednesday.

The campaign includes so-called spearphishing attacks—which use fraud or persuade the victim to reveal a password or other sensitive information—and social engineering schemes. It has been underway since at least February and represents a respite from a recent apparent lull in bank robberies by

spearphishing... and social engineering schemes

... means what?

Major Data Breaches

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

Entity	Year	Records	Organization type	Method
Clearview AI	2020	3,000,000,000 (Number of photos obtained)	information technology	hacked
Yahoo	2013	3,000,000,000	web	hacked
First American Corporation	2019	885,000,000	financial service company	poor security
Facebook	2019	540,000,000	social network	poor security
Marriott International	2018	500,000,000	hotel	hacked
Yahoo	2014	500,000,000	web	hacked
Friend Finder Networks	2016	412,214,295	web	poor security / hacked
Exactis	2018	340,000,000	data broker	poor security
Truecaller	2019	299,055,000	Telephone directory	unknown
MongoDB	2019	275,000,000	tech	poor security
Facebook	2019	267,000,000	social network	poor security
Microsoft	2019	250,000,000	tech	data exposed by misconfiguration
MongoDB	2019	202,000,000	tech	poor security
Unknown agency (believed to be tied to United States Census Bureau)	2020	200,000,000	financial	accidentally published

Learning Objectives

Understand the system's **security goals**

Learn to spot security **vulnerabilities**

Think through how **attacks** would play out

Understand and deploy **countermeasures**

Course Personnel

Instructor: **Vitaly Shmatikov**

- Office hours by request

TA: **Congzheng Song**

- Office hours TBA

Graders: **Pratyush Sharma, Anam Tahir**

Course website: <https://cs5435.github.io/>

- Reading materials, lecture notes

Piazza for discussions and Q&A

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
 - You must have detailed understanding of x86 architecture, 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**

Course Logistics

Mix of live and recorded lectures, recitations

- Tuesday, Thursday 12n-12:50p, 10-10:50p ET
- Zoom link posted as a Canvas announcement

Four homeworks (60% of the grade)

Midterm (15% of the grade)

Final (15% of the grade)

- Both exams are take-home

Attendance and participation (10% of the grade)

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 assigned readings

- Will be posted on the course website

Attend **two sessions per week**

- Either at 12 or 10, your choice
- One live lecture, one recitation... at least for now

Watch recorded lectures

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

A Few Helpful Books

Ross Anderson's "Security Engineering"

- Focuses on design principles for secure systems
- Wide range of entertaining examples: banking, nuclear command and control, burglar alarms

"The Shellcoder's Handbook"

- Practical how-to manual for hacking attacks
- Not a required text, but you may find it useful for the buffer overflow project

Kevin Mitnick's "The Art of Intrusion"

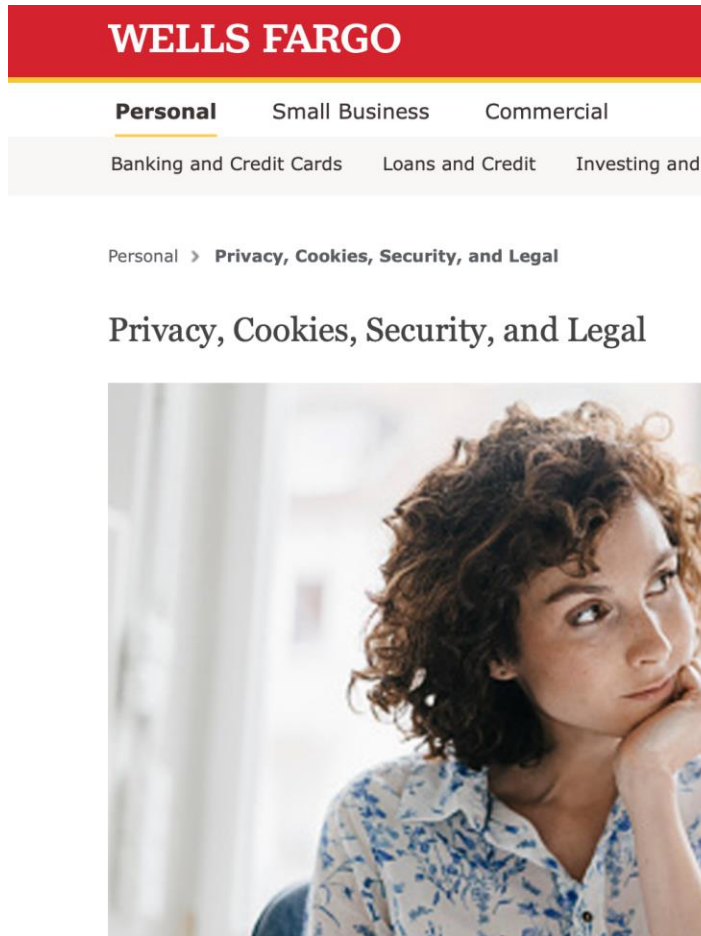
- Real-world hacking stories
- Good illustration for many concepts in this course

Motivation



A screenshot of the Wells Fargo website. The browser's address bar shows 'wellsfargo.com' with a red starburst effect around the lock icon. The website has a red header with the 'WELLS FARGO' logo and navigation links for 'Enroll', 'Customer Service', 'ATMs/Locations', and 'Español'. Below the header is a navigation bar with categories like 'Personal', 'Small Business', 'Commercial', 'Financial Education', and 'About Us'. A secondary navigation bar lists services such as 'Banking and Credit Cards', 'Loans and Credit', 'Investing and Retirement', 'Wealth Management', and 'Rewards and Benefits'. An alert banner with a red triangle icon states: 'Alert Here for you – updates on COVID-19 assistance and services. Learn more >'. The main content area features a large background image of a man carrying a young child on his shoulders. On the left, there is a 'View Your Accounts' login form with fields for 'Username' and 'Password', a 'Save username' checkbox, a red 'Sign On' button, and links for 'Forgot Password/Username?', 'Enroll Now', 'Security Center', and 'Privacy, Cookies, and Security'. On the right, the text 'Simplified banking' is displayed, followed by 'Everyday Checking provides convenient fast access' and a 'Start Now >' link. At the bottom of the image, there are three small white circles.

“Privacy, Cookies, Security, and Legal”



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?

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

...

Who Are the Adversaries?

"31337" script kiddies

Abusers / harassers / cyberstalkers

"Hacktivists"

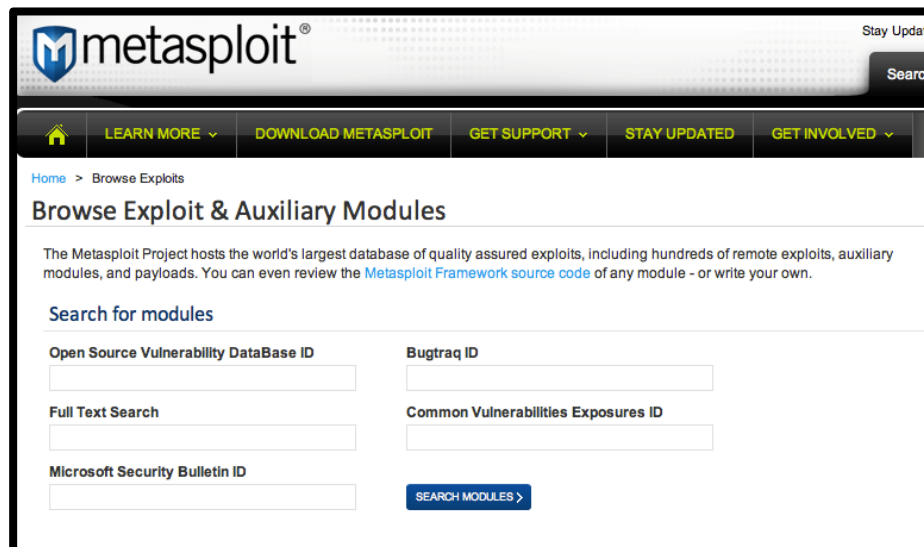
Criminals (often economically motivated)

Nation states

Hacking Commoditized

Metasploit

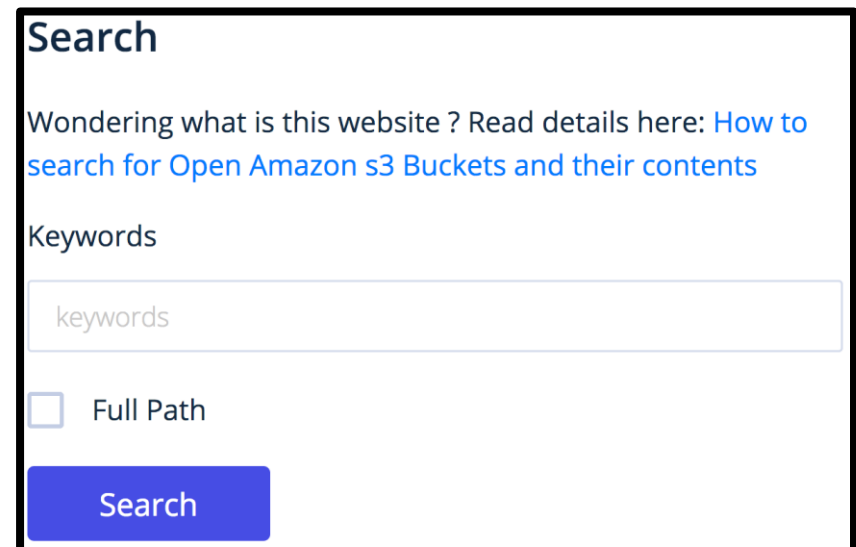
- All-in-one penetration testing tool
- Easy-to-use exploit libraries



The screenshot shows the Metasploit website's 'Browse Exploits' page. At the top is the Metasploit logo and a navigation bar with links: 'LEARN MORE', 'DOWNLOAD METASPLOIT', 'GET SUPPORT', 'STAY UPDATED', and 'GET INVOLVED'. Below the navigation bar, the page title is 'Browse Exploit & Auxiliary Modules'. A paragraph explains that the Metasploit Project hosts a large database of quality-assured exploits, including remote exploits, auxiliary modules, and payloads. It also mentions that users can review the 'Metasploit Framework source code' of any module or write their own. Below this text is a 'Search for modules' section with four input fields: 'Open Source Vulnerability DataBase ID', 'Bugtraq ID', 'Full Text Search', and 'Common Vulnerabilities Exposures ID'. There is also a 'Microsoft Security Bulletin ID' field. A 'SEARCH MODULES >' button is located at the bottom right of the search section.

Public Amazon S3 buckets, AWS credentials

- Source of many recent breaches



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

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 to Not 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

August 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
 - ...

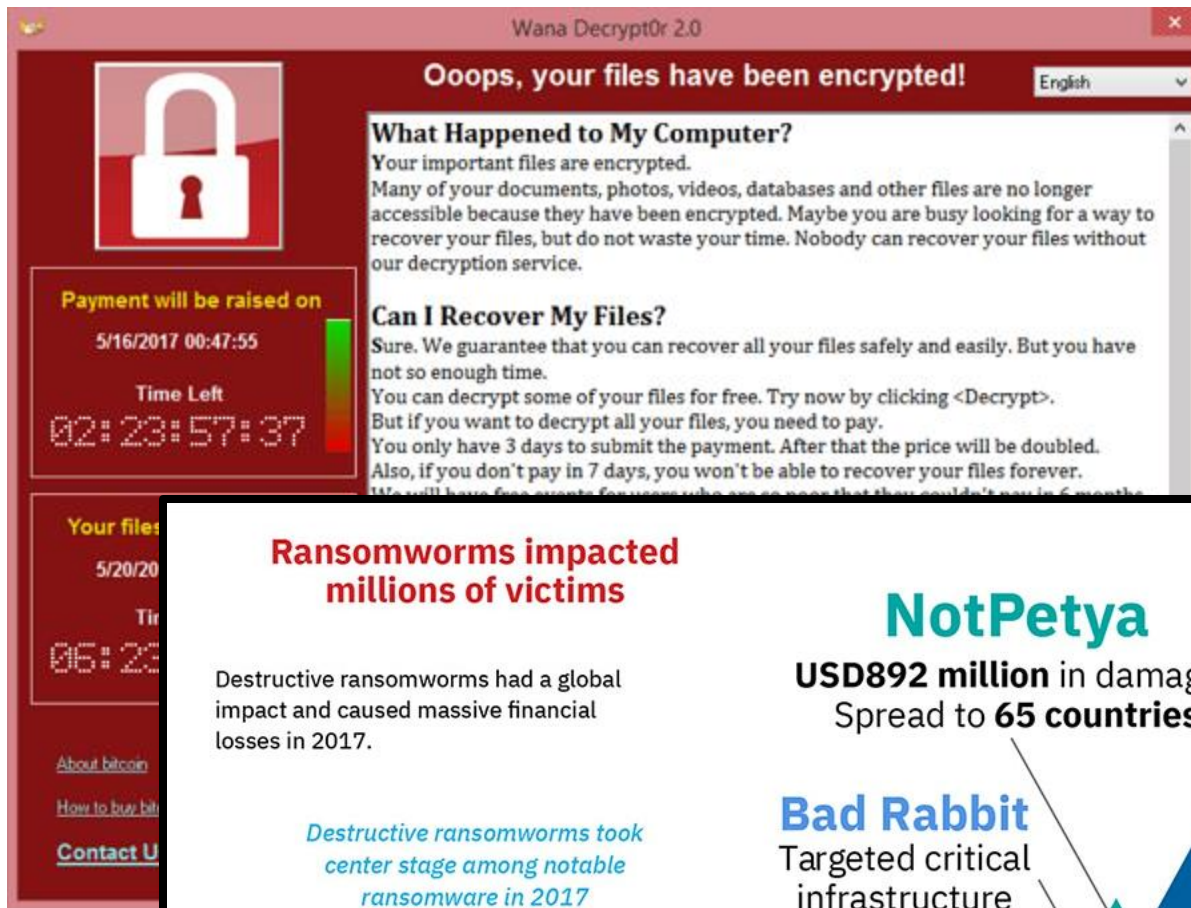


"Hacktivists"

WE ARE ANONYMOUS
WE ARE LEGION.
WE DO NOT FORGIVE.
WE DO NOT FORGET.
EXPECT US.



Economically Motivated Criminals



Ransomware impacted millions of victims

Destructive ransomworms had a global impact and caused massive financial losses in 2017.

Destructive ransomworms took center stage among notable ransomware in 2017

NotPetya

USD892 million in damages
Spread to **65 countries**

Bad Rabbit

Targeted critical infrastructure

WannaCry

Spread to **150 countries**
USD8 billion+ in damages

Brief History of WannaCry (2017)

Exploit used for propagation: EternalBlue

- 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 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 <u>without</u> 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 <u>without</u> 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) <u>without</u> a sandbox escape (previously: \$50,000) \$100,000 - Safari RCE (iOS) <u>without</u> 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

 [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 since then, indicating supply glut

Marketplace for Victims

 [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

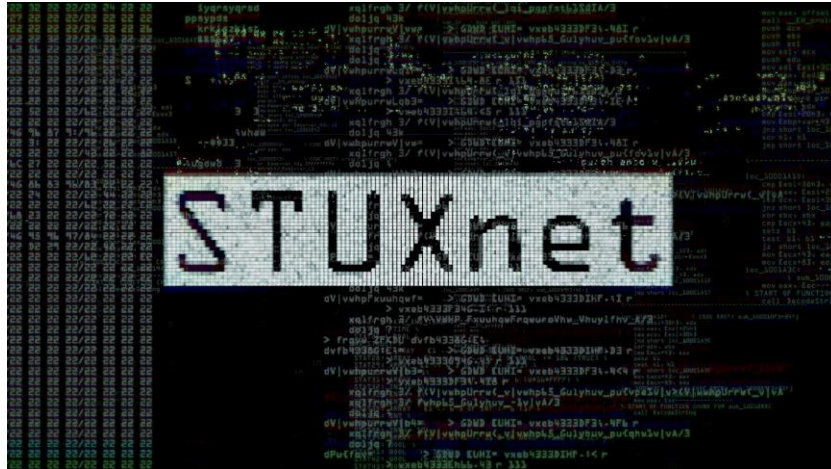
- DDoS: up to \$100/hour
- Spam: from \$1/10,000 emails

Tools and services

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



Nation-States



Sabotage of Iranian nuclear program

2016 hack of Democratic National Committee



Russian 'actors' tried to interfere with Britain's general election, U.K. government says

"The Government has concluded that it is almost certain that Russian actors sought to interfere in the 2019 General Election."

Main Themes of the Course

Vulnerabilities of modern systems and networks

- Phishing, denial of service, worms and botnets, attacks on Web applications, attacks on infrastructure

Defensive technologies

- Authentication
- Web and mobile security
- Basic cryptography, application- and transport-layer security protocols
- Protection of software: memory integrity, firewalls, 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...

Peek at the Dark Side



CULT OF THE DEAD COW
PARAMEDIA • est. 1984 w/666

BlackHat
USA • EUROPE • ASIA
Training



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

Correctness versus 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 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

[Bruce Schneier]

NOW! YOUR VERY OWN EXCITING ANT FARM AS SEEN ON TV!

AN ANT'S ENTIRE WORLD! COMPLETE WITH STOCK OF LIVE ANTS!

WHAT IS AN "ANT FARM"?

The ANT FARM is a clear, unbreakable plastic, insect-proof case, measuring 9" x 7", containing farm buildings, a windmill, silo, trees and landscape, complete with soil, weather and a pond. The ants work down into the soil and are the master builders of their hills. The FARM is so constructed that the ants are visible from every angle, both above ground and underground.

FASCINATING!

A living TV screen. The ants put on a quiet but exciting drama that will keep you fascinated for hours.

EDUCATIONAL!

An education in nature study as well as work and patience.

WORLD'S TINIEST ENGINEERS!

Ants are actually the world's finest construction engineers. They perform feats of stonemasonry that, if they were to be duplicated by humans, it would take millions of dollars and hundreds of thousands of tons of equipment to perform the same job. But one tiny ant can do it. What's more, the ants seem to have a special sense for construction which has actually been studied by human engineers.

NOW! YOUR VERY OWN

SEE YOUR TINY PETS...

Watch these tiny tunnels run down build rooms - tunnel as they erect bridges and move mountains before your very eyes. Ants are the world's finest engineers and among them plan and construct their intricate highways and sidewalks in fascinating. But they do much more than that! Through the clear plastic walls of your ANT FARM you see the soil within gardening the roads... the laborers carrying their loads... the supply convoys moving ever food for the rest of the colony. Yes, the ANT FARM is actually a LIVING TV SCREEN that will keep you fascinated for hours.

ANTS CANNOT ESCAPE FROM FARM ENCLOSURE!

EXTRA SPECIAL

the new GIANT Ant Farm, a big 30" high for 12" wide case which includes a year's supply of Ant Food, Liquid Feeder, Supply of California Soil, "Ant Watcher's Handbook" and "Black Certificate" for a genuine supply of live ants.

ONLY \$2.98

\$6.95

MAX, TODAY... Money Back Guarantee!... No C.O.D.'s

ANT FARM, Department 63
P.O. Box 281, Rockville Centre, New York

Rush me my ANT FARM which will include a "Stock Certificate" for a free supply of ants and an "Ant Watcher's Manual." Enclosed is \$2.98, plus 22% postage for each ANT FARM ordered.

Send me the GIANT sized ANT FARM which is 30" x 12", in size and includes an "Ant Watcher's Handbook," a Certificate for a free supply of ants, Ant Food, Ant Feeder, for only \$6.95 each, plus 50% postage.

NAME _____

ADDRESS _____

CITY _____ STATE _____ ZIP CODE _____

DISCOVER HOW ANTS LIVE... WORK... PLAY! ORDER NOW!

Ken Thompson



ACM Turing Award, 1983

"Reflections on Trusting Trust"

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



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"

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



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?

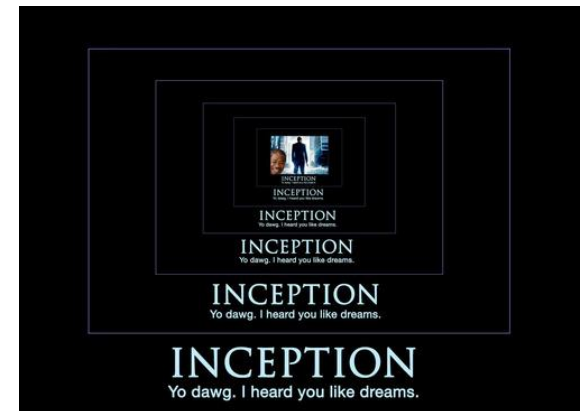
"Reflections on Trusting Trust"

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



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 */  
}
```



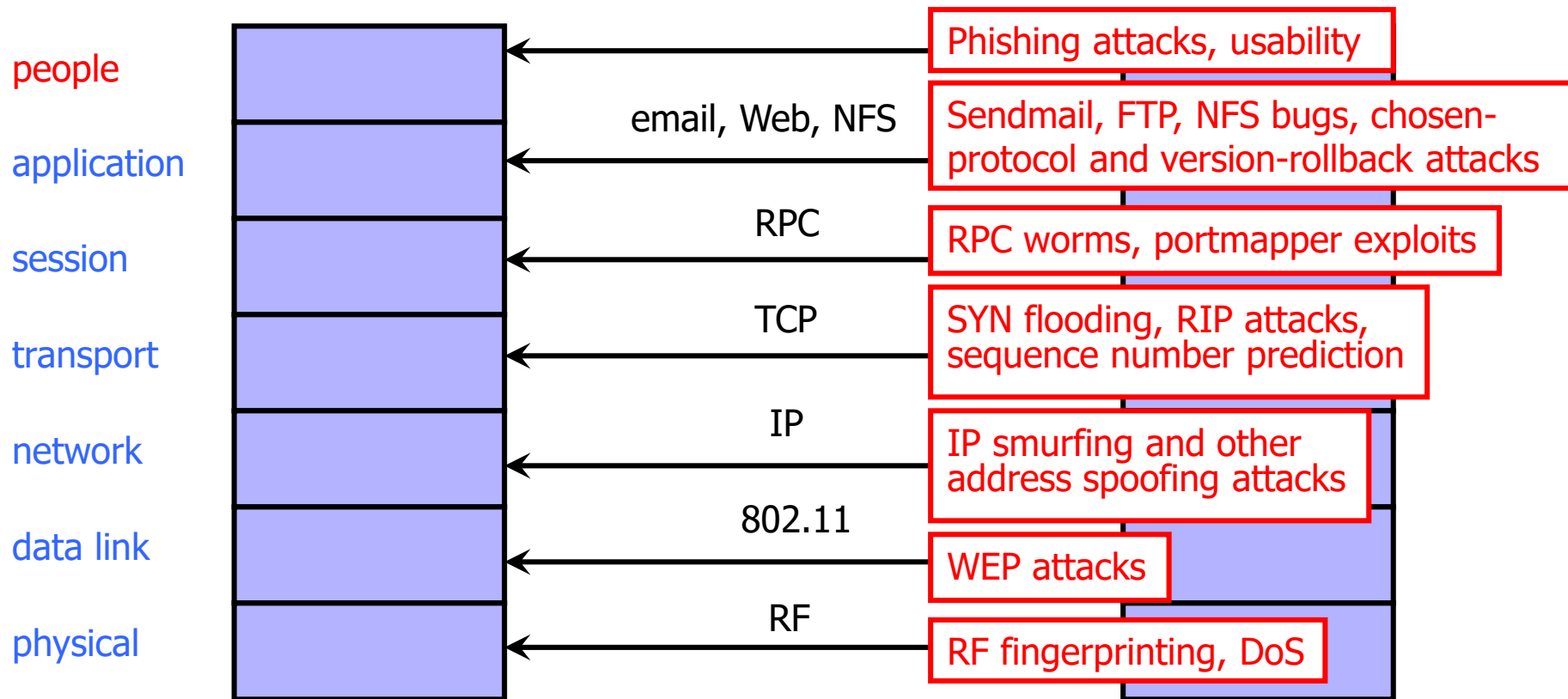
"Reflections on Trusting Trust"

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



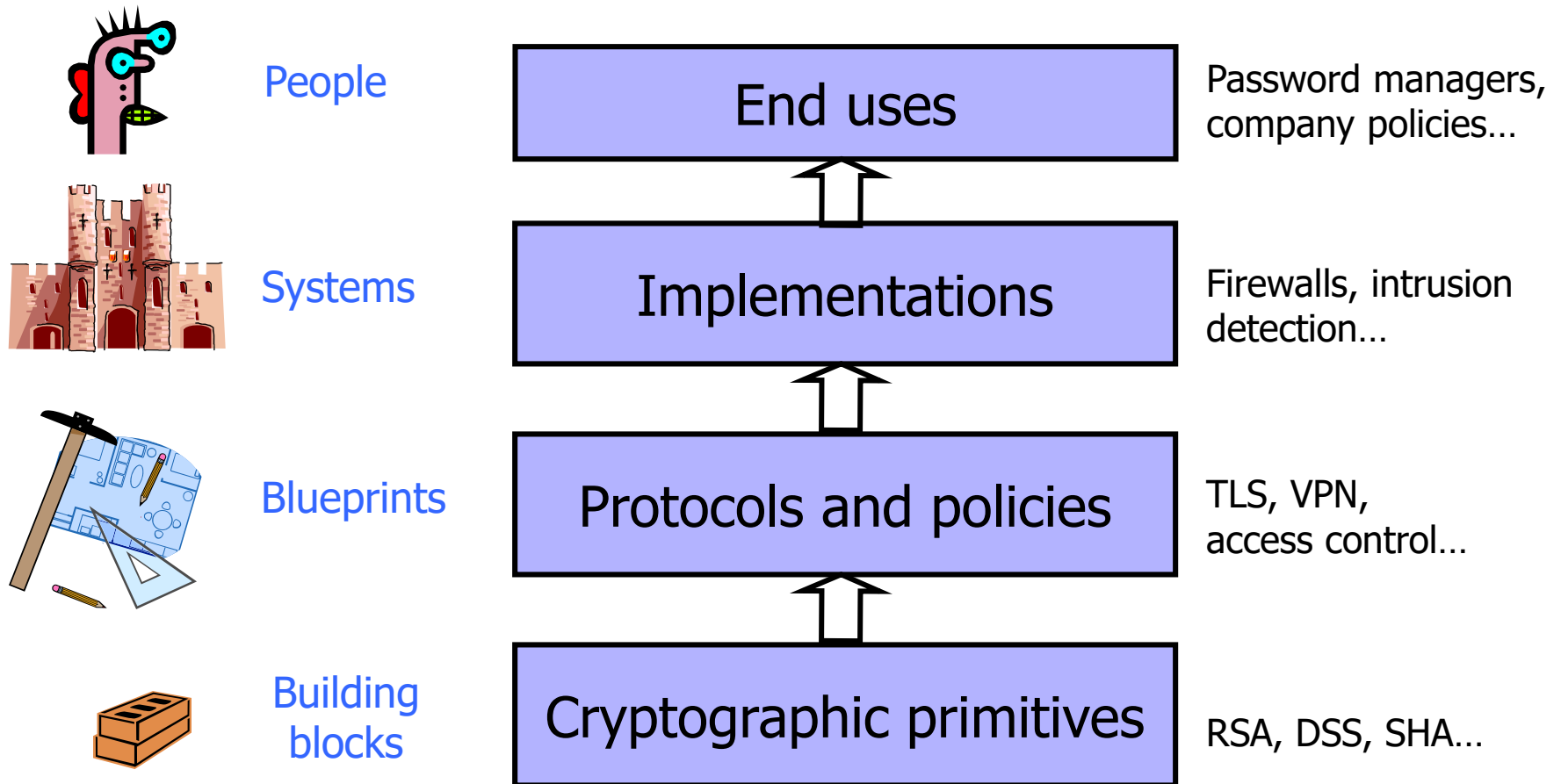
"The moral is obvious. You can't trust code that you did not totally create yourself. (Especially code from companies that employ people like me.)"

Network Stack



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

Network Defenses



All defense mechanisms must work correctly and securely

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 misunderstanding

Security awareness and user "buy-in" help

Other important factors: usability and economics

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