ÉCOLE POLYTECHNIQUE
FÉDÉRALE DE LAUSANNE

COM-402
Information Security and Privacy

Course Introduction and Basic Concepts

(slide credits: Linus Gasser, Ceyhun Alp, Sandra Siby, Cristina Basescu, Bryan Ford)

Lecture 1: Course introduction

- **Course logistics**
  - Course web sites and tools
  - Tentative schedule and topic outline
  - Programming exercises overview
- **Course overview**
  - How and what information is sensitive?
  - Threats: what can go wrong?
  - Data encryption and anonymization
  - User management (access control, authentication) & Operational security
  - Machine learning security and privacy
  - Blockchains and smart contracts
  - Many others

Important course sites and tools

- Moodle for COM-402
    - http://moodle.epfl.ch/course/view.php?id=15351
    - Announcements and discussion forum
    - Slides, exercises, solutions
    - Project descriptions
- SpeakUp
    - https://goo.gl/4T5OB7
    - Questions/comments during class
- Clicker
    - http://clickers.epfl.ch/students
    - Respond to poll-style questions during class
    - Only mobile apps

Moodle

Speak-up

Clicker

Tentative Course Syllabus

Date	Content	Date	Content
20.02	Course introduction and basic concepts	17.04	Security policy and regulation
27.02	Common threats	24.04	Anonymization and de-anonymization
06.03	Crypto basics	01.05	Machine learning security & privacy
13.03	Database security	08.05	Advanced privacy techniques
20.03	Personally identifying information (PII)	15.05	Blockchains & smart contracts
27.03	User management	22.05	Side-channel attacks/defenses
10.04	Network security: detection / response	29.05	What’s hot in security research

Contact information

Lecture instructors:

- Bryan Ford - bryan.ford@epfl.ch - BC210
- Linus Gasser - linus.gasser@epfl.ch - BC208

Teaching assistants:

- Cristina Basescu - cristina.basescu@epfl.ch - BC263
- Kirill Nikitin - kirill.nikitin@epfl.ch - BC209
- Sandra Siby - sandra.siby@epfl.ch - INR015
- Ceyhun Alp - enis.alp@epfl.ch - INR012
- Raphaël Dunant - raphael.dunant@epfl.ch

Exercises and grading

- Weekly workload
  - Lectures: 2h - Tuesdays 4:15pm in CM1
  - Exercises: 2h - Fridays 3:15pm in CM3
  - Homework: 5-10h / week
- Grading structure:
  - Exercises: approx 40% of grade, lowest-scoring homework dropped
  - Final exam: approx 60% of grade

Programming Exercises Overview

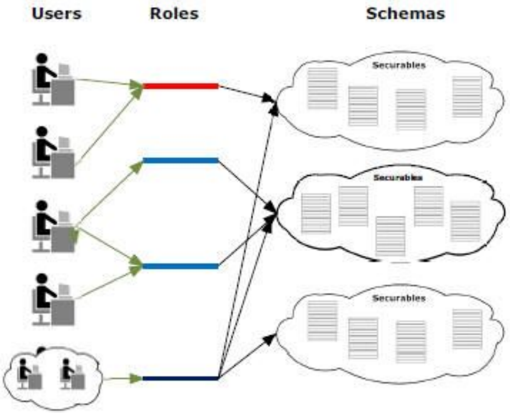
- **Six exercise sets over the semester (approx every 2 weeks)**
- **Friday group exercise sessions (3:15pm-5pm CM3)**
  - Introduce tools to be used in assignments (e.g., Docker, WireShark, etc.)
  - Introduce programming assignments
  - Practice, walk through example problems in group context
  - Answer questions and help with use of tools
- **Main problem-solving and programming to be done “on your own”**
  - For each assignment we will provide a Docker container to start with
  - You will need to install and run on your preferred laptop/desktop
    - You will use programming tools provided in container (Python, JavaScript, SQL)
    - You can use native host editors, IDEs, etc., via Docker shared directories
  - Many problems require you to obtain a token for an all-or-nothing grade for that problem

Programming Exercise Outline

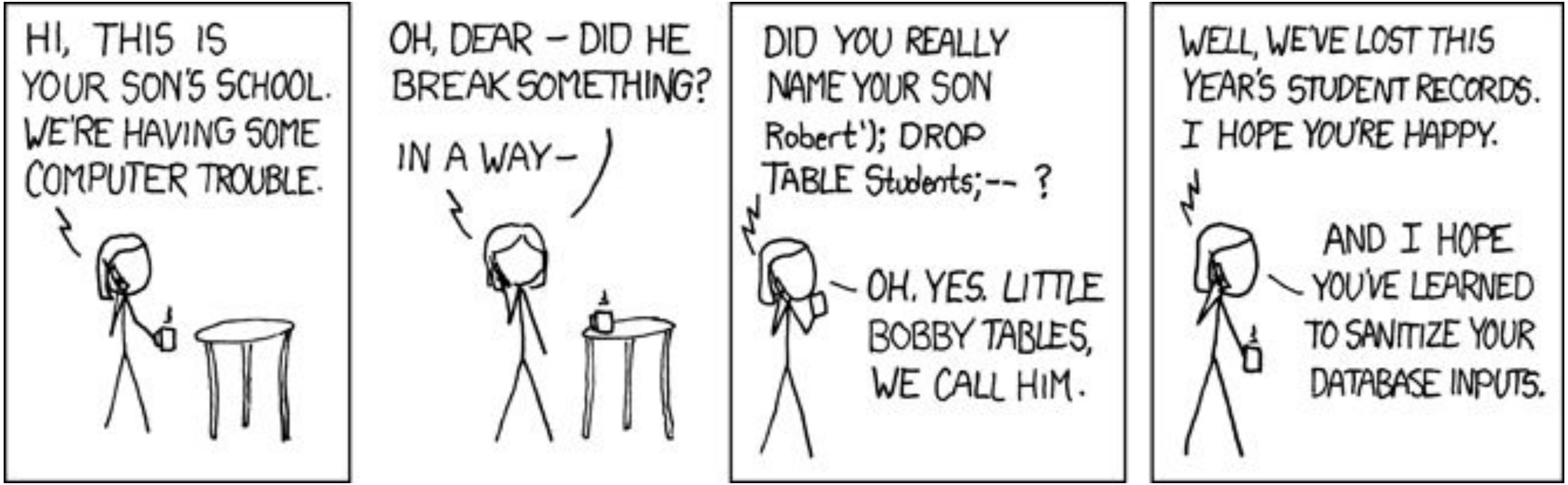
Set	Type	Topics
1	Attack	Hacking 101: sniffing networks; exploiting bugs and humans
2	Defense	Basic encryption and security-hardening practices
3	Attack	Database-centric attacks: SQL injection, credential databases
4	Defense	Better database hardening, naive anonymization
5	Attack	De-anonymization via correlation (e.g., “Netflix attack”)
6	Defense	Differential privacy and anti-correlation techniques

Attack/defense hw1&2 - Data access security

What fun data can a malicious network operator or cyber-cafe lurker get unauthorized access to?



Attack/defense hw3&4 - database security


HI, THIS IS YOUR SON'S SCHOOL. WE'RE HAVING SOME COMPUTER TROUBLE.
OH, DEAR – DID HE BREAK SOMETHING?
IN A WAY–
DID YOU REALLY NAME YOUR SON Robert'); DROP TABLE Students;-- ?
OH. YES. LITTLE BOBBY TABLES, WE CALL HIM.
WELL, WE'VE LOST THIS YEAR'S STUDENT RECORDS. I HOPE YOU'RE HAPPY.
AND I HOPE YOU'VE LEARNED TO SANITIZE YOUR DATABASE INPUTS.

https://xkcd.com/327/

Attack/defense hw5&6 - Data privacy, anonymization

DOGBERT CONSULTS
CUSTOMER DATA IS AN ASSET THAT YOU CAN SELL.
DilbertCartoonist@gmail.com
Dilbert.com
IT'S TOTALLY ETHICAL BECAUSE OUR CUSTOMERS WOULD DO THE SAME THING TO US IF THEY COULD.
10-13-10 © 2010 Scott Adams, Inc./Dist. by UFS, Inc.
SOUNDS FAIR.
IN PHASE ONE, WE'LL DEHUMANIZE THE ENEMY BY CALLING THEM "DATA."

Lecture 1: Course introduction

- **Course logistics**
  - Course web sites and tools
  - Tentative schedule and topic outline
  - Programming exercises overview
- **Course overview**
  - How and what information is sensitive?
  - Threats: what can go wrong?
  - Data encryption and anonymization
  - User management (access control, authentication) & Operational security
  - Machine learning security and privacy
  - Blockchains and smart contracts
  - Many others

Information Sensitivity

Many types of information -> many kinds and levels of *sensitivity*

- What might happen, and how bad, if “the wrong person” gets information?

Example: photos inside home “more sensitive” than photos taken in public park

- But what if taken with long-distance telephoto aimed at bedroom window?

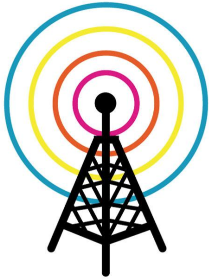
Sensitivity can depend on Context

Information sensitivity often depends on context

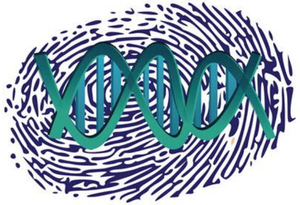
- You may be perfectly comfortable with your friends seeing party photos…
- But may be harmful if seen by future employer (or border control)...

Forget the resume, son. Let's just take a look at what you have posted on your facebook instead.

Sensitivity can depend on Longevity



- Ephemeral, rapidly-changing, automatically-collected data
  - Mobile cell tower logs, security cameras, website visit logs, …
  - Each data point typically not very sensitive by itself,
    but more sensitive in aggregate (user profiling) and/or at particular times (clinic visit)
- Information actively provided by users
  - E-mail, phone calls, chat logs, social media comments, online purchases & reviews
  - Sensitivity in principle governed by awareness & consent … but many surprises lurking
- Slowly-changing or difficult-to-change information
  - Social security number, AHV-number, passport-number
  - Sensitive in part because difficult to recover when breached

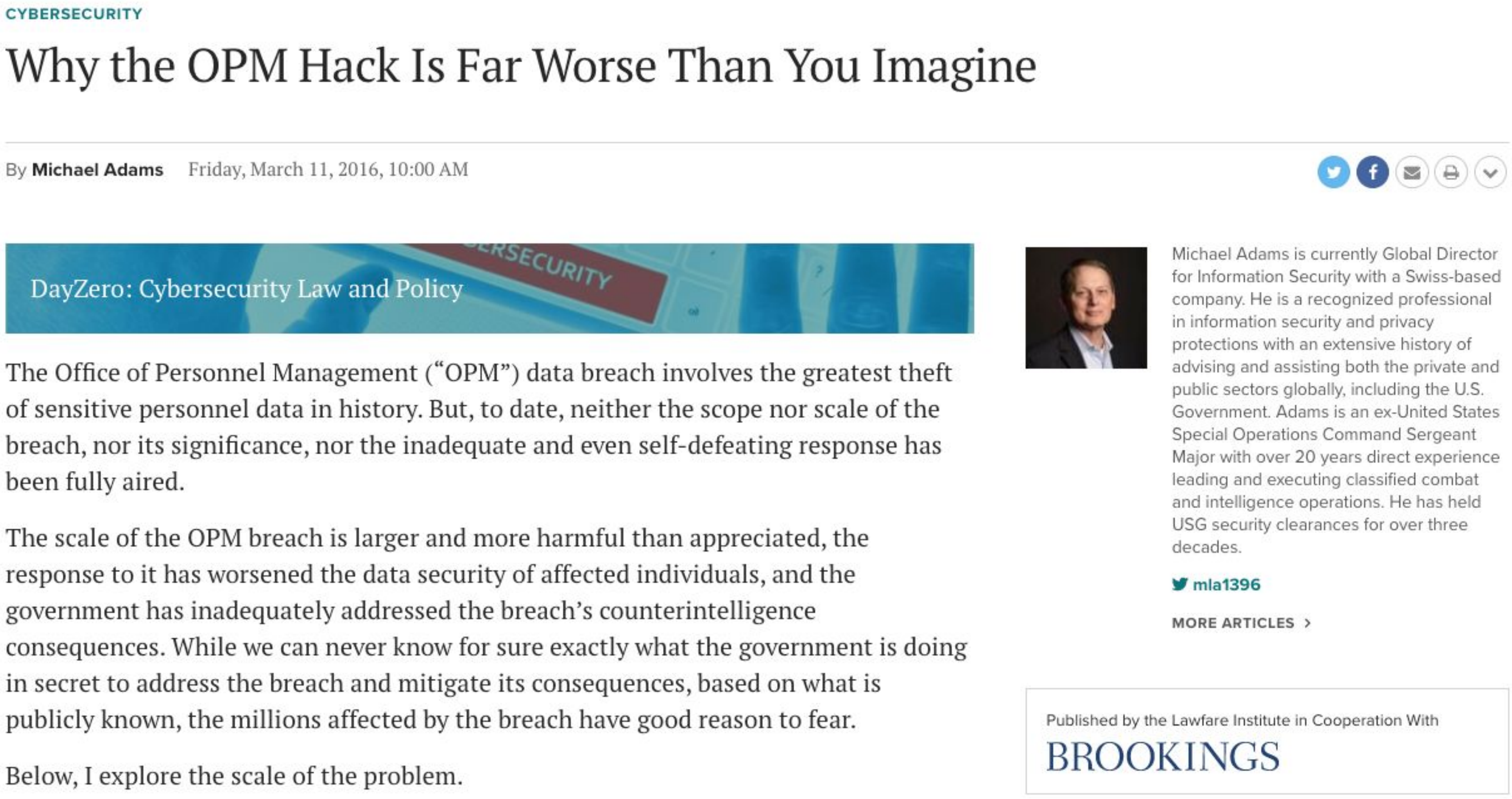


- Practically unchangeable information, e.g., biometrics
  - Fingerprints, DNA, ‘Omics and other medical data
  - Can’t change your DNA if breached, *and* can also breach privacy of your relatives...

Lecture 2: Common Threats

Examples of things that can go wrong (and have)

- Data breaches: when hackers get in and grab sensitive data
  - US Office of Personnel Management (OPM): 21.5 million security clearance records
  - Swiss RUAG: long-term, well-maintained malware infection over several years
- De-anonymization: when “anonymized” datasets are sensitive after all
  - Netflix Prize dataset: de-anonymized by correlating with IMDB film reviews
- Ransomware: pay to decrypt your own data
  - 10+ US hospitals infected in 2016, one paid $17,000
- Phishing: acquire credentials to break into business, personal accounts
  - Identity theft, or stepping-stone into employee’s organization



CYBERSECURITY

Why the OPM Hack Is Far Worse Than You Imagine

By **Michael Adams** Friday, March 11, 2016, 10:00 AM

The Office of Personnel Management ("OPM") data breach involves the greatest theft of sensitive personnel data in history. But, to date, neither the scope nor scale of the breach, nor its significance, nor the inadequate and even self-defeating response has been fully aired.

The scale of the OPM breach is larger and more harmful than appreciated, the response to it has worsened the data security of affected individuals, and the government has inadequately addressed the breach's counterintelligence consequences. While we can never know for sure exactly what the government is doing in secret to address the breach and mitigate its consequences, based on what is publicly known, the millions affected by the breach have good reason to fear.

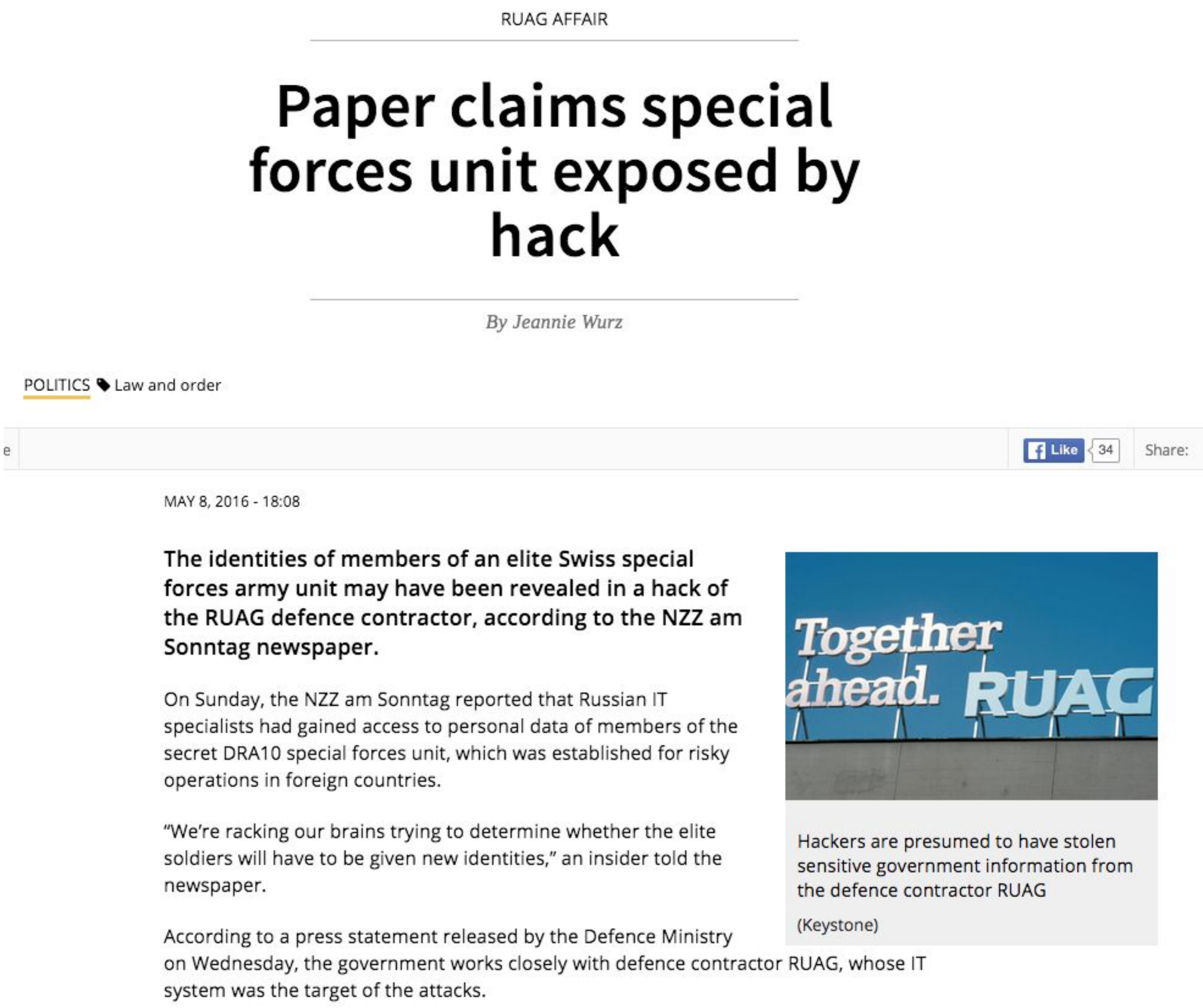
Below, I explore the scale of the problem.

Michael Adams is currently Global Director for Information Security with a Swiss-based company. He is a recognized professional in information security and privacy protections with an extensive history of advising and assisting both the private and public sectors globally, including the U.S. Government. Adams is an ex-United States Special Operations Command Sergeant Major with over 20 years direct experience leading and executing classified combat and intelligence operations. He has held USG security clearances for over three decades.

mla1396

MORE ARTICLES ›

Published by the Lawfare Institute in Cooperation With
BROOKINGS



RUAG AFFAIR

Paper claims special forces unit exposed by hack

By Jeannie Wurz

POLITICS Law and order

Like 34 Share:

MAY 8, 2016 - 18:08

The identities of members of an elite Swiss special forces army unit may have been revealed in a hack of the RUAG defence contractor, according to the NZZ am Sonntag newspaper.

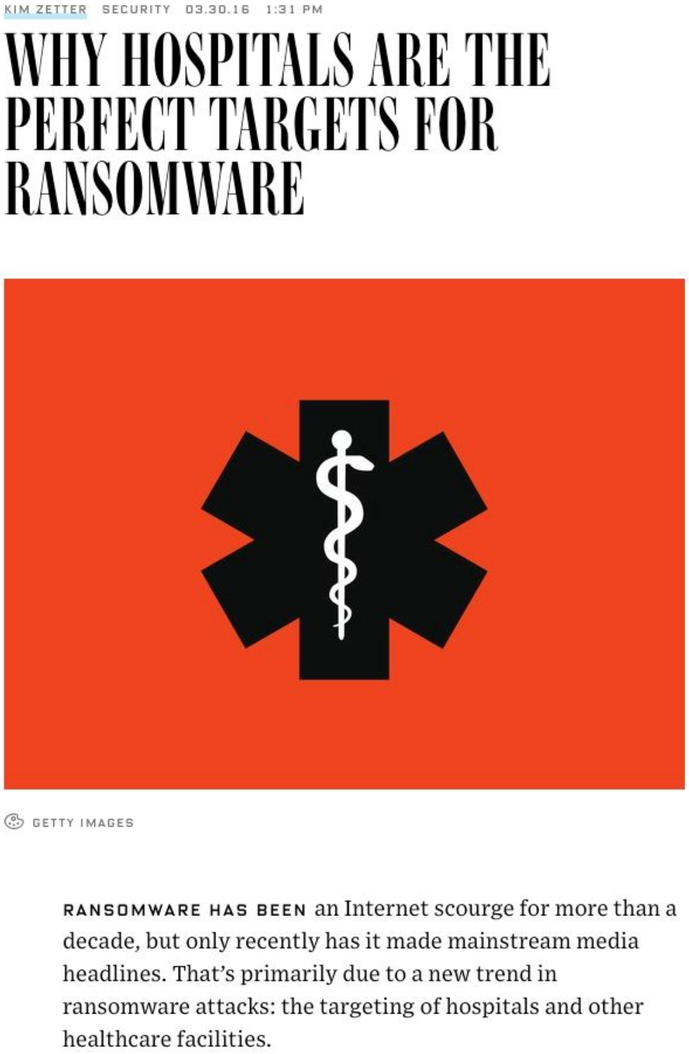
Hackers are presumed to have stolen sensitive government information from the defence contractor RUAG

(Keystone)

On Sunday, the NZZ am Sonntag reported that Russian IT specialists had gained access to personal data of members of the secret DRA10 special forces unit, which was established for risky operations in foreign countries.

"We're racking our brains trying to determine whether the elite soldiers will have to be given new identities," an insider told the newspaper.

According to a press statement released by the Defence Ministry on Wednesday, the government works closely with defence contractor RUAG, whose IT system was the target of the attacks.



KIM ZETTER SECURITY 03.30.16 1:31 PM

WHY HOSPITALS ARE THE PERFECT TARGETS FOR RANSOMWARE

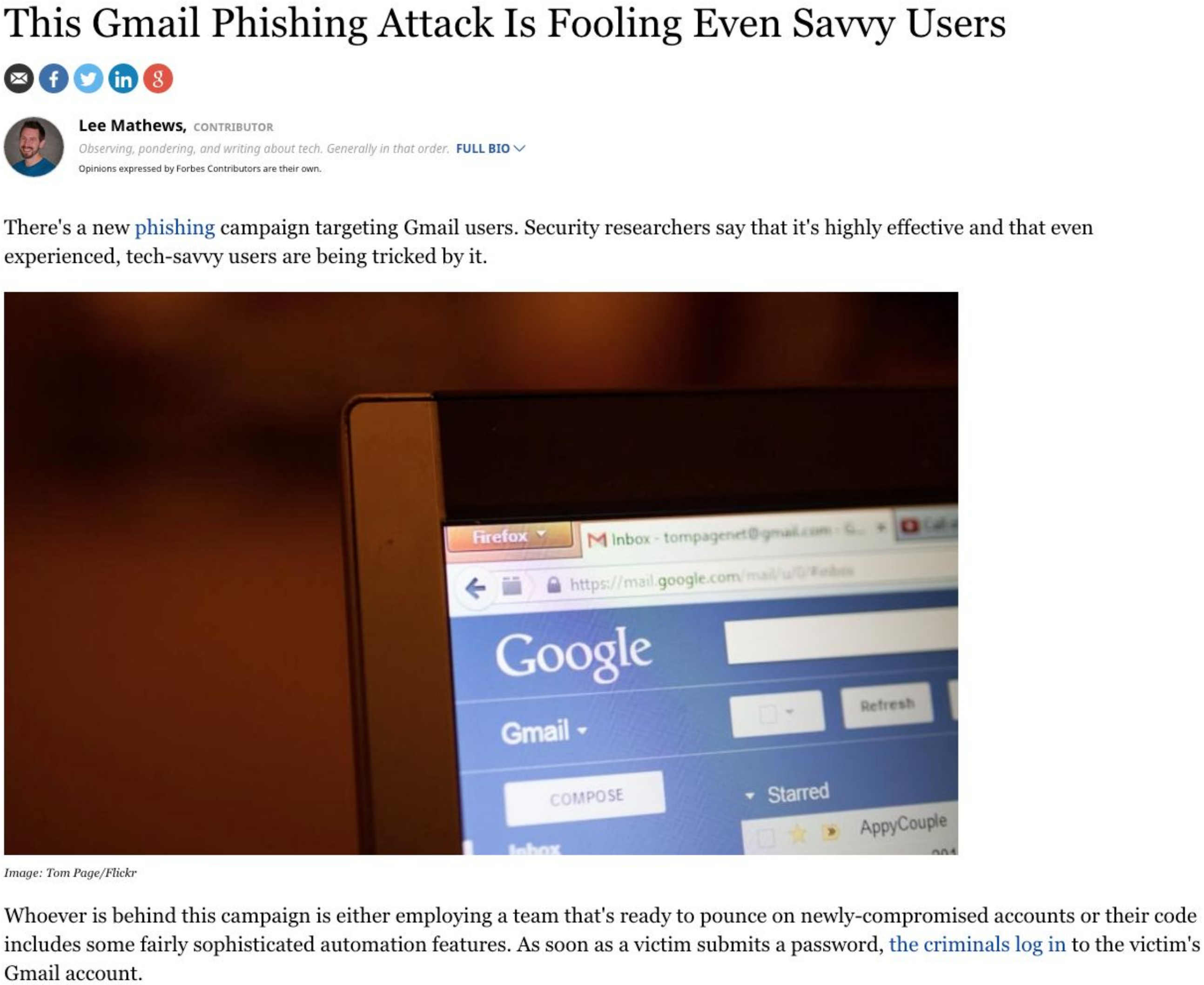
GETTY IMAGES

RANSOMWARE HAS BEEN an Internet scourge for more than a decade, but only recently has it made mainstream media headlines. That's primarily due to a new trend in ransomware attacks: the targeting of hospitals and other healthcare facilities.

Who all might present a “threat”?

Many threat models, often with different levels of budget & capability

- Random people: friends, partners, journalists, competitors, trolls
    - Attack: domestic spying, “spouseware”
- Crooks: theft, ransom, blackmail
    - Attack: E-mail phishing
    - Attack: Microsoft chatbot Tay
    - Attack: The DAO
- State agencies: law enforcement, espionage, tax office
    - Attack: Stuxnet
    - Attack: Apple-FBI



This Gmail Phishing Attack Is Fooling Even Savvy Users

Lee Mathews, CONTRIBUTOR
Observing, pondering, and writing about tech. Generally in that order. **FULL BIO**
Opinions expressed by Forbes Contributors are their own.

There's a new phishing campaign targeting Gmail users. Security researchers say that it's highly effective and that even experienced, tech-savvy users are being tricked by it.

Firefox
Inbox - tompagenet@gmail.com
https://mail.google.com/mail/u/0/#inbox
Google
Gmail
Refresh
COMPOSE
Starred
AppyCouple
Inbox

Image: Tom Page/Flickr

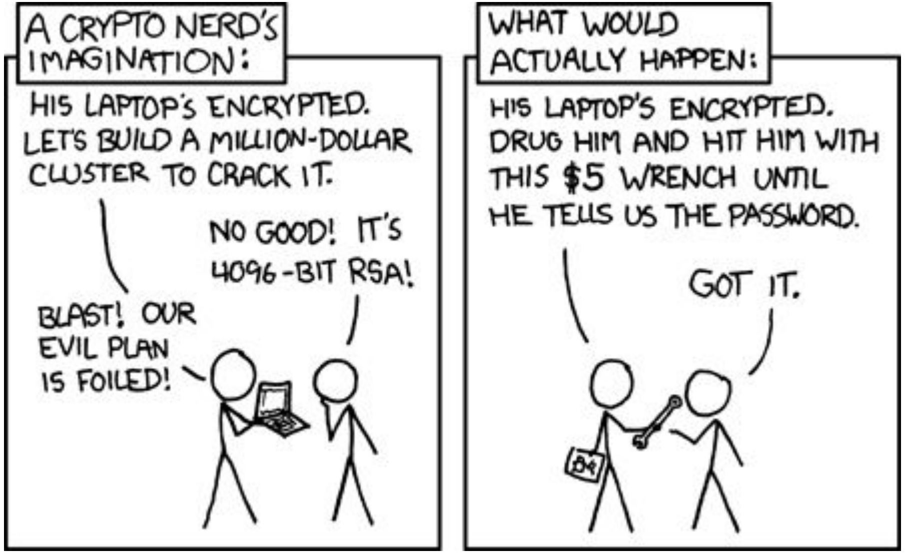
Whoever is behind this campaign is either employing a team that's ready to pounce on newly-compromised accounts or their code includes some fairly sophisticated automation features. As soon as a victim submits a password, the criminals log in to the victim's Gmail account.

Lecture 3: Cryptography Basics

- Cryptography is an essential toolbox for many security mechanisms
  - Secure communication (e.g., HTTPS, SSH, GSM)
  - File & disk encryption (e.g., VeraCrypt, GPG)

- Goals
  - Confidentiality
  - Integrity
  - Authentication

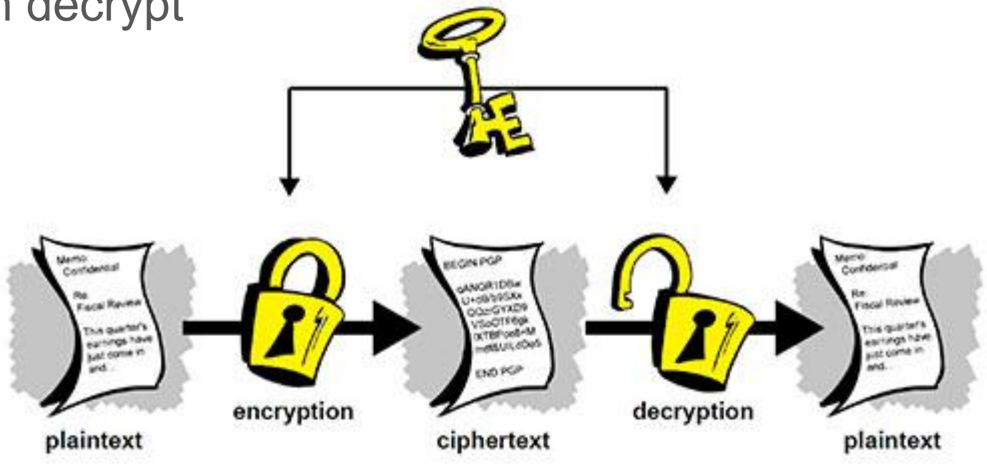
- Achieve these goals using various tools
  - Symmetric (private-key) encryption
  - Asymmetric (public-key) encryption
  - Cryptographic hash functions
  - Public key infrastructure (PKI)


A CRYPTO NERD'S IMAGINATION:
HIS LAPTOP'S ENCRYPTED. LET'S BUILD A MILLION-DOLLAR CLUSTER TO CRACK IT.
NO GOOD! IT'S 4096-BIT RSA!
BLAST! OUR EVIL PLAN IS FOILED!
WHAT WOULD ACTUALLY HAPPEN:
HIS LAPTOP'S ENCRYPTED. DRUG HIM AND HIT HIM WITH THIS $5 WRENCH UNTIL HE TELLS US THE PASSWORD.
GOT IT.

Encryption: Making Data Unintelligible

Keep information private while stored or communicated via non-private channels

- Modern encryption relies on *keys*
- Even with full knowledge of *algorithm,* only holder of correct *key* can decrypt



Encryption At Rest

Encrypted hard disk partitions, databases, folders

- Protect from some attacks: e.g., stolen laptop or phone
  - Provided device was turned off or locked when stolen
  - Provided password isn't easily guessable, encryption software not readily crackable, …
- Who holds the encryption keys?
  - User device? If device is stolen, thief can use it to break into a lot more
  - Central database? If server breached, hacker can get into *many* users' accounts
- What if a key is lost/misplaced/forgotten?
  - With "strong" encryption, losing a key means there is no way to recover data
  - If there is a "legit" way to recover a key, an attacker or spy might do the same
- What happens when sending the data to another server?

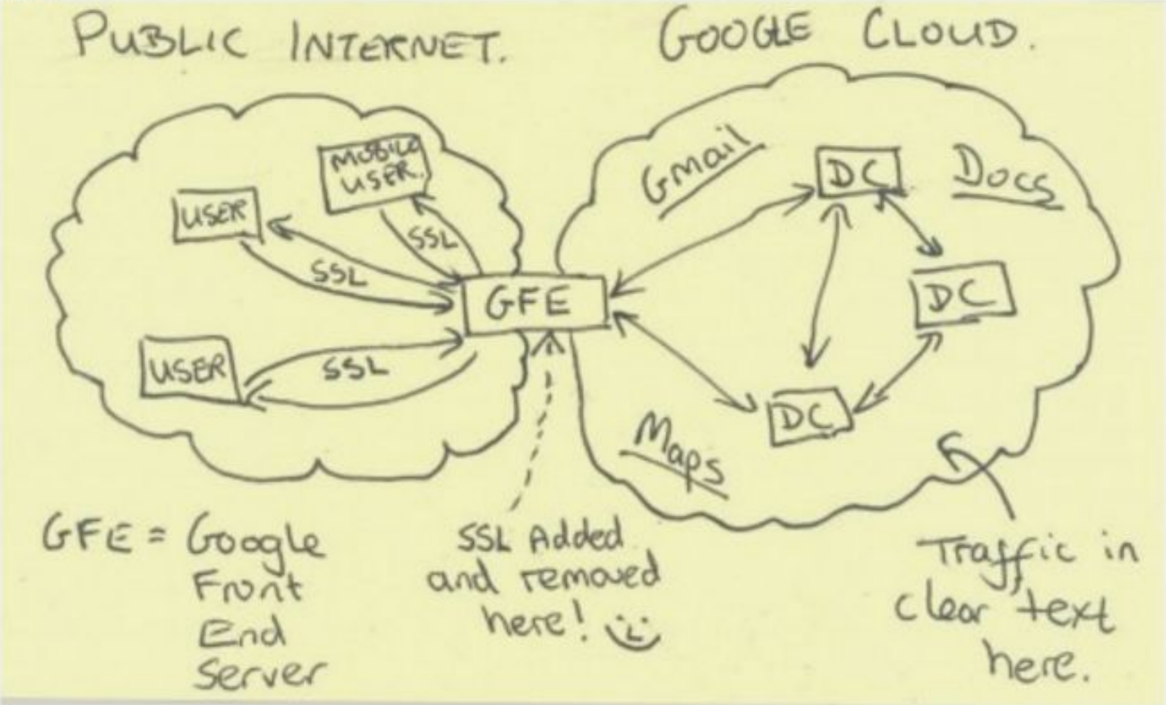
Encryption in Transit

How to get data securely between user and server, between company sites?

- Between data warehouses
  - NSA-attack on Google
- Between user and web sites, E-mail servers, etc.
  - HTTP - TLS
  - SMTP - TLS
- Between users: encrypted E-mail, encrypted chat
  - Skype - not sure what the protection is - probably opened to government inquiries
  - WhatsApp - relies on secure protocol, but has some user-friendly downgrades
  - Signal - open source, highly security-conscious, but still known weaknesses

TOP SECRET//SI//NOFORN

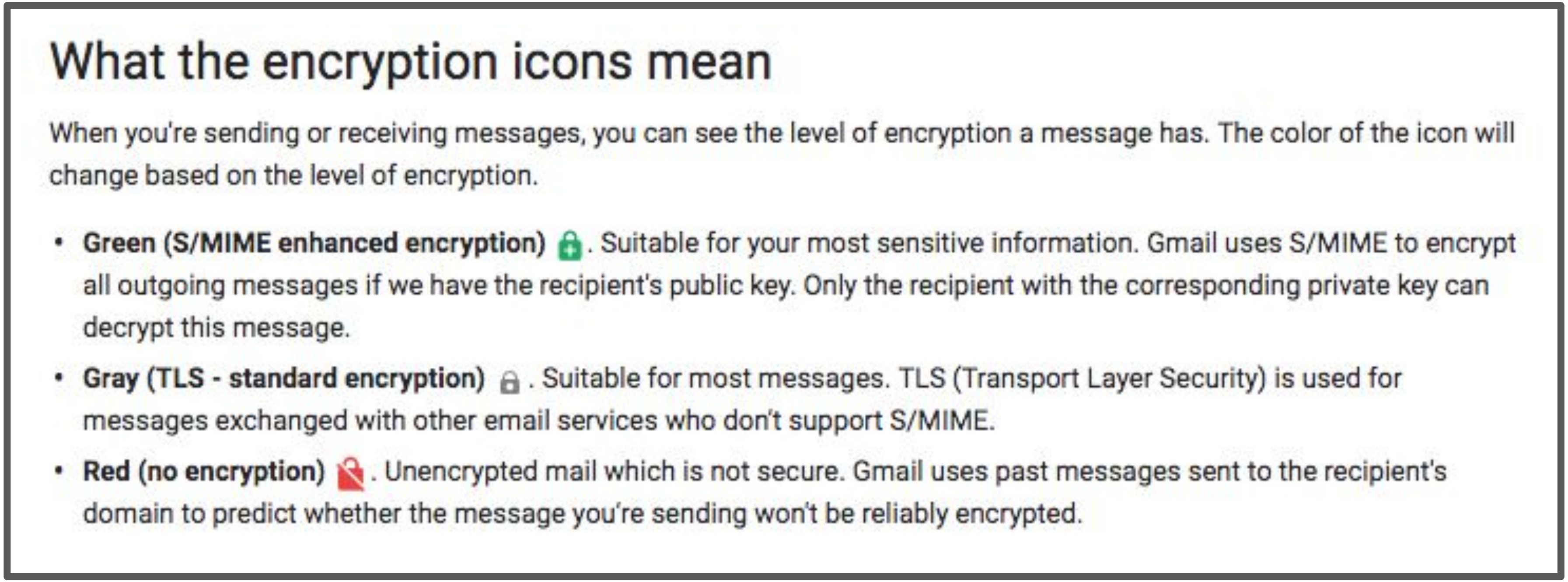
Current Efforts - Google


PUBLIC INTERNET.
GOOGLE CLOUD.
MOBILE USER.
USER
USER
SSL
SSL
SSL
GFE
Gmail
DC
Docs
DC
DC
Maps
GFE = Google Front End Server
SSL Added and removed here! :-)
Traffic in clear text here.

TOP SECRET//SI//NOFORN

The Challenges of “Usable Encryption”

Will typical users really understand…



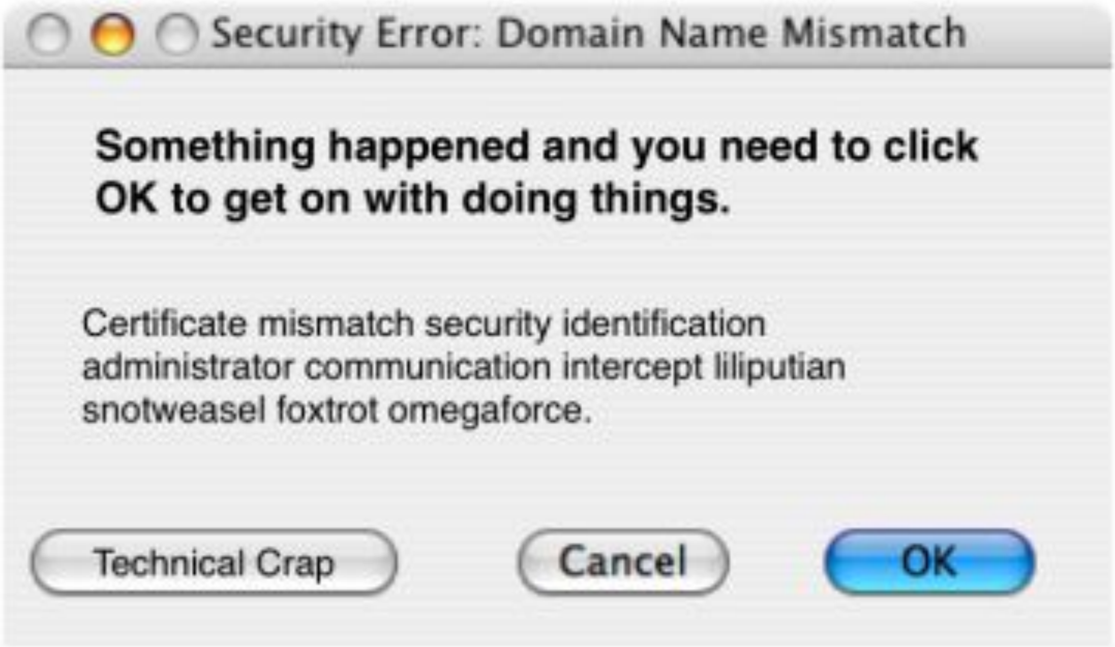
What the encryption icons mean

When you're sending or receiving messages, you can see the level of encryption a message has. The color of the icon will change based on the level of encryption.

- **Green (S/MIME enhanced encryption)** 🔒. Suitable for your most sensitive information. Gmail uses S/MIME to encrypt all outgoing messages if we have the recipient's public key. Only the recipient with the corresponding private key can decrypt this message.
- **Gray (TLS - standard encryption)** 🔒 . Suitable for most messages. TLS (Transport Layer Security) is used for messages exchanged with other email services who don't support S/MIME.
- **Red (no encryption)** 🔒 . Unencrypted mail which is not secure. Gmail uses past messages sent to the recipient's domain to predict whether the message you're sending won't be reliably encrypted.

The Challenges of “Usable Encryption”

...let alone what it means and what to do if something goes wrong?



Security Error: Domain Name Mismatch

Something happened and you need to click OK to get on with doing things.

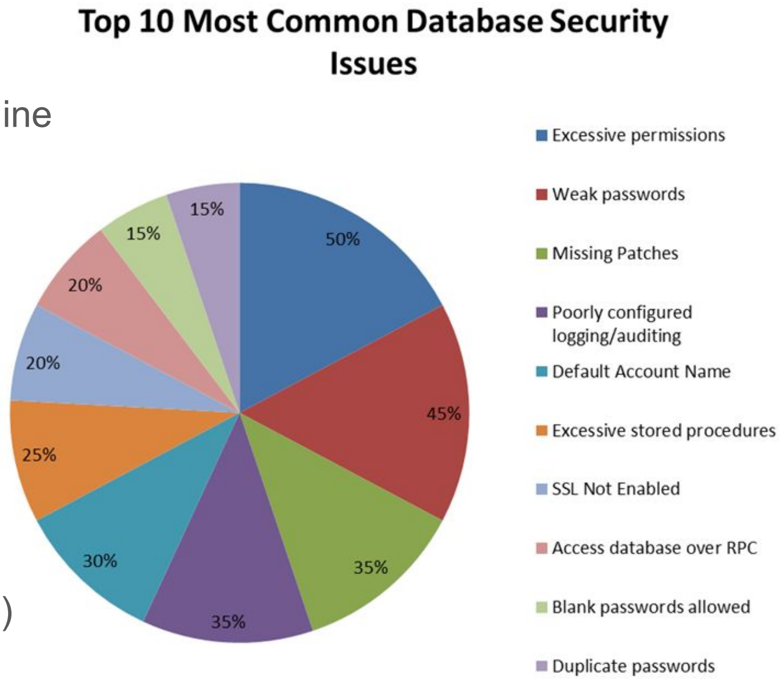
Certificate mismatch security identification administrator communication intercept liliputian snotweasel foxtrot omegaforce.

Lecture 4: Database Security

- Databases are used everywhere
  - Banking, industry, government, social media, etc.
  - Leads to new types of analysis (e.g., big data, machine learning)

- Critical to think about its security
  - Security requirements
  - Main attack vectors
  - Main protections

- Some issues:
  - Access control (authenticating users and their rights)
  - Input validation & SQL injections
  - Protection of the sensitive data (passwords, credit card info, medical records, etc.)



Lecture 5: Personally Identifiable Information

- What is personally identifiable information (PII)?
    - Both sensitive and nonsensitive information
    - Has value for third parties

- Nonsensitive data can become sensitive by combining different sources
    - Co-location and position information
    - De-anonymization of databases (e.g., Netflix deanonymization)

- Management concepts
    - How to collect the data and operate on it

- Legislation around the world

Lecture 6: User and Access Management

- Access control
  - Role-based access control
  - Discretionary access control
  - Mandatory access control

- Authentication
  - Passwords
  - Kerberos - network authentication protocol from MIT
  - Multi-factor authentication
    - One-time passwords
    - Biometrics
  - LDAP

- How to stay safe online?
  - Training the weakest link in the system (aka the users!)

Access Control

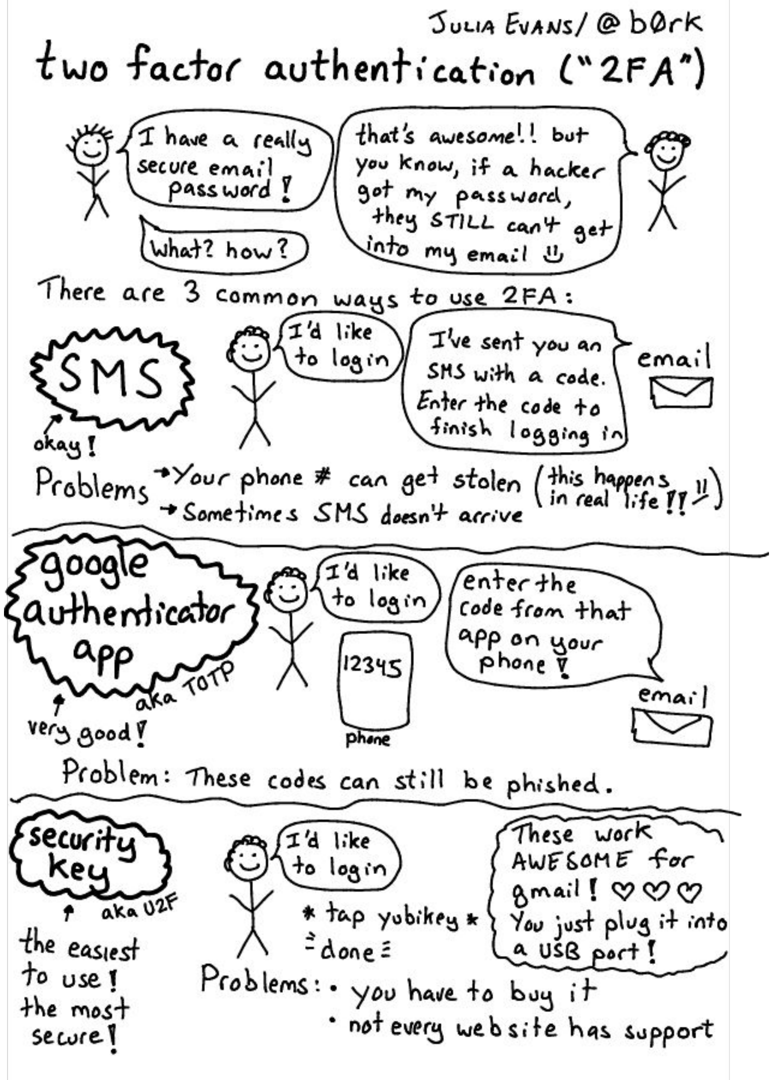
Access control is a mechanism defining who *should* have access to information

- Who?
  - Might be specified by individual: Alice, Bob, Charlie, Dave, …
  - Might be specified by group/role: Doctors, Board Members, Accounting, …
- What?
  - Access to one document, a whole folder/tree
  - Access to perform certain queries on a database
- How?
  - Authorization to read document? Edit document? Share access? Revoke access?
- When?
  - Is granted access indefinite, or does it end at a particular time (Dec 31)
    or at occurrence of a particular event (revocation, employment termination)?

Authentication of Users

How does Alice prove she’s Alice (e.g., to obtain access to information)?

- Simple username (e.g., IRC)
  - No security, anyone can be “Alice”
- Typical: username + password (most Web accounts)
  - Security relies completely on “something you know” (password)
- Two factor Authentication (2FA): username + password + token
  - Combination of “something you know” (password) plus “something you have” (token)
- Device-centric authentication
  - Web persistent login, SSH public key login, Kerberos file sharing


JULIA EVANS / @b0rk
two factor authentication ("2FA")
I have a really secure email password!
what? how?
that's awesome!! but you know, if a hacker got my password, they STILL can't get into my email!!
There are 3 common ways to use 2FA:
SMS
okay!
I'd like to login
I've sent you an SMS with a code. Enter the code to finish logging in
email
Problems → Your phone # can get stolen (this happens in real life!!!)
→ Sometimes SMS doesn't arrive
google authenticator app
aka TOTP
very good!
I'd like to login
12345
phone
enter the code from that app on your phone!
email
Problem: These codes can still be phished.
security key
aka U2F
the easiest to use! the most secure!
I'd like to login
* tap yubikey *
done
These work AWESOME for gmail! ♡♡♡ You just plug it into a USB port!
Problems: • you have to buy it
• not every website has support

Authentication of Remote Servers and Users

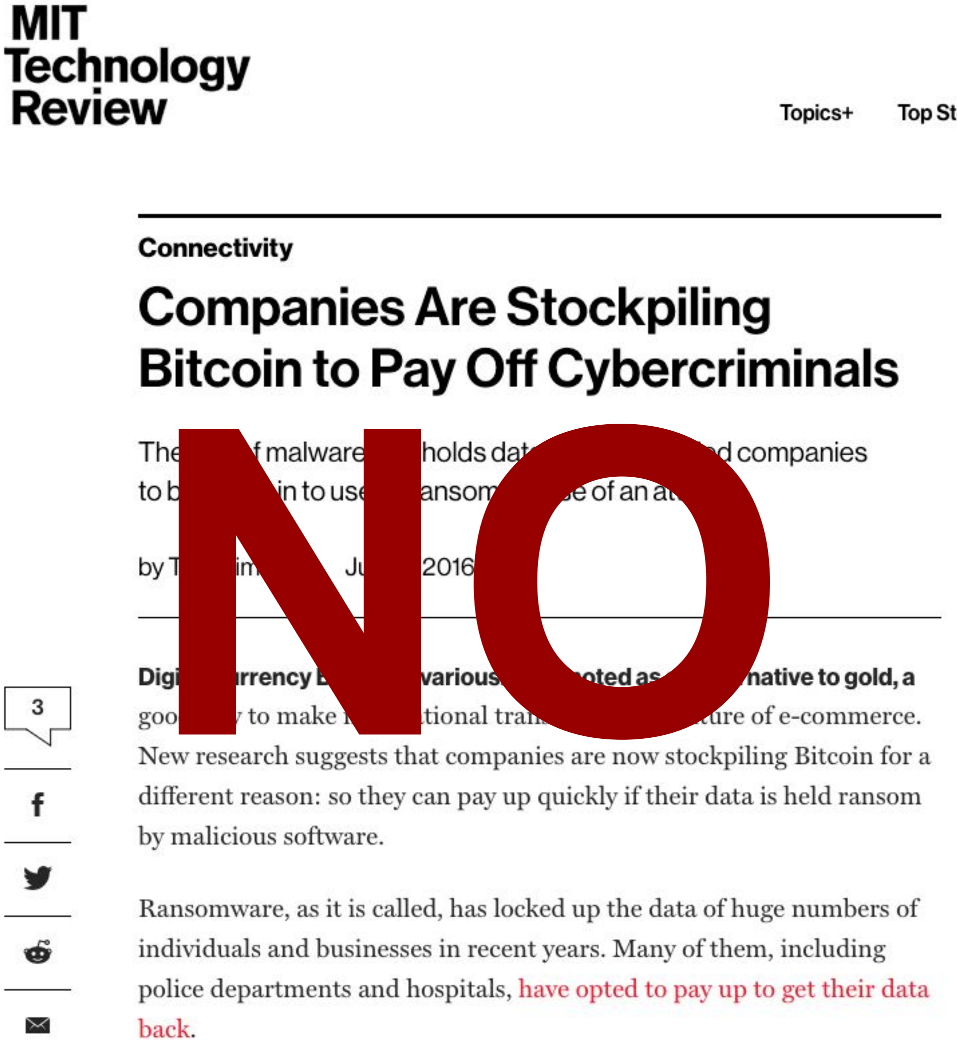
Authenticating *servers* is just as critical as authenticating *users*:
How does Alice know she's connecting to the *real* "**google.com**"?

- Many attacks (phishing) rely on tricking the user into trusting a *fake* version of an otherwise-uncompromised service
  - Alice enters her username+password; hacker captures and uses them
- Public Key Infrastructure (PKI) Certificates
  - Chain of Certificate Authorities (CAs) attest to correct ownership of "google.com"
- Peer-to-peer authentication: PGP keys, SSH fingerprints, Signal verification
  - Peer users supposed to verify in-person or out-of-band… (but how often do they?)

Lecture 7: Network and Operational Security Practices

Set of practices for identifying threats and minimizing risks of compromise

- Identify the risk
  - Know your network
  - Update the information regularly
  - Evaluate what information is valuable
- Minimize the risk
  - Compartmentalization (access control, separation of data)
  - Protection on network level
  - Backup
- Prepare response
  - Have a plan what to do
  - Save logs in case of an attack



MIT Technology Review

Topics+ Top Stories

Connectivity

Companies Are Stockpiling Bitcoin to Pay Off Cybercriminals

The f malware holds dat d companies to b in to use ansom e of an at

by T im Ju 2016

3

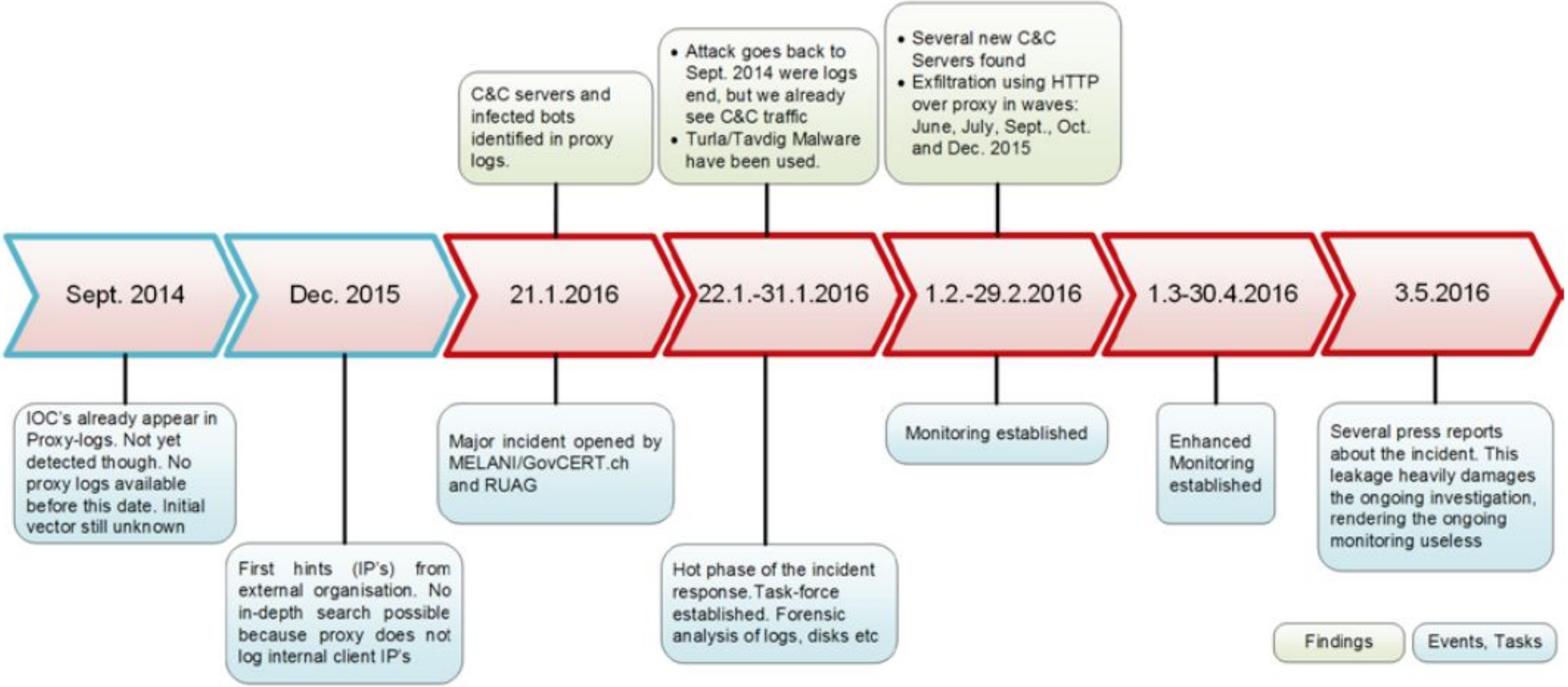
Digi rrency B various oted as native to gold, a goo y to make i tional tra ure of e-commerce. New research suggests that companies are now stockpiling Bitcoin for a different reason: so they can pay up quickly if their data is held ransom by malicious software.

Ransomware, as it is called, has locked up the data of huge numbers of individuals and businesses in recent years. Many of them, including police departments and hospitals, have opted to pay up to get their data back.

NO

ÉCOLE POLYTECHNIQUE FÉDÉRALE DE LAUSANNE

RUAG response - not prepared



Sept. 2014

IOC's already appear in Proxy-logs. Not yet detected though. No proxy logs available before this date. Initial vector still unknown

Dec. 2015

First hints (IP's) from external organisation. No in-depth search possible because proxy does not log internal client IP's

21.1.2016

C&C servers and infected bots identified in proxy logs.

Major incident opened by MELANI/GovCERT.ch and RUAG

22.1.-31.1.2016

- Attack goes back to Sept. 2014 were logs end, but we already see C&C traffic
- Turla/Tavdig Malware have been used.

Hot phase of the incident response. Task-force established. Forensic analysis of logs, disks etc

1.2.-29.2.2016

- Several new C&C Servers found
- Exfiltration using HTTP over proxy in waves: June, July, Sept., Oct. and Dec. 2015

Monitoring established

1.3-30.4.2016

Enhanced Monitoring established

3.5.2016

Several press reports about the incident. This leakage heavily damages the ongoing investigation, rendering the ongoing monitoring useless

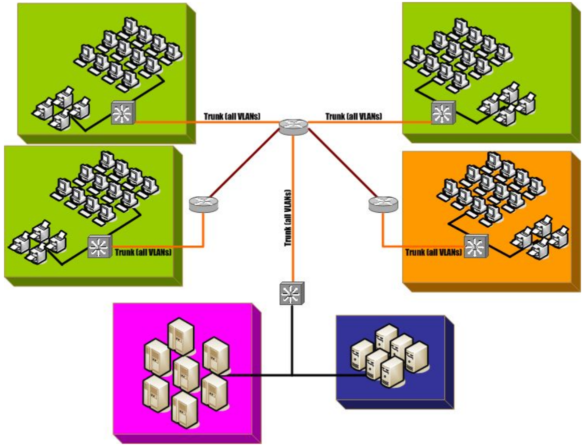
Findings

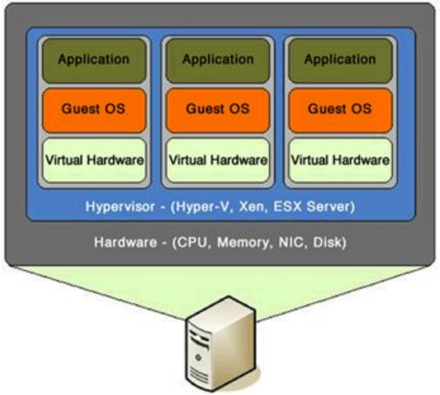
Events, Tasks

Compartmentalization

General principle: limit potential damage of breaching any one component

- Principle of least-privilege, “need-to-know”
- Networks: isolate “zones” with different functions, access
- Operating systems, virtual machines: isolate different users, apps, guests





Lecture 8: Security/Privacy Policy

- What incentives do companies have to implement security measures in their products and processes?
- Policy approaches for better security
  - Standardized algorithms, licensing
  - Independent authorities to evaluate products
  - Legal liability for failures
- Privacy vs the State: *Should governments be allowed to access personal data?*
  - Individuals' rights to privacy vs the government's duty to provide safety against criminals etc.
- Data protection laws vary across countries
  - Comparison between laws in the US and Europe
- Privacy and Online Speech
  - Can we provide freedom of speech but also protection against abuse and trolling?

Lecture 9: Data Anonymization

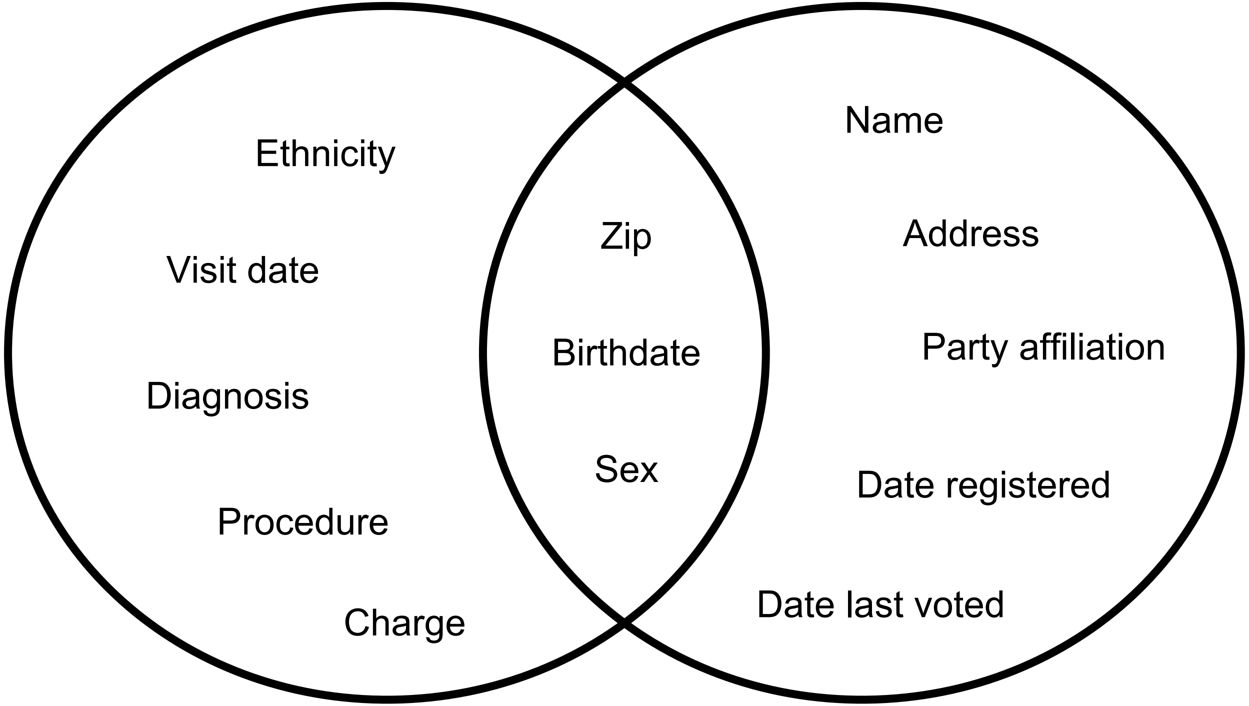
Is it possible to “scrub” sensitive information from data?

- Often to make it available to the public, and/or to researchers

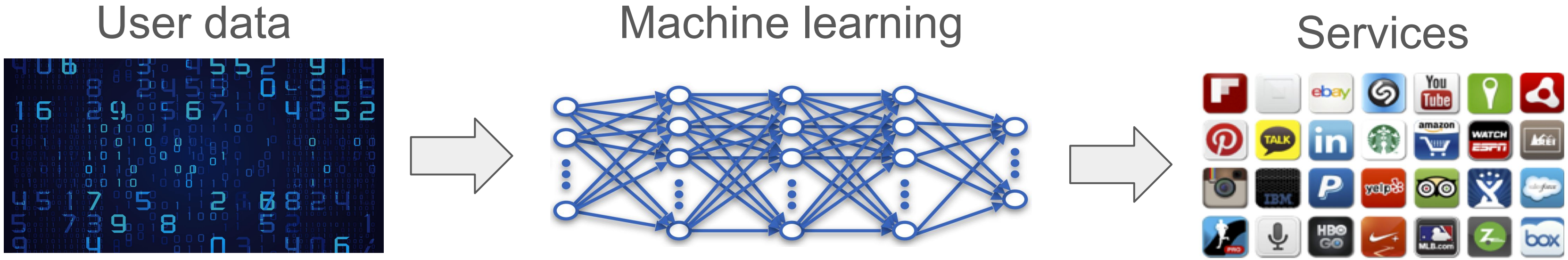
Anonymization failures

Sensitive data, but with “no names”:
e.g., medical data, Netflix history

Separate “auxiliary information”:
e.g., voter registration, IMDB reviews



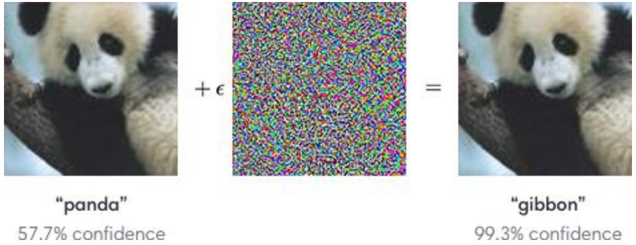
Lecture 10: Machine Learning Security & Privacy

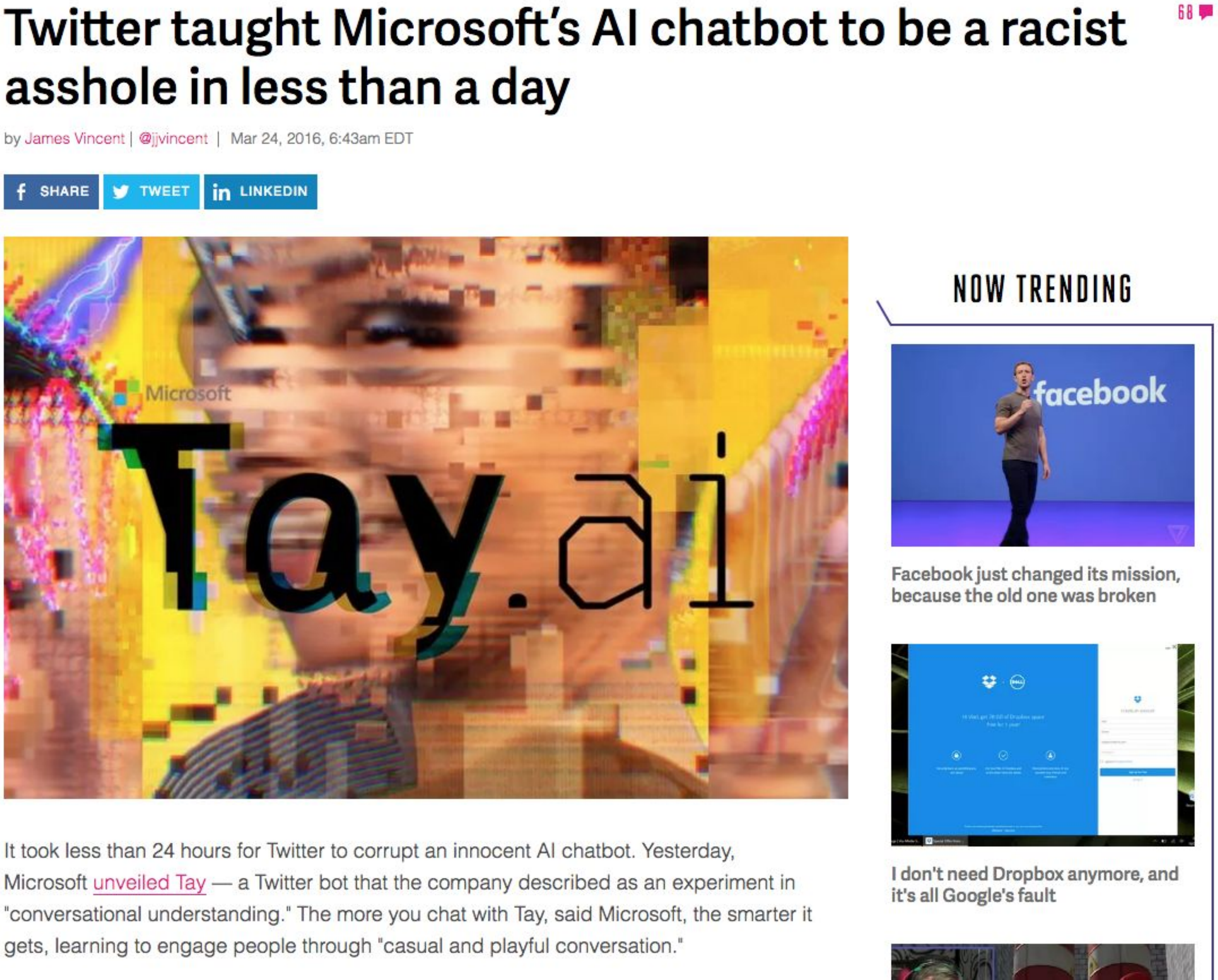


- **ML is becoming ubiquitous**
  - Data security, Financial trading, Healthcare, Marketing personalization, Fraud detection, Recommendations
- **The dark sides of ML: are algorithms "fair"?**
  - Algorithmic bias: Google ads
- **Attacking and defending ML**
  - Cause AI to make mistakes
  - Membership inference attacks against black-box models

INDY/TECH

GOOGLE'S ALGORITHM SHOWS PRESTIGIOUS JOB ADS TO MEN, BUT NOT TO WOMEN





Twitter taught Microsoft's AI chatbot to be a racist asshole in less than a day

68

by James Vincent | @jjvincent | Mar 24, 2016, 6:43am EDT

It took less than 24 hours for Twitter to corrupt an innocent AI chatbot. Yesterday, Microsoft unveiled Tay — a Twitter bot that the company described as an experiment in "conversational understanding." The more you chat with Tay, said Microsoft, the smarter it gets, learning to engage people through "casual and playful conversation."

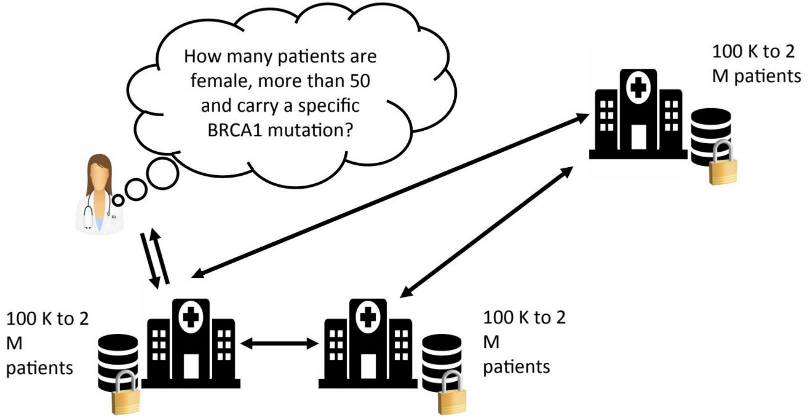
NOW TRENDING

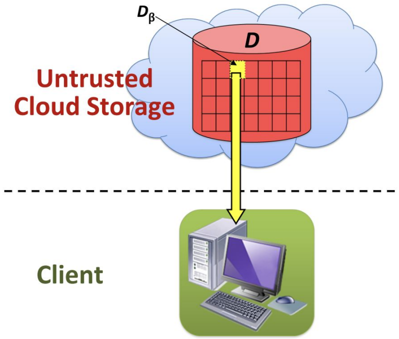
Facebook just changed its mission, because the old one was broken

I don't need Dropbox anymore, and it's all Google's fault

Lecture 11: Advanced Privacy Topics

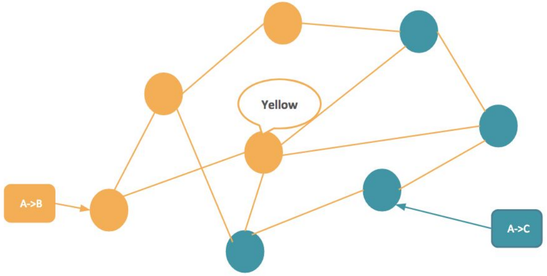
- **Crypto from the users' perspective**
- **Secure multi-party computation**
    - Examples: Electronic voting, Electronic auctions, Electronic cash schemes, Contract signing, Anonymous transactions
    - Enable parties to carry out distributed computing tasks in a secure manner
    - An attacker may try to alter the results
    - Different adversary types, e.g., honest-but-curious
- **Privacy and cloud computing**
    - Control privacy of data stored in the cloud
    - Private information retrieval
    - Oblivious RAM
    - Privacy vs overhead

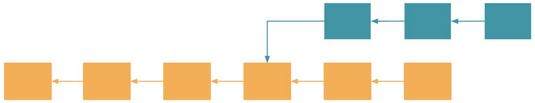

How many patients are female, more than 50 and carry a specific BRCA1 mutation?
100 K to 2 M patients
100 K to 2 M patients
100 K to 2 M patients

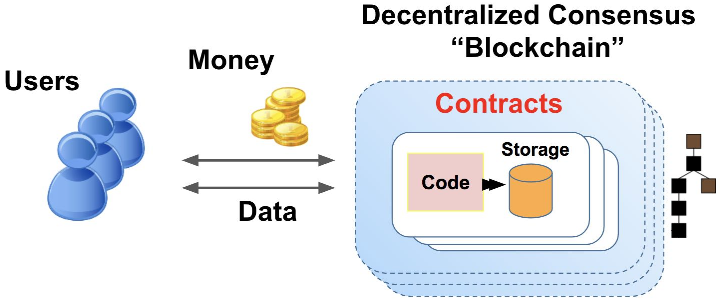


Lecture 12: Blockchains & Smart Contracts

- **Redundancy and fault tolerance**
  - The CAP theorem: Consistency, Availability, Partitions
- **Consensus & Byzantine failures**
  - Properties: validity, agreement, termination, integrity
- **Bitcoin & blockchains**
  - Conflict resolution through leader election (proof of work)
  - Unstable consensus (forks): risk or wait?
  - Double-spending attacks
- **Smart contracts**
  - User-defined programs running on top of blockchains
  - Ethereum






Decentralized Consensus
“Blockchain”

Users

Money

Data

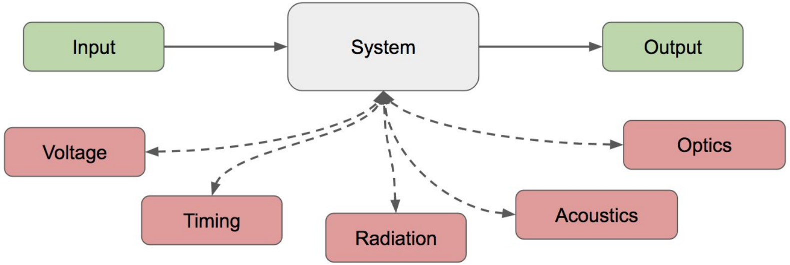
Contracts

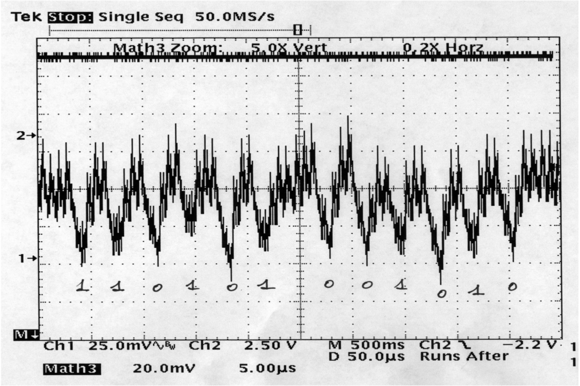
Storage

Code

Lecture 13: Side-Channel Attacks and Defenses

- **Embedded applications are on the rise**
  - RFID, Sensor networks, “Internet of Things”
  - Hardware-implemented crypto often shows severe vulnerabilities
- **Side-channel attacks target crypto implementations**
  - How much power the computer uses: triple DES power analysis
  - How long computation cases take


Input
System
Output
Voltage
Optics
Timing
Radiation
Acoustics



- **Prevention**
  - Example: Avoid conditional branch and secret intermediates
  - Using XOR, OR etc operations instead of IF / ELSE
  - Takes the same amount of time *and* power

Conclusion

- **This Wednesday (tomorrow!) on Moodle**
  - Instructions on setting up homework tools
  - First homework online
- **This Friday**
  - First exercise session
  - First homework Q & A
- **Next Tuesday**
  - More on common threats

Thanks for coming!