CPSC 467: Cryptography and Security

Michael J. Fischer

Lecture 1
September 1, 2020

Slide credits: Mariana Raykova, Tom Ristenpart, Stefano Tessaro, as well as the teaching slides for *Introduction to Security* by Goodrich, Tamassia

Highlights from Syllabus

Course Overview

Data Breaches

Highlights from Syllabus

Expectations

Read the syllabus! Some highlights:

- This course uses two web sites:
  - Canvas: `yale.instructure.com`
  - Zoo: https://zoo.cs.yale.edu/classes/cs467/2020f/index.html
- Pay attention to policies on plagiarism, submitting your work, and participating in class.
- Teaching assistant is Talley Amir. The UTA is Diego Meucci.
- Assessment will be by scheduled quizzes and exams. They will all be open book and open notes, which means they will be designed to test understanding, not memorization.
- You will use the Zoo for programming and Canvas for homework submissions.

Class attendance

Class attendance and class participation are required. Why?

- I say things that don’t find their way into the lecture notes.
- Your questions help me pace my lectures and address the needs of the class.
- I like teaching much better than lecturing to a silent Zoom screen.
- If you’re confused, others are likely confused too and might be brave enough to ask for clarification. You can learn from them.

Please always feel free to ask questions.

Also, please let me know in case you have to miss class.

Course Overview

Course modules

1. Information Security: Attackers and their motivations
2. Classical Cryptography: Principles of cryptography
3. One-Key Cryptosystems: Modern private key cryptosystems
4. Two-Key Cryptosystems: Modern public key cryptosystems
5. Digital Signatures: Protecting information integrity
6. Cryptographic Hash Functions: Digital fingerprints; blockchain
7. Authentication: Establishing legitimacy of information
8. Multiparty Protocols: Controlling flow of information

Each module comprises roughly three lectures, one or two homework assignments, and one quiz.

Computer science, mathematics and cryptography

Cryptography cuts across both computer science and mathematics.

Computer science: Cryptography underlies much security software. The algorithms must be implemented correctly and efficiently.

Mathematics: Mathematics underlies both algorithms and their security analysis.

Many cryptographic primitives are based on:

- Number theoretic problems such as factoring and discrete log;
- Algebraic properties of structures such as elliptic curves.

Some useful mathematics

Cryptography cuts across traditional areas of mathematics. Some topcs relevant to cryptography:

- Probability and statistics.
- Coding theory.
- Complexity theory.
- Number theory.
- Algebra.

We will draw from pure mathematics to provide insight for how algorithms work and why they are believed secure. No specific prior knowledge of any of these areas is expected. The relevant mathematical facts will be presented as needed.

Organization

The main body of the course is organized around *cryptographic primitives*. For each one:

- What can be done with it? Study of cryptographic algorithms and protocols.
- What are its properties? Modeling and analysis. Requires complexity theory, probability theory, and statistics.
- How does it work? Requires some mathematics, particularly number theory and algebra.
- How is it implemented? Requires attention to detail, especially to prevent accidental leak of secret information.

What this course is not

This course is broad rather than deep.

- Only enough mathematics to understand algorithmes such as AES, RSA, ElGamal, and elliptic curves will be presented.
- It will only briefly touch on cryptanalysis, the flip side of cryptography.
- It will not go deeply into real-world security protocols.
- It will not talk about security mechanisms for computer and network devices and applications such as firewalls, operating system access controls, detecting software security holes, or dealing with web security vulnerabilities.

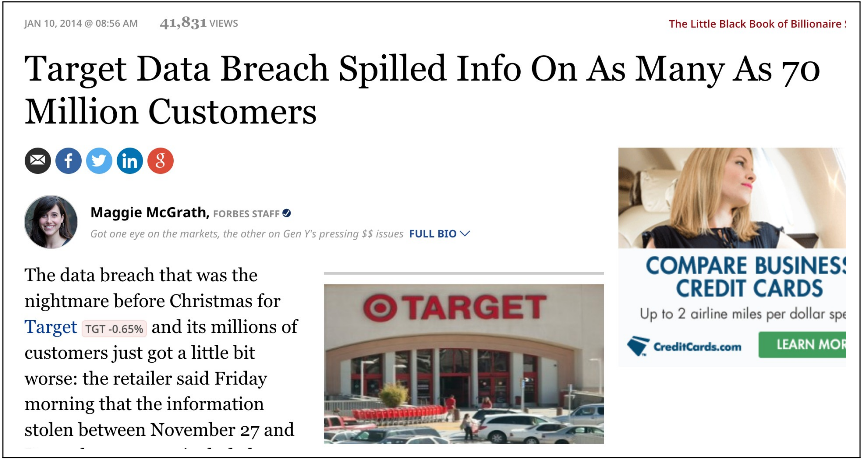
Data Breaches

Protecting information in the real world

Massive security breaches are disclosed almost daily.

- Identity theft.
- Industrial espionage.
- Cyberwarfare.
- Denial-of-service.
- Surveillance.
- Misuse of personal data.
- Ransomware attacks.

Credit card numbers stolen



JAN 10, 2014 @ 08:56 AM 41,831 VIEWS

The Little Black Book of Billionaire S

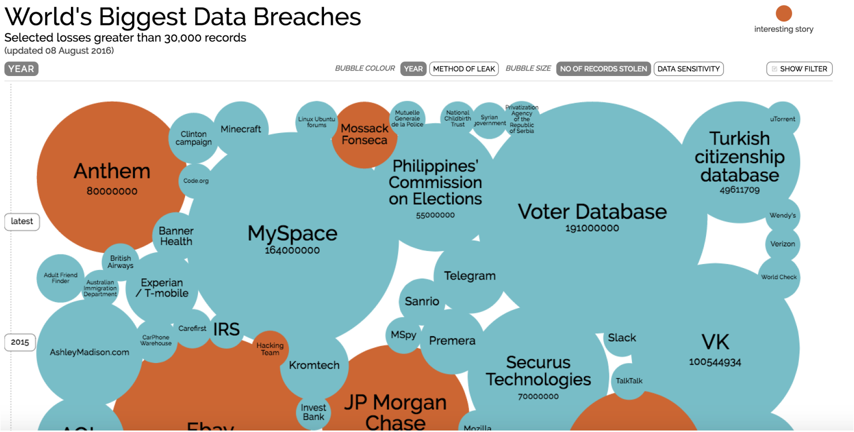
Target Data Breach Spilled Info On As Many As 70 Million Customers

Maggie McGrath, FORBES STAFF

Got one eye on the markets, the other on Gen Y's pressing $$ issues **FULL BIO**

The data breach that was the nightmare before Christmas for Target TGT -0.65% and its millions of customers just got a little bit worse: the retailer said Friday morning that the information stolen between November 27 and

How things looked in August 2016

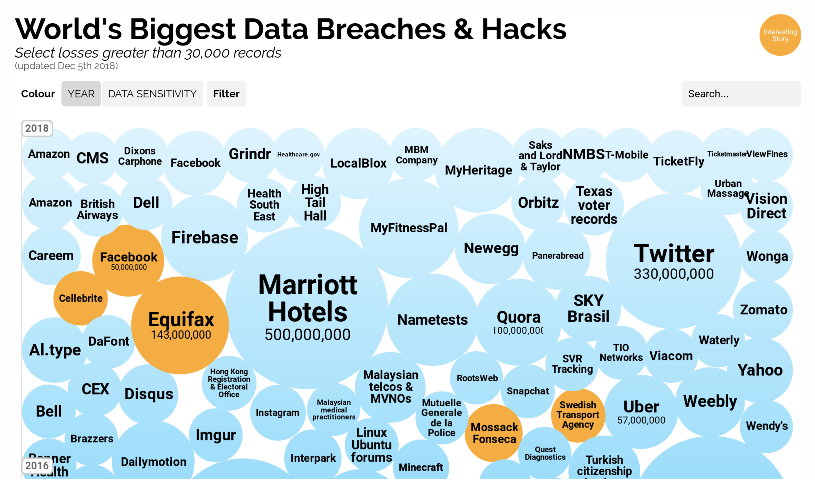


World's Biggest Data Breaches

Selected losses greater than 30,000 records

(updated 08 August 2016)

How things looked in December 2018

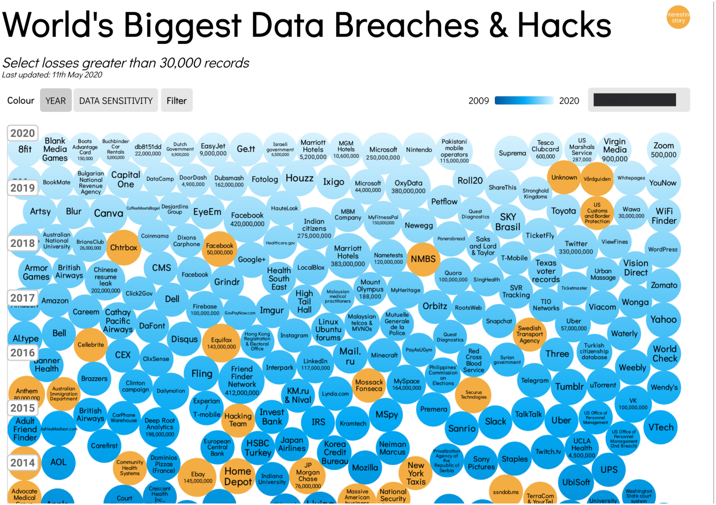


World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records

(updated Dec 5th 2018)

Fast forward to May 2020



World's Biggest Data Breaches & Hacks

Select losses greater than 30,000 records
Last updated: 11th May 2020

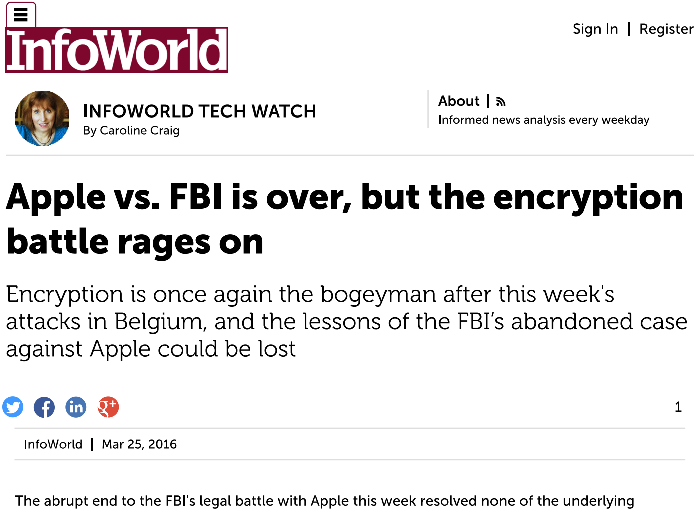
Colour YEAR DATA SENSITIVITY Filter 2009 2020 [redacted]

Interactive visualization

The previous images came from the Information is Beautiful interactive web site, `http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks`.

Click here to try it for yourself.

Round 2 of the crypto wars



InfoWorld

Sign In | Register

INFOWORLD TECH WATCH

By Caroline Craig

About |

Informed news analysis every weekday

Apple vs. FBI is over, but the encryption battle rages on

Encryption is once again the bogeyman after this week's attacks in Belgium, and the lessons of the FBI's abandoned case against Apple could be lost

1

InfoWorld | Mar 25, 2016

The abrupt end to the FBI's legal battle with Apple this week resolved none of the underlying

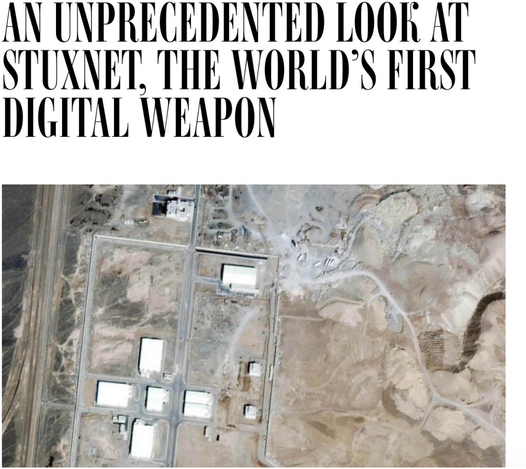
Round 3 of the crypto wars

WASHINGTON—When Attorney General William Barr returned to the Justice Department last year, law-enforcement officials briefed him on how encryption and other digital-security measures were hindering investigations into everything from child sex abuse to terrorism.

Mr. Barr was surprised and puzzled, according to people familiar with the meeting. The government was struggling with similar problems when he first served as attorney general nearly 30 years ago, he told advisers. Why had they not been solved?

[The Wall Street Journal, Jan. 17, 2020.
Barr's Encryption Push Is Decades in the Making, but Troubles Some at FBI]

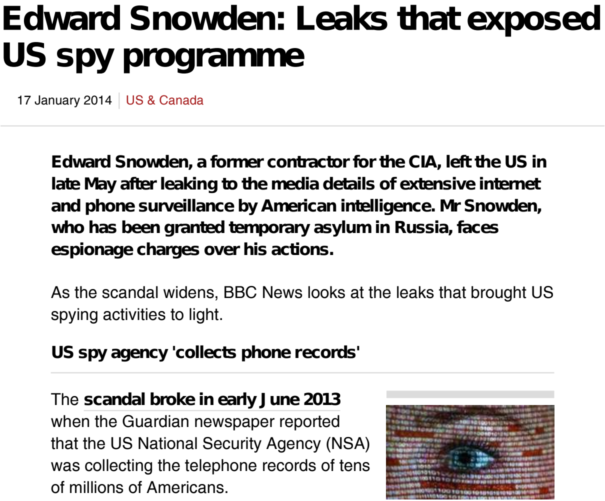
Cyberwarfare



AN UNPRECEDENTED LOOK AT STUXNET, THE WORLD'S FIRST DIGITAL WEAPON

Wired, Nov. 3, 2014

Even the NSA can’t protect its secrets



Edward Snowden: Leaks that exposed US spy programme

17 January 2014 | US & Canada

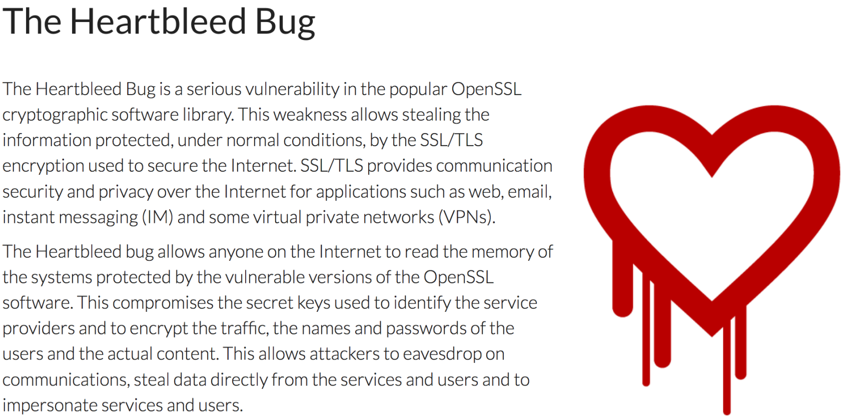
Edward Snowden, a former contractor for the CIA, left the US in late May after leaking to the media details of extensive internet and phone surveillance by American intelligence. Mr Snowden, who has been granted temporary asylum in Russia, faces espionage charges over his actions.

As the scandal widens, BBC News looks at the leaks that brought US spying activities to light.

US spy agency 'collects phone records'

The **scandal broke in early June 2013** when the Guardian newspaper reported that the US National Security Agency (NSA) was collecting the telephone records of tens of millions of Americans.

Security software bugs can be exploited

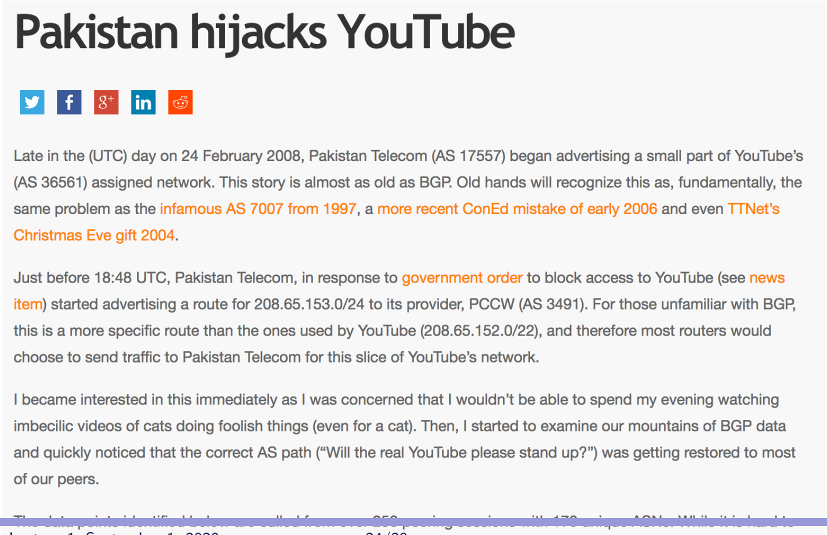


The Heartbleed Bug

The Heartbleed Bug is a serious vulnerability in the popular OpenSSL cryptographic software library. This weakness allows stealing the information protected, under normal conditions, by the SSL/TLS encryption used to secure the Internet. SSL/TLS provides communication security and privacy over the Internet for applications such as web, email, instant messaging (IM) and some virtual private networks (VPNs).

The Heartbleed bug allows anyone on the Internet to read the memory of the systems protected by the vulnerable versions of the OpenSSL software. This compromises the secret keys used to identify the service providers and to encrypt the traffic, the names and passwords of the users and the actual content. This allows attackers to eavesdrop on communications, steal data directly from the services and users and to impersonate services and users.

Network configuration errors



Pakistan hijacks YouTube

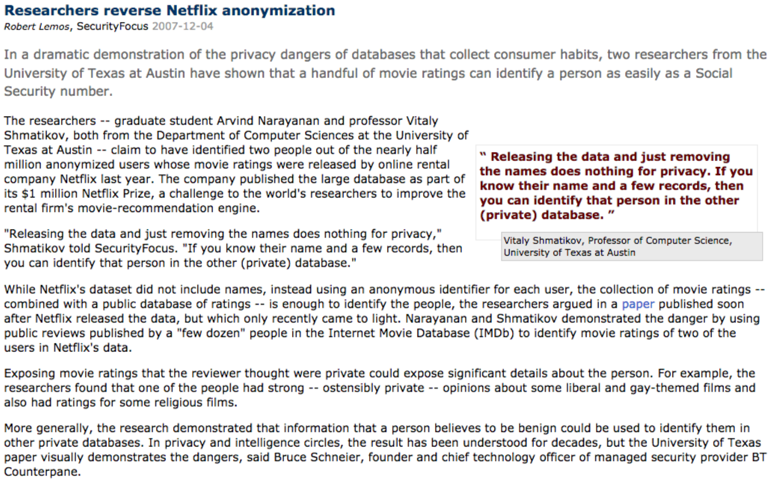
Late in the (UTC) day on 24 February 2008, Pakistan Telecom (AS 17557) began advertising a small part of YouTube's (AS 36561) assigned network. This story is almost as old as BGP. Old hands will recognize this as, fundamentally, the same problem as the infamous AS 7007 from 1997, a more recent ConEd mistake of early 2006 and even TTNet's Christmas Eve gift 2004.

Just before 18:48 UTC, Pakistan Telecom, in response to government order to block access to YouTube (see news item) started advertising a route for 208.65.153.0/24 to its provider, PCCW (AS 3491). For those unfamiliar with BGP, this is a more specific route than the ones used by YouTube (208.65.152.0/22), and therefore most routers would choose to send traffic to Pakistan Telecom for this slice of YouTube's network.

I became interested in this immediately as I was concerned that I wouldn't be able to spend my evening watching imbecilic videos of cats doing foolish things (even for a cat). Then, I started to examine our mountains of BGP data and quickly noticed that the correct AS path ("Will the real YouTube please stand up?") was getting restored to most of our peers.

The data points identified below are culled from over 250 peering sessions with 170 unique ASNs. While it is hard to

Personal info can be compromised despite anonymization



Researchers reverse Netflix anonymization

Robert Lemos, SecurityFocus 2007-12-04

In a dramatic demonstration of the privacy dangers of databases that collect consumer habits, two researchers from the University of Texas at Austin have shown that a handful of movie ratings can identify a person as easily as a Social Security number.

The researchers -- graduate student Arvind Narayanan and professor Vitaly Shmatikov, both from the Department of Computer Sciences at the University of Texas at Austin -- claim to have identified two people out of the nearly half million anonymized users whose movie ratings were released by online rental company Netflix last year. The company published the large database as part of its $1 million Netflix Prize, a challenge to the world's researchers to improve the rental firm's movie-recommendation engine.

"Releasing the data and just removing the names does nothing for privacy," Shmatikov told SecurityFocus. "If you know their name and a few records, then you can identify that person in the other (private) database."

" Releasing the data and just removing the names does nothing for privacy. If you know their name and a few records, then you can identify that person in the other (private) database. "

Vitaly Shmatikov, Professor of Computer Science, University of Texas at Austin

While Netflix's dataset did not include names, instead using an anonymous identifier for each user, the collection of movie ratings -- combined with a public database of ratings -- is enough to identify the people, the researchers argued in a paper published soon after Netflix released the data, but which only recently came to light. Narayanan and Shmatikov demonstrated the danger by using public reviews published by a "few dozen" people in the Internet Movie Database (IMDb) to identify movie ratings of two of the users in Netflix's data.

Exposing movie ratings that the reviewer thought were private could expose significant details about the person. For example, the researchers found that one of the people had strong -- ostensibly private -- opinions about some liberal and gay-themed films and also had ratings for some religious films.

More generally, the research demonstrated that information that a person believes to be benign could be used to identify them in other private databases. In privacy and intelligence circles, the result has been understood for decades, but the University of Texas paper visually demonstrates the dangers, said Bruce Schneier, founder and chief technology officer of managed security provider BT Counterpane.

WannaCry Ransomware[1]

Criminals go where the money is, and cybercriminals are no exception.

And right now, the money is in ransomware.

It's a simple scam. Encrypt the victim's hard drive, then extract a fee to decrypt it. The scammers can't charge too much, because they want the victim to pay rather than give up on the data. But they can charge individuals a few hundred dollars, and they can charge institutions like hospitals a few thousand. Do it at scale, and it's a profitable business.

[1] Notes by Bruce Schneier, *Crypto-Gram*, June 15, 2017.

WannaCry Ransomware (cont.)

And scale is how ransomware works. Computers are infected automatically, with viruses that spread over the internet. Payment is no more difficult than buying something online – and payable in untraceable bitcoin – with some ransomware makers offering tech support to those unsure of how to buy or transfer bitcoin. Customer service is important; people need to know they'll get their files back once they pay.

And they want you to pay. If they're lucky, they've encrypted your irreplaceable family photos, or the documents of a project you've been working on for weeks. Or maybe your company's accounts receivable files or your hospital's patient records. The more you need what they've stolen, the better.

The particular ransomware making headlines is called WannaCry, and it's infected some pretty serious organizations.

Case study: Garmin ransomware attack

GPS maker Garmin suffered a devastating attack in July 2020 that disrupted services.

- Garmin's four-day service meltdown was caused by ransomware
- A cyberattack on Garmin disrupted more than workouts
- Garmin confirms ransomware attack took down services
- Garmin begins recovery from ransomware attack
- The Garmin ransomware hack is horrifying
- Experts: Devastating ransomware attack on Garmin highlights danger of haphazard breach responses

Garmin was aware of the problem. In an annual report submitted to the SEC in December 2019, Garmin officials noted just how damaging a cyberattack would be to its services, reputation, and more.

How to Deal With Ransomware

A recent in-depth article on the extent of ransomware attacks and some suggestions for how to deal with them.

The Steps CIOs Must Take To Deal With Ransomware Attacks Like The One That Hit Garmin, Mark Weatherford, former CISO and Deputy Undersecretary for Cybersecurity at DHS.