CPSC 467: Cryptography and Computer Security

Michael J. Fischer

Lecture 1
August 30, 2017

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

Highlights from Syllabus

Data Breaches

Defending Against Attacks

Highlights from Syllabus

Expectations

Read the syllabus! Some highlights:

- Pay attention to policies on plagiarism, submitting your work, and electronics in class.
- Teaching assistant is Senia Sheydvasser.
- The midterm and final exam are both scheduled. Keep those dates clear.
- You will use the Zoo for programming and Canvas for homework submissions.
- Do problem set 1!

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 an empty room.
- 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.

Electronics during class

You may use laptops, smart phones, and other electronic devices *for purposes related to the lecture only*.

Permitted:

- Taking notes.
- Looking briefly at lecture-related materials on the web.

Not permitted:

- Reading email.
- Visiting Facebook, Twitter, and other social media sites.
- Texting/messaging your friends.

If you must answer a call or engage in a not-permitted activity, please step out of the room so as to not disrupt class.

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.

Credit card numbers stolen

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

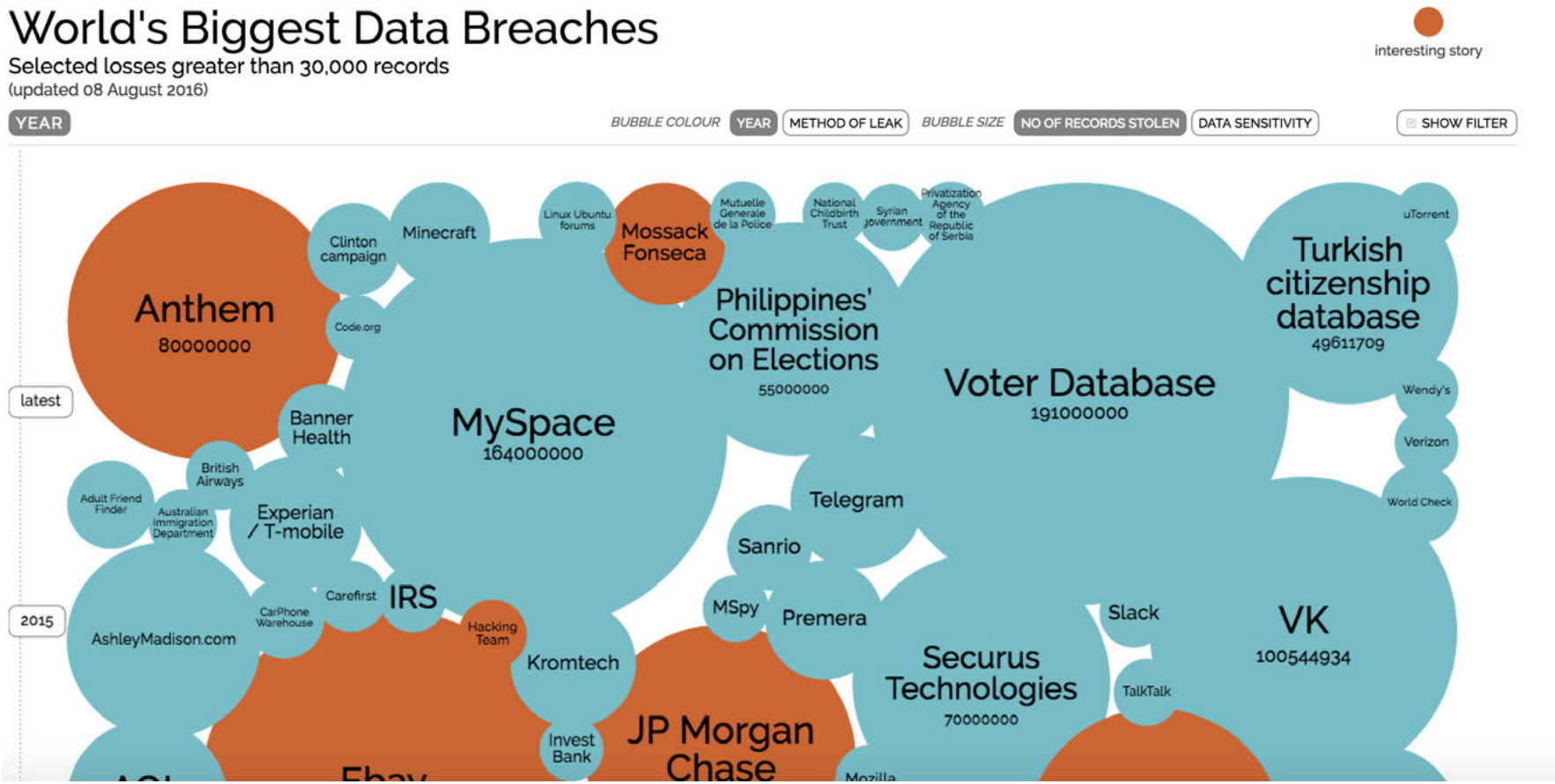
The Little Black Book of Billionaire S

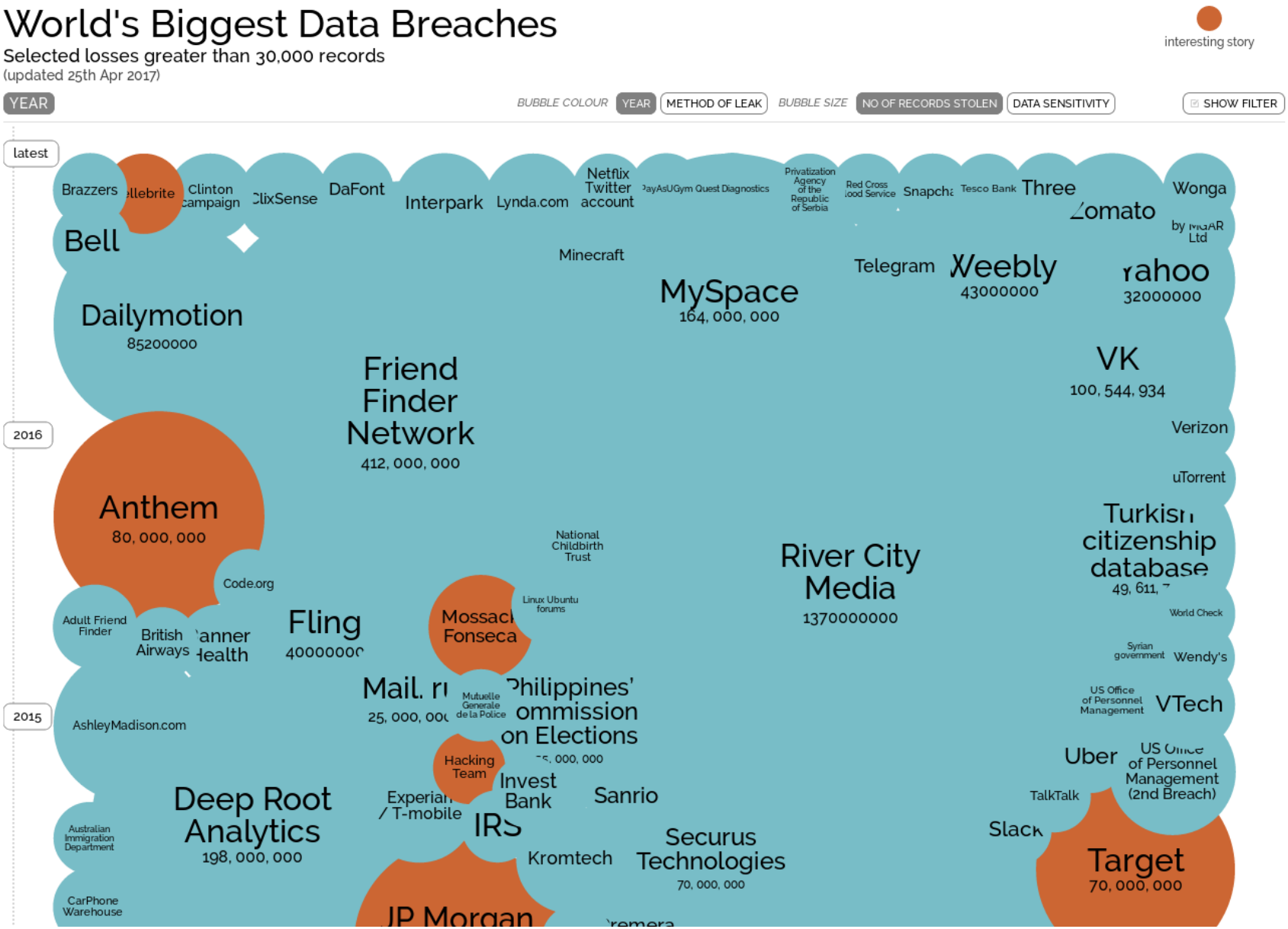
Target Data Breach Spilled Info On As Many As 70 Million Customers

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


World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 08 August 2016)
interesting story
YEAR
BUBBLE COLOUR
YEAR
METHOD OF LEAK
BUBBLE SIZE
NO OF RECORDS STOLEN
DATA SENSITIVITY
SHOW FILTER
latest
2015
Anthem
80000000
Clinton campaign
Minecraft
Code.org
Linux Ubuntu forums
Mossack Fonseca
Mutuelle Generale de la Police
National Childbirth Trust
Syrian government
Privatization Agency of the Republic of Serbia
Philippines' Commission on Elections
55000000
MySpace
164000000
Banner Health
British Airways
Adult Friend Finder
Australian Immigration Department
Experian / T-mobile
Voter Database
191000000
Turkish citizenship database
49611709
uTorrent
Wendy's
Verizon
World Check
Telegram
Sanrio
MSpy
Premera
Carefirst
IRS
CarPhone Warehouse
AshleyMadison.com
Hacking Team
Kromtech
Invest Bank
JP Morgan Chase
Securus Technologies
70000000
Slack
TalkTalk
VK
100544934
Mozilla


World's Biggest Data Breaches
Selected losses greater than 30,000 records
(updated 25th Apr 2017)
interesting story
YEAR
BUBBLE COLOUR
YEAR
METHOD OF LEAK
BUBBLE SIZE
NO OF RECORDS STOLEN
DATA SENSITIVITY
SHOW FILTER
latest
2016
2015
Brazzers
Clinton campaign
ClixSense
DaFont
Interpark
Lynda.com
Netflix Twitter account
Privatization Agency of the Republic of Serbia
Red Cross
Snapch
Tesco Bank
Three
Wonga
Bell
Minecraft
Telegram
Weebly
43000000
MySpace
164, 000, 000
32000000
Dailymotion
85200000
Friend Finder Network
412, 000, 000
VK
100, 544, 934
Verizon
uTorrent
Anthem
80, 000, 000
National Childbirth Trust
River City Media
1370000000
Code.org
Adult Friend Finder
British Airways
Fling
40000000
Linux Ubuntu forums
World Check
Syrian government
Wendy's
US Office of Personnel Management
VTech
AshleyMadison.com
Mutuelle Generale de la Police
Hacking Team
Uber
US Office of Personnel Management (2nd Breach)
TalkTalk
Deep Root Analytics
198, 000, 000
Invest Bank
Sanrio
IRS
Kromtech
Securus Technologies
70, 000, 000
Target
70, 000, 000
Australian Immigration Department
CarPhone Warehouse

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

Cyberwarfare

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

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. 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

"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."

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.

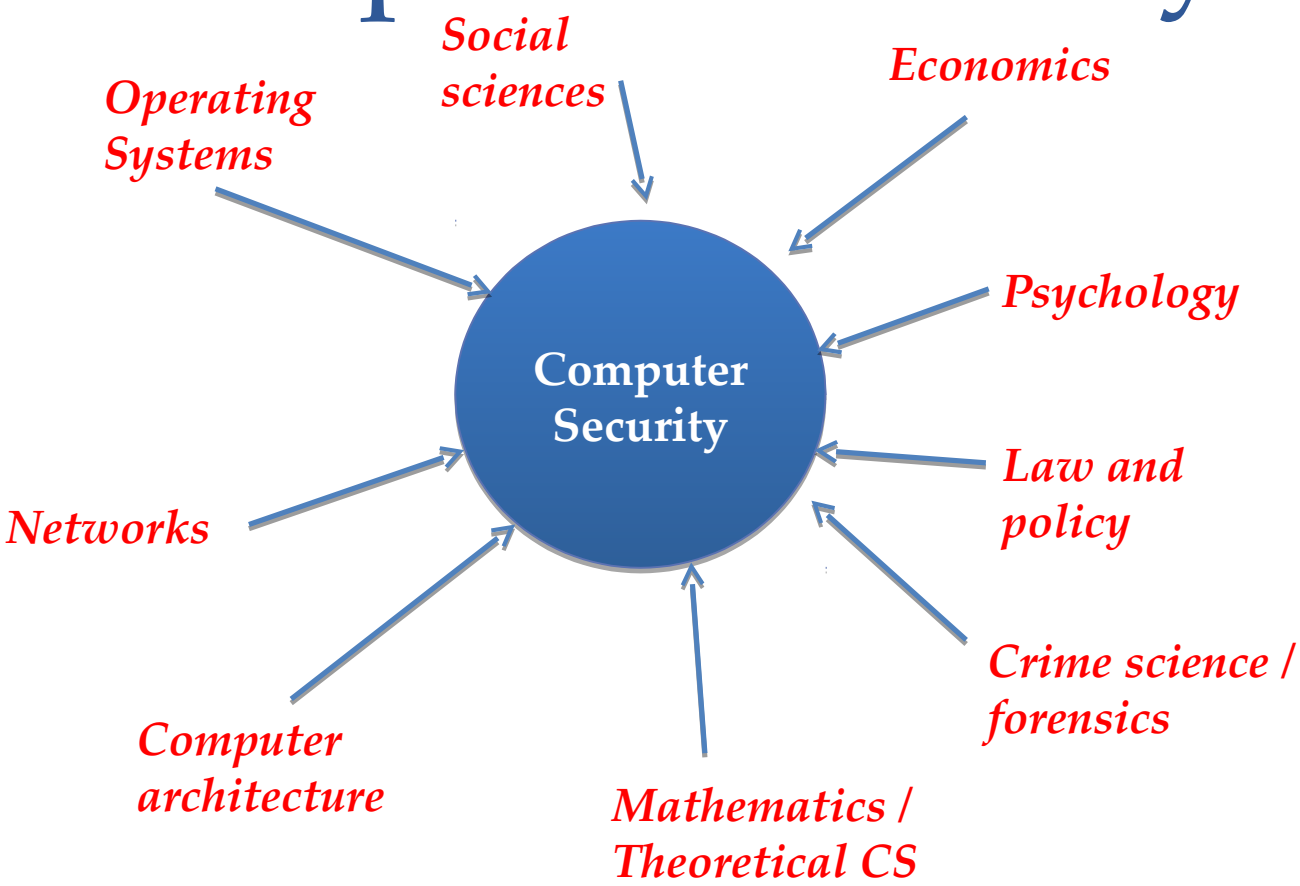
And they want you to pay. If they're lucky, they've encrypted your irreplaceable family photos, or the documents of a project you've been working on for weeks. Or maybe your company's accounts receivable files or your hospital's patient records. The more you need what they've stolen, the better.

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

Defending Against Attacks

The Digital Landscape

Computer Security



How is security achieved in the real world?

- **Prevention:** Physical barriers, access controls, encryption, firewalls, human awareness, etc.
- **Detection:** Audits, checks and balances.
- **Legal means:** Laws, patents, trademarks, copyrights, sanctions against wrongdoers.
- **Concealment:** Camouflage, steganography.

Different stakeholders have differing interests

Consider an on-line banking web site.

- What are the interests of the customer?
- What are the interests of the bank?
- What are the interests of possible intruders?
- Can the bank trust the customer? Why or why not?
- Can the customer trust the bank? Why or why not?