Università
della
Svizzera
italiana

Facoltà
di
scienze
informatiche

Edge Computing in the IoT

Security and Privacy

Alberto Ferrante (alberto.ferrante@usi.ch)

Università
della
Svizzera
italiana

Facoltà
di
scienze
informatiche

Security

Security - Introduction

- Security is not a product nor a technique, security is a process
  - In systems involving human beings, the latter are often the weakest element
    - Poorly chosen passwords
    - Default username and password not changed by users
    - …
  - The process begins while designing a system
    - Including security in the requirements from the beginning of the process is key

Alberto Ferrante, Igor Kaitovic, and Jelena Milosevic. Modeling requirements for security-enhanced design of embedded systems. In ICETE SECRYPT, Vienna, Austria, August 2014. ICETE

Ferrante, A., J. Milosevic, and M. Janjusevic, A Security-enhanced Design Methodology For Embedded Systems, ICETE SECRYPT 2013, Reykjavik, Iceland, ICETE, 07/2013.

Security Principles

- Security of the whole system is equivalent to security of the weakest part of the system

Security Principles

- There is no absolute security
  - Relative concept, it depends on
    - Effort that the attacker is willing to put in violating a system
    - Resources and skills of the attacker
  - Dynamically changing: if something is sufficiently secure today, it does not mean it is going to be also tomorrow
    - New attacks that may require different countermeasures
    - New vulnerabilities may lead to novel attacks
      - Software
      - Hardware
      - Cryptographic algorithms

Vulnerabilities

- A vulnerability is a weakness in a system that can potentially be exploited by an attacker
- Some vulnerabilities might be more critical than others, depending on the context:
  - The risk presented by a vulnerability is based on the likelihood that an attacker is going to take advantage of it

An example: Canon’s Picture Transfer Protocol Vulnerabilities

- Check Point researchers demonstrated an attack to some Canon cameras at the DEFCON 2019 conference
- Some vulnerabilities were discovered on the Picture Transfer Protocol
  - CVE-ID: CVE-2019-5994, CVE-2019-5995, CVE-2019-5998, CVE-2019-5999, CVE-2019-6000, CVE-2019-6001
- Identified risks:
  - Over the air update with a fake firmware
  - Remote access and modification of the memory card contents
    - Ransomware

Security Requirements

- Security should be analyzed from the stand point of the attacks that the system should withstand
- What do we need to protect from?
  - What are the important things that we are willing to protect?
    - Data?
    - System?
    - …
- What are the resources that we are willing to invest in security?

Alberto Ferrante, Igor Kaitovi´c, and Jelena Milosevic. Modeling requirements for security-enhanced design of embedded systems. In ICETE SECRYPT, Vienna, Austria, August 2014. ICETE

Ferrante, A., J. Milosevic, and M. Janjusevic, A Security-enhanced Design Methodology For Embedded Systems, ICETE SECRYPT 2013, Reykjavik, Iceland, ICETE, 07/2013.

Security Countermeasures

- Implementing countermeasures in IoT devices may be difficult
  - Limited resources
  - Limited energy
  - No or limited user interaction
  - Security is often not perceived as a selling point
  - Edge network topology is (partly) unknown in advance and network infrastructure is limited

Security From the Stand Point of Attacks

- Security is often thought starting from security techniques
  - E.g., I use encryption, therefore my system is secure
  - ➔ This is wrong:
    - First we need to know the problems, then we solve them
- Security can only be evaluated against the attacks that we foresee for the considered system
  - What are the known attacks?
  - Which are the ones that are relevant to our system?
- Security solutions are deployed based on the foreseen attacks

Security for IoT

- We should consider security for the whole system, of which IoT devices are only a part
  - Security of edge, fog, and cloud
  - Communication security

Designing a Secure System

1) Identify the known attacks relevant to our system

2) Identify the relevant attacks that may pose a significant risk to our system

3) Identify/design security solutions that are suitable for the selected attacks
   - Solutions may cover (totally or partially) multiple attacks
   - Some attacks may have multiple solutions
   - Some attacks may require multiple solutions

4) Find the optimal combination of security solutions to cover the identified attacks
   - Consider costs of the different solutions
     - Silicon area
     - Computational resources
     - Power/Energy
     - ...

Alberto Ferrante, Igor Kaitovi´c, and Jelena Milosevic. Modeling requirements for security-enhanced design of embedded systems. In ICETE SECRYPT, Vienna, Austria, August 2014. ICETE

Ferrante, A., J. Milosevic, and M. Janjusevic, A Security-enhanced Design Methodology For Embedded Systems, ICETE SECRYPT 2013, Reykjavik, Iceland, ICETE, 07/2013.

Attacks for Embedded Devices

- Targeted attacks
- Malware
- Side channel attacks
- Man in the middle
- ...

Targeted Attacks

- Manual or semi-automatic attacks targeted at specific systems
- They usually follow some patterns
  - .e.g., port scanning to discover the type of device + some actions if the device is of a certain type
- They exploit vulnerabilities
  - Hardware and software vulnerabilities
  - Misconfiguration
  - Social engineering

Malware

- Malware=malicious software
- Many different families with different purposes and behavior
  - Malware is specific for each operating system or piece of software
    - Huge amount of malware for smartphones and alike
      - IoT devices may be involved too: e.g., Android Things or Android Auto
    - Malware for Linux-based IoT devices
    - ...

Malware

- It mostly targets IoT devices that run an operating system
  - Easier to target many devices that have similarities
  - Devices with applications running on bare metal may be targeted, but each application requires a specific method
    - Software libraries may provide a common ground
    - Hardware vulnerabilities may provide a common ground
- Not always easy to detect
  - Limited resources of devices
  - Remote detection might not be compatible with constraints on network
  - Limited possibility to update signature database when new malware appears
  - No interaction with users

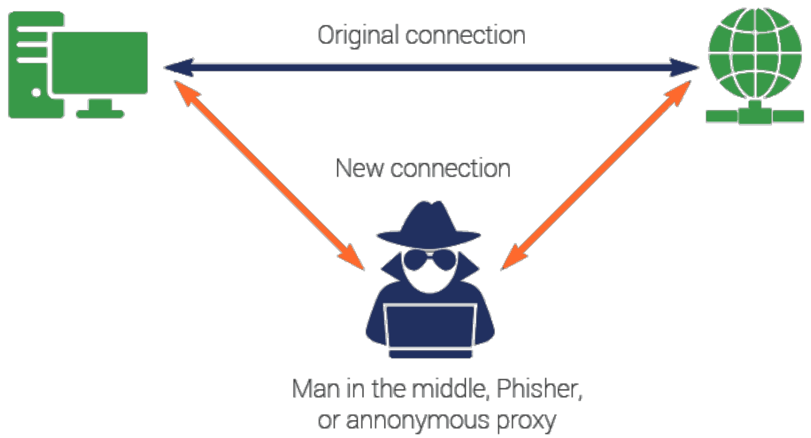
Side-channel Attacks

- Any attack based on information gained from the implementation of a computer system, rather than weaknesses in the implemented algorithm itself
  - Cache attack — attacks based on attacker's ability to monitor cache accesses made by the victim in a shared physical system as in virtualized environment or a type of cloud service
  - Timing attack — attacks based on measuring how much time various computations (such as, say, comparing an attacker's given password with the victim's unknown one) take to perform
  - Power-monitoring attack — attacks that make use of varying power consumption by the hardware during computation
  - Electromagnetic attack — attacks based on leaked electromagnetic radiation, which can directly provide plaintexts and other information
  - Acoustic cryptanalysis — attacks that exploit sound produced during a computation
  - Differential fault analysis — in which secrets are discovered by introducing faults in a computation

https://en.wikipedia.org/wiki/Side-channel_attack

Man-in-the-middle Attacks

- An attack where the attacker secretly relays and possibly alters the communications between two parties who believe they are directly communicating with each other
- Common countermeasure: encryption + authentication



https://en.wikipedia.org/wiki/Man-in-the-middle_attack

Purposes of Attacks

- Denial of Service / Distributed Denial of Service
  - Including impacts on safety
- Data stealing / corruption

Trends in IoT Threats

- Consumer grade IoT devices (routers, cameras, NAS boxes, and smart home components) multiply every year
  - Their number is predicted to exceed 29 billion by 2030
- The first-ever large-scale malware attacks on IoT devices were recorded back in 2008, and their number has only been growing ever since.

SECURELIST by Kaspersky; Overview of IoT threats in 2023. September 2023. https://securelist.com/iot-threat-report-2023/110644/

Trends in IoT Threats

- Two main infection routes:
  - Brute-forcing weak passwords
    - Telnet and SSH services running on IoT devices typically use widely known default passwords
    - Users tend to leave these passwords unchanged
    - Many IoT devices have unalterable main passwords set by manufacturers
  - Exploiting vulnerabilities in network services
- Telnet is the main target of brute-forcing
  - A successful password cracking enables hackers to execute arbitrary commands on a device and inject malware
  - Brute-force attacks on services that use SSH can yield similar outcomes.
    - It takes more resources to attack SSH, while the number of services accessible online is smaller compared to Telnet
  - 98% of attempts registered by Kaspersky honeypots targeted Telnet; 2%, SSH

SECURELIST by Kaspersky; Overview of IoT threats in 2023. September 2023. https://securelist.com/iot-threat-report-2023/110644/

Trends in IoT Threats - Objectives and types of malware for IoT

- DDoS botnets: Trojans that hijack a device and use it to initiate DoS attacks targeting various services are the most frequently observed type of IoT malware
- Ransomware: ransomware largely targets IoT devices that contain user data
- Miners: attackers made attempts at using IoT devices for Bitcoin; the practice has not become widespread due to relative inefficiency
- DNS changer: e.g., an Android app whose capabilities included modifying DNS settings on Wi-Fi routers through the administration interface
- Proxy bots: leverage IoT devices as proxy servers that redirect malicious traffic, making it difficult to track; mostly employed for spam campaigns, evasion of antifraud systems, and various network attacks

SECURELIST by Kaspersky; Overview of IoT threats in 2023. September 2023. https://securelist.com/iot-threat-report-2023/110644/

An Example: Mirai

- Mirai is malware
- Used in some of the largest and most disruptive distributed denial of service (DDoS) attacks
- Turns networked devices running Linux into remotely controlled bots that become part of a botnet in large-scale network attacks
  - Once infected, the device monitors a command and control server which indicates the target of an attack
- Devices continuously scan the internet for the IP address of other IoT devices
  - Primary targets are online consumer devices such as IP cameras and home routers
  - Vulnerable IoT devices are identified by using a table of more than 60 common factory default usernames and passwords: if any of the works, the malware logs in and infect them

An Example: Mirai

- Infected devices will continue to function normally, except for occasional sluggishness and an increased use of bandwidth
- A device remains infected until it is rebooted
  - After a reboot, unless the login password is changed immediately, the device will be reinfected within minutes
- Upon infection Mirai will identify any "competing" malware, remove it from memory, and block remote administration ports
- The code of Mirai have been shared on Github
  - It has been used in numerous variations

Security Solutions

- Secure communication protocols:
  - Encryption
  - Authentication
- Memory and process isolation
- Malware detection
- Network protection
  - Firewall
  - Intrusion detection
  - ...

Encryption

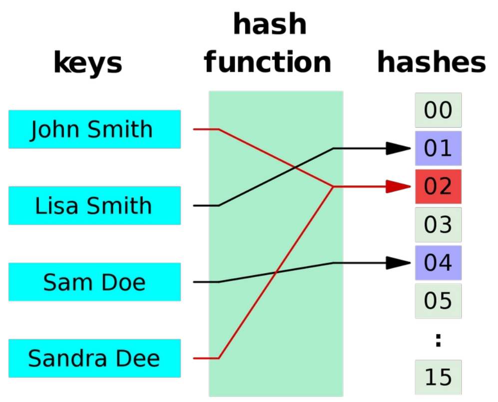
- Encryption is useful for obfuscating information in such a way that it cannot be read by unintended parties
- Encryption can be
  - Symmetric: one key per communication that is shared among parties
    - Used for encryption and decryption
    - More efficient algorithms
  - Asymmetric: data are encrypted by using the public key of the recipient
    - It can be decrypted only by using the corresponding private key
- **There exist cases in which even encryption is not sufficient:**
  - E.g., the fact that our device is transmitting something is already a valuable information, even though it is encrypted

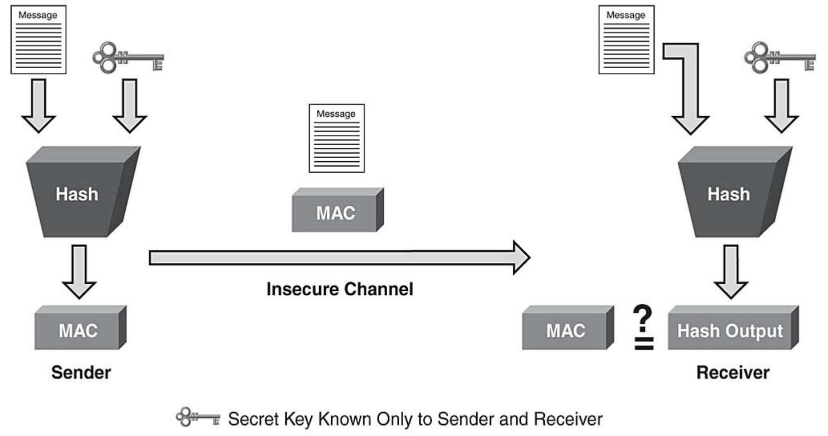
Identity Authentication

- A secret is used to authenticate the identity of a user/device
  - Password
  - Certificate
    - Set of information protected by suitable cryptographic primitives that render them verifiable
  - ...

Data Authentication

- A mechanism to certify that data have not been modified by unintended third parties
  - Combined use of
    - Hash algorithms
      - Summary of data computed by using a function that provides collisions with a very small probability
    - Cryptographic algorithms
      - The hash is mixed with pubic/symmetric keys: HMAC
- Data authentication can be performed by using
  - A symmetric key
  - A private key
    - The corresponding public key is used to verify signature





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

Secure Communication Protocols

- Encryption and authentication algorithms cannot be used alone
  - How to manage and exchange keys?
  - Set up connection
    - Which algorithms to use?
    - Which algorithm settings?
    - …
- Secure communication protocols offer security by relying on encryption and authentication algorithms
- They can be used at different levels of the OSI stack
  - IPSec: Internet layer (layer 3)
  - SSL/TLS (SSL is deprecated): application layer
- In embedded devices, hardware support for encryption algorithms is fundamental

Security Protocols / Cryptography and Embedded Devices

- Management of certificates and keys is an issue when deploying many devices
  - Each device should have different keys and certificates
  - Firmware is usually installed on devices by installing a binary that is the same for all devices
- Encryption, and especially authentication, are resource consuming (energy, computational resources)
  - The use of hardware accelerators greatly contributes to making them applicable
  - Not all devices may support full security protocols
  - There exist algorithms and protocols designed for limited-resource devices

Process Isolation

- Allow processes to access only specified resources
  - Memory
  - Files
  - Network interfaces
  - …
- Security Enhanced Linux (SELinux)
  - Is a Linux kernel security module that provides a mechanism for supporting access control security policies, including mandatory access controls (MAC)
  - Used in Android
  - Policies describe what subjects can do on objects
    - E.g., processes of a certain class can access files in a certain directory and devices of a certain class
- ARM Trustzone
  - Hardware support for process isolation

https://www.nsa.gov/what-we-do/research/selinux/

Malware Detection

- Still an open research problem for IoT, at least in the general case
  - Where to perform detection (edge, fog, cloud)?
  - How to perform detection?
  - How to update the detection methods to detect new malware families?
- No (direct) user interaction implies that false positives must be extremely unlikely, yet, detection performance must be good
- What to do after detection?
  - Depends on the system and on the malware family
  - In IoT, reboot of the device usually solves the problem
  - Process isolation can be used to confine the malicious process
  - Process killing is also a possibility

Software Vulnerabilities and IoT Devices

- Dealing with vulnerabilities (and bugs) usually means updating software
- May be done (provided that devices support it) through Over The Air (OTA) updates
  - Otherwise, it should be done by hand...
- May not be easy/feasible:
  - Devices may be in remote locations with limited network connectivity
    - E.g., extremely limited bandwidth
  - Devices may be equipped with very limited energy
    - OTA can be expensive
- Even when feasible, updates may be risky

What About Privacy?

JOIN MWU | GAMES | BROWSE THESAURUS | WORD OF THE DAY | WORDS AT PL

Merriam-Webster SINCE 1828

privacy

DICTIONARY | THESAURUS

privacy *noun*

pri·va·cy | \ ˈprī-və-sē, *especially British* ˈpri-\

plural **privacies**

Definition of *privacy*

1 **a** **:** the quality or state of being apart from company or observation **:** SECLUSION

b **:** freedom from unauthorized intrusion

// one's right to privacy

2 **a** **:** SECRECY

b **:** a private matter **:** SECRET

3 *archaic* **:** a place of seclusion

Support The Guardian
Available for everyone, funded by readers
Contribute → Subscribe →

Search jobs Sign in Search International edition

The Guardian

News Opinion Sport Culture Lifestyle More

World UK Environment Science Cities Global development Football Tech Business Obituaries

Apple

This article is more than 1 month old

Apple apologises for allowing workers to listen to Siri recordings

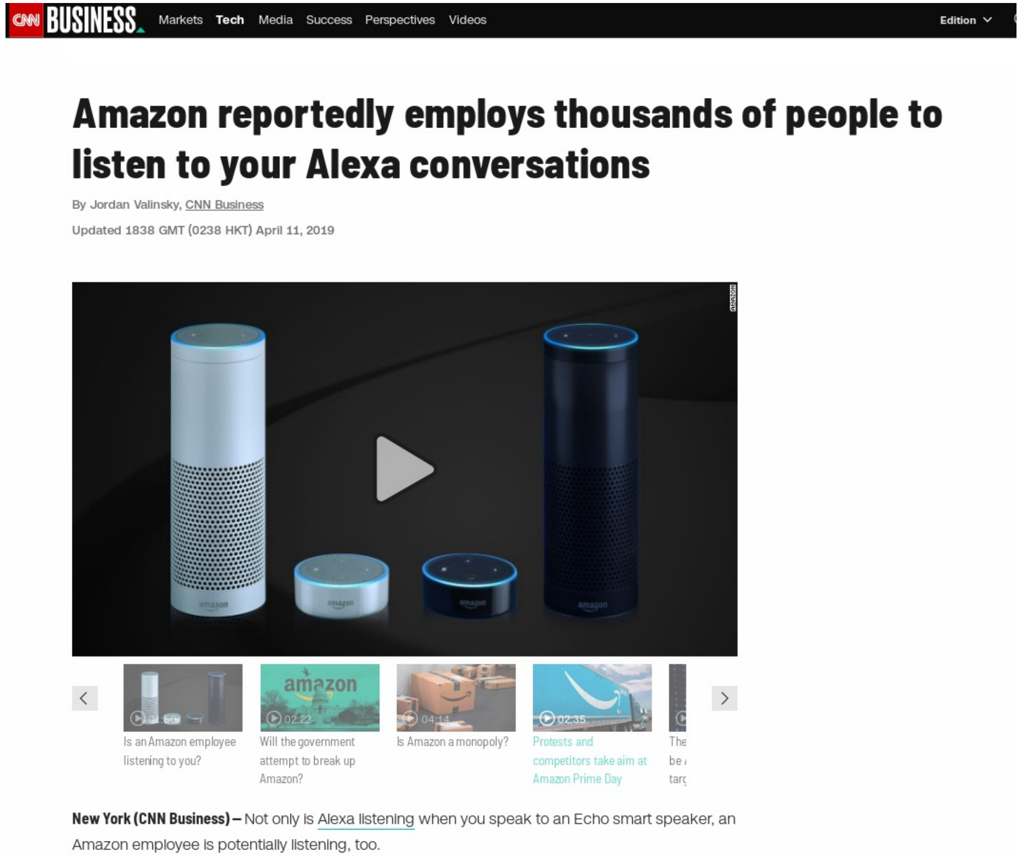
Contractors graded accidental activations including recordings of users having sex

Alex Hern *Technology editor*
@alexhern
Thu 29 Aug 2019 10.59 BST

261

Apple has apologised to Siri users for not 'fully living up to our ideals'. Photograph: Bloomberg/Getty

Apple has apologised for allowing contractors to listen to voice recordings of Siri users in order to grade them.



CNN BUSINESS Markets Tech Media Success Perspectives Videos Edition

Amazon reportedly employs thousands of people to listen to your Alexa conversations

By Jordan Valinsky, CNN Business
Updated 1838 GMT (0238 HKT) April 11, 2019

Is an Amazon employee listening to you?
Will the government attempt to break up Amazon?
Is Amazon a monopoly?
Protests and competitors take aim at Amazon Prime Day

New York (CNN Business) — Not only is Alexa listening when you speak to an Echo smart speaker, an Amazon employee is potentially listening, too.

- The chief privacy risk implied by a world of sensing, connected devices is greater monitoring of human activity
  - Context awareness through enhanced audio, video, location data, and other forms of detection is touted as a central value of the IoT
  - The privacy implication is clear: you will be under observation by your machines and devices you do not control
- A direct result of enhanced monitoring is greater ease in tracking people’s movements
  - More devices—and therefore more organizations and systems—will know where you are, where you’ve been, and, increasingly, where you’re going next

Gilad Rosner, *Privacy and the Internet of Things*. O’Reilly Media, 2016.

Consense

- The introduction of more sensing devices into the human environment raises questions of consent
  - Although individuals can consent data collection by devices they purchase and install, what of the people who enter spaces and don't know the devices are there?

Gilad Rosner, *Privacy and the Internet of Things*. O'Reilly Media, 2016.

Privacy, is there any?

- Most used technique to collect data and protect privacy: data anonymization
- Is anonymization effective?
  - By using known characteristics of a user, data can be de-anonymized, e.g.:
    - By locating four times an user in one year, it was possible to extract complete user location information from an anonymized database of 1.5 million mobile phone users [3]
    - By using data emitted from accelerometers of different devices, it is possible to correlate multiple persons and use the location of one of them to compute the location of the others [4]

[3] Yves-Alexandre de Montjoye; César A. Hidalgo; Michel Verleysen; Vincent D. Blondel. "Unique in the Crowd: The Privacy Bounds of Human Mobility," Scientific Reports, March 2013, No. 1376.

[4] Jun Han, E. Owusu, L. T. Nguyen, A. Perrig and J. Zhang, "ACComplice: Location inference using accelerometers on smartphones," 2012 Fourth International Conference on Communication Systems and Networks (COMSNETS 2012), Bangalore, 2012, pp. 1-9.

How is Privacy Protected?

- Law and policy
- Contract
  - Privacy policy
  - Terms and conditions
- Market Controls
  - The market rewards and punishes based on the preferences of consumers and buyers
- Self-regulation
- Certification
- Best practices
- Technology

FTC Recommendations for Best Practices in IoT

- Conduct a privacy and/or security risk assessment
- Test security measures before launching products
- Incorporate the use of smart defaults, such as requiring consumers to change default passwords during the setup process
- Implement reasonable access control measures to limit the ability of an unauthorized person to access a consumer’s device, data, or network
- Inform consumers about the “shelf-life” of products—how long a company plans to support them and release software and security patches

FTC Recommendations for Best Practices in IoT

- Impose reasonable limits on the collection and retention of consumer data (data minimization).
- Companies should consider de-identifying stored consumer data, publicly commit not to re-identify the data, and have enforceable contracts in place with any third parties with whom they share the data, requiring them to commit to not re-identifying the data as well
- Continue to implement Notice and Choice, that is, providing consumers data use or privacy policies and giving them the ability to agree to or decline data collection

EU Article 29 Working Party (European Data Protection Board) Opinion on the IoT

- Raw data should be deleted as soon as the necessary data has been extracted
  - Developers who do not need raw data should be prevented from ever seeing it
  - The transport of raw data from the device should be minimized as much as possible
- If a user withdraws his/her consent, device manufacturers should be able to communicate that fact with all other concerned stakeholders
- IoT devices should offer a “Do Not Collect” option to schedule or quickly disable sensors
- Devices should disable their own wireless interfaces when not in use or use random identifiers to prevent location tracking via persistent IDs

EU Article 29 Working Party (European Data Protection Board) Opinion on the IoT

- Users should be given a friendly interface to be able to access the aggregate or raw data that a device or service stores
- Devices should have settings to be able to distinguish between different people using it so that one user cannot learn about another’s activities
- Manufacturers and service providers should perform a Privacy Impact Assessment on all new devices and services before deploying them
- Applications and devices should periodically notify users when they are recording data
- Information published by IoT devices on social media platforms should, by default, not be public nor indexed by search engines

Designing for Privacy

- When designing an IoT system we should at least think about privacy:
  - What privacy do we offer to our users?
  - How?
- Privacy implications are often very difficult to predict:
  - One set of data may not reveal much alone, but joined with other datasets it can
- When dealing with personal data we should be even more careful
  - Medical data
  - …
- When collecting data, we have some rules to follow
  - GDPR in Europe
  - Think about possible legal implications of our system