Security and Privacy com-402

Introduction

19.02.2019

Introduction

- Course logistics
  - Course web sites and tools
  - Tentative schedule and topic outline
  - Programming exercises overview
- Course overview
  - Threats: what can go wrong?
  - Crypto and trust in Internet protocols
  - Database security
  - Privacy, attacks and defenses
  - User management (access control, authentication)
  - NetSec & OpSec, software security
  - Blockchains and smart contracts
  - Ethics/policies, personal health data
  - E-voting protocols
- The big picture

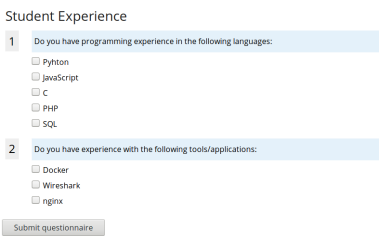
Course logistics

Course site and tools

- Moodle for COM-402

  http://moodle.epfl.ch/course/view.php?id=15812
  - announcements
  - slides
  - project descriptions
  - hand-in of project solutions

- Polls
  - Please fill out the poll in the introduction part of the Moodle to tell us about your experience



Tentative course syllabus

date	content	date	content
19.02	Introduction / Cyber Threats (pho)	09.04	Midterm
26.08	Owasp top 10 / Lowlevel attacks (pho)	16.04	User & access mgmt (pho)
05.03	Crypto basics / TLS PKI Trust (pho)	30.04	Machine learning (ct)
12.03	Database Security (pho)	07.05	NetSec OpSec (pho)
19.03	Privacy (ct)	14.05	Blockchains (jph)
26.03	Attacks on Privacy / Anonymization(ct)	21.05	Ethics, health data (jph)
02.04	Advanced privacy topics (jph)	28.05	E-voting protocols (pho)

Contact information

- Instructors
  - Philippe Oechslin - **philippe.oechslin@epfl.ch**
  - Carmela Troncoso - **carmela.troncoso@epfl.ch**
  - Jean-Pierre Hubaux - **jean-pierre.hubaux@epfl.ch**
- Teaching assistants:
  - Cristina Basescu - **cristina.basescu@epfl.ch**
  - Sylvain Chatel - **sylvain.chatel@epfl.ch**
  - Bogdan Kulynych - **bogdan.kulynych@epfl.ch**
  - Sandra Siby - **sandra.siby@epfl.ch**
  - Igor Zablotchi - **igor.zablotchi@epfl.ch**
- The best way to ask questions is to post them on the forum.

Exercices and grading

- Weekly workload
  - Lectures: 4h - Tuesdays 13:15-17:00 CM1
  - Project: 2h - Friday 15:15-17:00 CM3
  - Homework on project: 4h
- Grading structure
  - Exercises: 30% of grade
  - Midterm: 20% of grade
  - Final exam: 50% of grade
  - The lowest-scoring homework dropped
  - If the midterm grade is lower than the exam, it is replaced by the exam grade

$$G = 0.3\,\mathrm{best5of6}(homework) + 0.2\,\max(midterm, final) + 0.5\,final$$

Programming exercices 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 (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

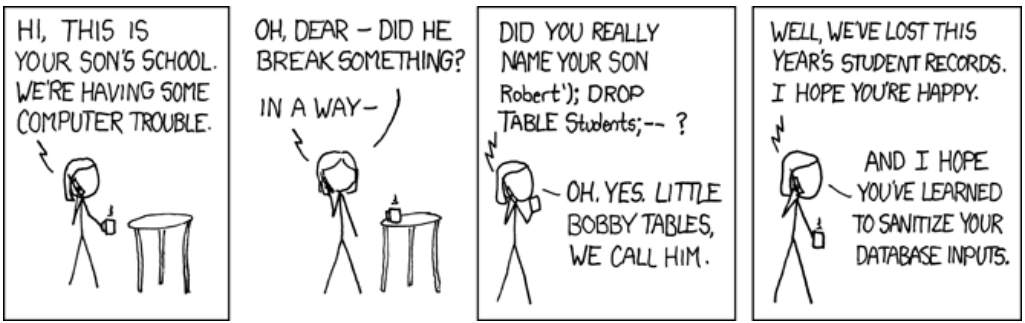
Set	Type	content
1	attack	hacking login forms, sniffing
2	defense	server-side login, key exchange, MACs, HTTPS certificates
3	attack	deanonymisation, cracking passwords, downgrade attack
4	defense	anonymisation, bcrypt password hashing, protecting against SQL injection, HSTS
5	attack	buffer overflows, stegano, timing attacks, attacks against ML
6	defense	IDS, blockchain and PETs (PIR)

Attack/defense homework 1&2

- Authentication
  - Break client-side authentication,
  - Implement it server-side
- Sniffing
  - Sniff credit card numbers and passwords
  - Use HTTPS to protect your data
- Tampering
  - Intercept and modify delivery address
  - Protect data with auhtentication codes

Attack/defense homework 3&4

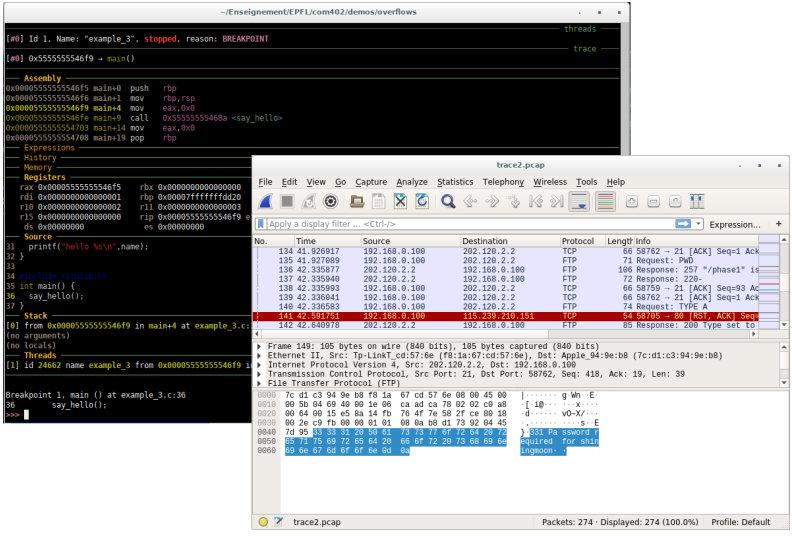
- Database security



source: **xkcd 327**

Attack/defense homework 5&6

- A mix of different attacks and defenses



Outline

- Course logistics
  - Course web sites and tools
  - Tentative schedule and topic outline
  - Programming exercises overview
- Course overview
  - Threats: what can go wrong?
  - Crypto and trust in Internet protocols
  - Database security
  - Privacy, attacks and defenses
  - User management (access control, authentication)
  - NetSec & OpSec, software security
  - Blockchains and smart contracts
  - Ethics/policies, personal health data
  - E-voting protocols
- The big picture

Course overview

Cyber Threats

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

- details and clearance of 4 mil people (mostly gov.) **lawfareblog.com**

Cyber Threats

Paper claims special forces unit exposed by hack

By Jeannie Wurz

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.

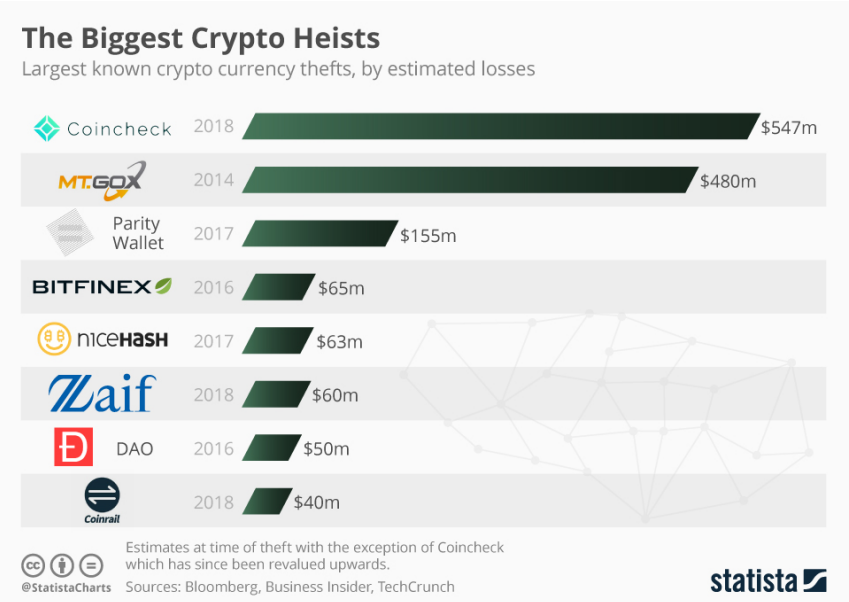
On Sunday, the NZZ am Sonntag reported that Russian IT specialists had gained access to personal data of members of the secret DRA10 special forces unit, which was established for risky operations in foreign countries.

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

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

source: **swissinfo**

Cyber Threats



source: **statista**

Cyber Threats

POISONING THE WELL —

If you installed PEAR PHP in the last 6 months, you may be infected

Pear.php.net shuts down after maintainers discover serious supply-chain attack.

DAN GOODIN - 1/23/2019, 9:10 PM

Thomas Hawk

64

Officials with the widely used PHP Extension and Application Repository have temporarily shut down most of their website and are urging users to inspect their systems after discovering hackers replaced the main package manager with a malicious one.

"If you have downloaded this go-pear.phar [package manager] in the past six months, you should get a new copy of the same release version from GitHub (pear/pearweb_phars) and compare file hashes," officials wrote on the site's blog. "If different, you may have the infected file."

The officials didn't say when the hack of their Web server occurred or precisely what the malicious version of go-pear.phar did to infected systems. Initial indications, however, look serious. For starters, the advice applies to anyone who has downloaded the package manager in the past six months. That suggests the hack may have occurred in the timeframe of last July, and no one noticed either it or the tainted download until this week.

Software vulnerabilities (web)

How I was able to delete Google Gallery Data [IDOR]

Yogesh Tantak Follow

Dec 30, 2018 · 2 min read

Hi,

This is **Yogesh Tantak** a Security Researcher from India. Today I am writing about a critical bug that I found in Google's new Product "Gallery".

You can find out more information about this product by below url: https://www.theverge.com/2016/10/26/13418012/google-material-design-stage-gallery-pixate

This bug could allowed a malicious user to delete all collection from Gallery.io or Google gallery app.

source: medium.com

Software vulnerabilities (memory)

CVE-2018-8626 Detail

Current Description

A remote code execution vulnerability exists in Windows Domain Name System (DNS) servers when they fail to properly handle requests, aka "Windows DNS Server Heap Overflow Vulnerability." This affects Windows Server 2012 R2, Windows Server 2019, Windows Server 2016, Windows 10, Windows 10 Servers.

Source: MITRE
Description Last Modified: 12/11/2018
+View Analysis Description

Impact

CVSS v3.0 Severity and Metrics:
Base Score: 9.8 CRITICAL
Vector: AV:N/AC:L/PR:N/UI:N/S:U/C:H/I:H/A:H (V3 legend)
Impact Score: 5.9
Exploitability Score: 3.9

CVSS v2.0 Severity and Metrics:
Base Score: 10.0 HIGH
Vector: (AV:N/AC:L/Au:N/C:C/I:C/A:C) (V2 legend)
Impact Subscore: 10.0
Exploitability Subscore: 10.0

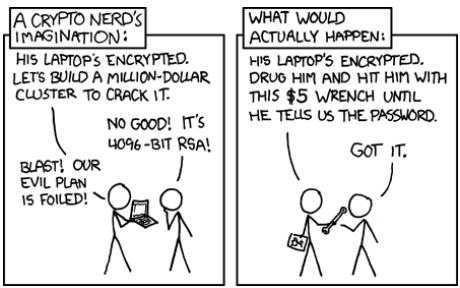
QUICK INFO

CVE Dictionary Entry:
CVE-2018-8626
NVD Published Date:
12/11/2018
NVD Last Modified:
01/03/2019

source: nist.gov

Crypto and Trust in the Internet

- Crypto (cryptography) protects data using keys
  - Communications (HTTPS, SSH, GSM)
  - Files and disks (Bitlocker, GPG, Veracrypt)
- Goals
  - Confidentiality
  - Integrity
  - Authentication
- It can only be trusted if keys are distributed securely



source: **xkcd 538**

Crypto and Trust

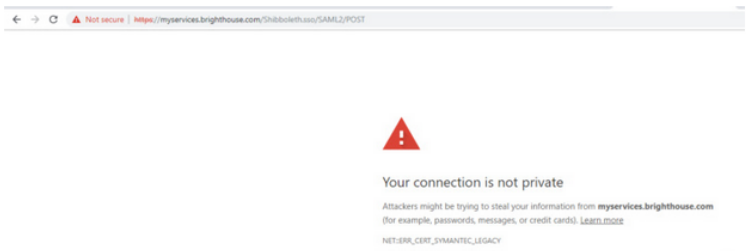
Google makes good on promise to remove some Symantec PKI certificates

If you get this digital certificate error using Chrome, then Google now considers that website's Symantec PKI certificate untrustworthy.

By **Roger A. Grimes**

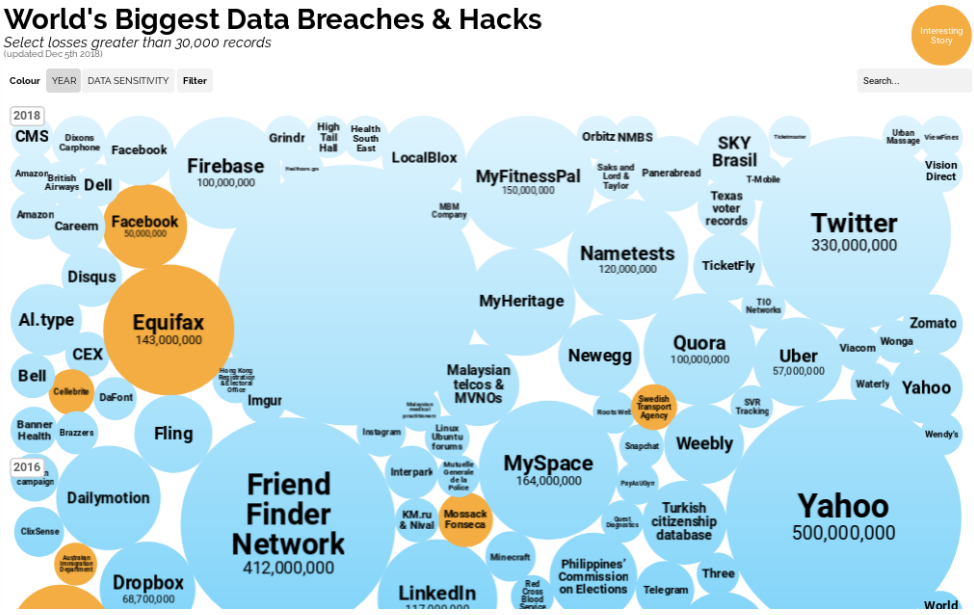
Columnist, CSO | NOV 21, 2018 11:26 AM PT

Thinkstock



source: **CSOonline**

Database security



source: **informationisbeautiful.net**

Privacy, attacks and defenses

Here are some of the biggest reveals from a fitness-tracker data map that may have compromised top-secret US military bases around the world

Daniel Brown Jan. 29, 2018, 4:08 PM

Screenshot/Twitter via @AlecMuffett

A fitness app called Strava updated the 2017 exercise routes of more than one billion people over the weekend.

In the process, Strava may have inadvertently revealed the locations and activities of US troops in secret bases around the world.

source: **businessinsider**

Privacy, attacks and defenses

Benjamin Mayo @bzamayo · 7h

This is not good — FaceTime call any iPhone and hear their microphone instantly, without their consent.

Major FaceTime bug lets you hear the audio of the person you are ...

A significant bug has been discovered in FaceTime and is currently spreading virally over social media. The bug lets you call anyone on Fa...

9to5mac.com

source: twitter

Privacy, attacks and defenses

source: **Enisa Workshop on Privacy**

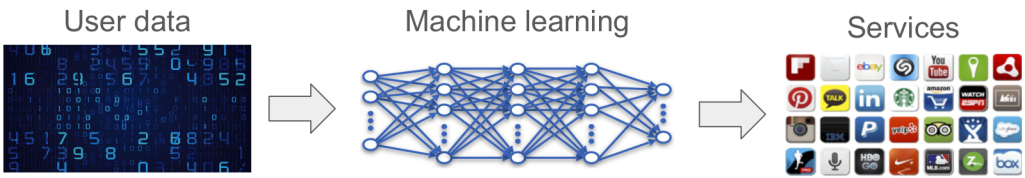
- e.g. Anomymization, pseudonimization, anonymous networks, payments...

User and Access Mgmt

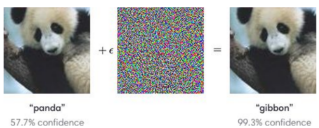
- Access control
  - Role-based access control
  - Discretionary access control
  - Mandatory access control
- Authentication
  - Passwords
  - Kerberos, from MIT to Microsoft
  - Multifactor auhtentication
    - OTP
    - Biometrics
    - Webauthn, U2F, FIDO2

Two Factor Authentication

Machine Learning Security & Privacy



- ML is becoming ubiquitous
  - data security, financial trading, healthcare, marketing, fraud detection
- The dark side of ML: are algorithms 'fair'?
- Attacking and defending ML
  - cause Ai do make mistakes
  - membership inference attacks against black-blx models



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

By James Vincent | Mar 24, 2016, 6:43am EDT

SHARE

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."

source: **The verge**

NetSec & OpSec, software security

source: NSA

source: NSA

NetSec & OpSec, software security

- Identify the risk
- Minimize the risk
  - segregation of networks and data
    - Firewalls, Vlans
  - protect apps and data
    - WAFs
- Prepare response
  - Have a plan
  - save logs

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
  - Unstable consensus (forks): risk or wait?
  - Double spending attacks (like this january on Ethereum Classic)
- Smart contracts
  - User-defined programs running on top of blockchains
  - Ethereum

Ethics/policies, personal health data

- What incentives do companies have to implement security
- Policy approaches
  - standardized algorithms
  - independent authorities to evaluate products
  - legal lieability
- Privacy vs the State
- Data protection laws
- Specific aspects of health data

E-voting protocols

- In some Swiss cantons you can vote by Internet
  - additionally to postal voting or going to the polling station
- The system is based on a cryptographic protocol
- The challenge is to prove that the votes have not been manipulated, while preserving the secrecy of the vote
- The protocols make abundant use of zero knowledge proofs and of homomorphic encryption
- This year, there is a public intrusion test where you can try to hack the system.

Outline

- Course logistics
  - Course web sites and tools
  - Tentative schedule and topic outline
  - Programming exercises overview
- Course overview
  - Threats: what can go wrong?
  - Crypto and trust in the Internet
  - Database security
  - Privacy, attacks and defenses
  - User management (access control, authentication)
  - NetSec & OpSec, software security
  - Blockchains and smart contracts
  - Ethics/policies, personal health data
  - E-voting protocols
- The big picture

The big picture

The big picture

- We want to protect
  - information,
  - information systems
  - real-world (physical) systems that depend of IT systems
  - people
- We need a method
  - to understand
  - classify &
  - prevent

  what can go wrong.

Basic properties (security)

- Confidentiality
  - keep information secret (e.g. recipe of Coca Cola)
  - give read access only to those who need to know
  - tools: access control, isolation, encryption
- Integrity
  - keep information correct (e.g. my accounts balance)
  - prevent modification of data
  - detect modification
  - tools: add a hash, a MAC or a signature, make public

Basic properties (security)

- Availability
  - keep information available (e.g. my photos)
    keep a system running
  - tool: make copies, duplicate/distribute systems, prevent intrusions
- Authenticity (aka integrity of origin)
  - demonstrate the authenticity of information (e.g gift card)
  - prevent fake information
  - detect modification
  - tool: add a keyed hash (MAC) or a signature

Basic properties (security)

- Non repudiation
  - prevent denial of a statement (e.g. payment order)
  - tool: add a signature as proof of origin

Basic properties (privacy)

- Confidentiality
  - keep information of the data subject[1] secret (e.g. my age, my opinions, health)
  - give access only to those who need to know
  - tool: access control, encryption, absence of data
- Anonymity
  - prevent a link between data and a subject (e.g. postal address and age)
  - reduce/modify information until no correlation is possible
  - tool: k-anonymity, differential anonymity
- Pseudonimity
  - reversible anonymity
  - replace all identifying information (name) by generic identifier (number)
  - difficult to get right

[1] the person mentioned in the data

Basic properties (privacy)

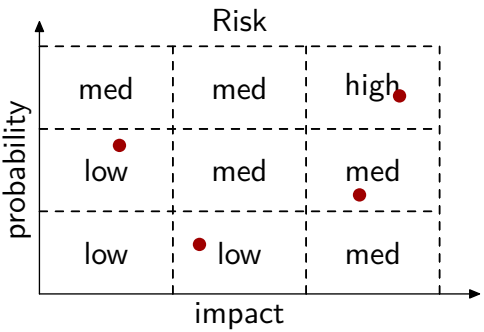
- Absence of information
  - Prevent abuse of information (e.g. reuse of your e-mail address for spam)
  - Don't request unnecessary information (duh!)
  - Delete information that is no longer needed
  - Work on encrypted information
  - tools: homomorphism, private information retrieval, zero knowledge proofs

Differences

- Security
  - Protects the data of data owners (e.g. company) against attacks.
- Privacy
  - Protects the data subject against abuse.
- It is in a company's interest to have good security.
- Protecting the privacy of its customer doesn't always have a benefit for a data owner. Some make money by abusing privacy (Facebook?)
- This is why we need strong laws to force companies to protect privacy.
- Privacy by design: chose a design that achieves its goal while minimizing the threats to privacy
  - e.g. passive GPS vs radar

The security lifecycle

- Risk assessment
  - identify assets, their threats and vulnerabilities
  - analyze the corresponding risk (impact, probability)
  - evaluate which risks are acceptable, which must be treated



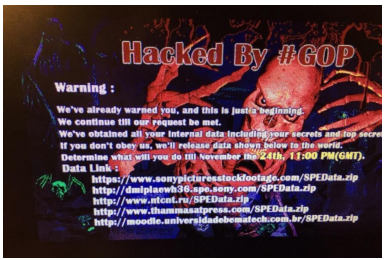
The security lifecycle

- Policy (rules that should reduce risk to acceptable)
  - what is, and what is not allowed
    - personal data must not be leaked
  - makes use of security mechanisms
    - pesonal data must be encrypted,
    - install anti-virus software
    - name a data protection officer
- Implementation
  - Specify, design and implement
- Operations and maintenance

Example: Sony Pictures Hack

The Sony Pictures hack

- Motivation (?)
  - The "Guardians of Peace" demanded money and the withdrawal of a movie mocking Kim Jong-Un



source: Internet

- The attack
  - Probably got into the network through a VPN connection with a phished password
  - they used a new vulnerability in Ms-Windows to become administrator
  - exfiltered Gygabytes of data
  - since no money was payed, they published everything

The Sony Pictures hack

- Impact
  - GoD tried to delete the hard disk of all computers
  - Published passwords, e-mails, internal documents, including
    - salaries of employees and actors
    - scripts of new tv series
    - medical information of employees
    - e-mails with comments about actors: angelina jolie “minimal talented spoiled brat”, Leonardo di Caprio “despicable”
  - The employees filed a class action suite for failure to protect their data.
    - Sony payed $8mio.
  - Sony estimated a total cost of $35 mio.

Lessons learned

- Network security is important...
- They could have reduced the impact by having less information online
  - archive or delete old information
- Leaking movie scripts is a security issue (hurts the company)
- Leaking medical information is a privacy issue (hurts the employees)
  ➡ also hurts the company if privacy laws are strict enough
- Their risk assessment probably did not identify an impact of tens of millions in case of a network based attack
- Do not write unnecessary degrading remarks in e-mails
- Do not mess with Kim Jong-Un

Lessons learned

- Compare the following two policies
  1. encrypt all medical data and limit access to strict minimum
  2. do not store any medical data, use it to make decisions then destroy it

- Cost-benefit analysis
  - if the probability of success of such an attack is 0.1% per year
  - it would be worth spending $35'000 a year to prevent it

Conclusions & Questions

Conclusions

- Security and privacy is about controlling risk
- Can't be secure without
  - knowing your assets, threats and risks,
  - have some basic trust assumptions (e.g. encryption can not be broken, my sysadmin is honest, ...)
- You just have to define your policy and mechanisms and implement them.
- It is an ongoing process
  - needs regular audit and improvement

Questions

- Encryption is usually used to protect
  - confidentiality, integrity or availability ?
- Cite a security mechanism that is could for security, but bad for privacy
- What are the two informations you need to measure the importance of a risk ?
- Does the subscription of an insurance that pays for losses in case of an attack reduce the risk ?