INF226 – Software Security

Håkon Robbestad Gylterud

2019–10–30

Last time. . .

Definition

Information privacy refers to the ability of the individual to control their personal information.

Personal information is any information attachable to a specific (physical) person and includes:

- Name and ID number
- Birtdate and gender
- Residence and location
- Healthcare records
- Political information
- Criminal records
- . . .

What constitutes threats to privacy

- Collection of information
- Aggregation of information
- Dissemination of information

Rights of the individual

According to GDPR the following are the rights of the data subject:

- Right of access
- Right to rectification
- Right to erasure
- Right to data restriction
- Right to data portability
- Right to object

GDPR: Obligations of the controller and processor

Obligations of the controller and processor

Some highlights:

- Data protection by design and by default
- **Security of processing**
- Communication of a personal data breach to the data subject
- Notificatoin of a personal data breach to the supervisory authority
- Data protection impact assessment
- Position of the data protection officer

Fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

Security of processing (article 32)

Taking into account the state of the art (· · ·) the controller and the processor **shall implement** (· · ·) measures (· · ·) including (· · ·):

1. the pseudonymisation and **encryption** of personal data;
2. the ability to ensure the ongoing:
    - **confidentiality**,
    - **integrity**,
    - **availability** and
    - **resilience** of processing systems and services;

(Contratst US gov's "Crypto wars")

3. the ability to restore the availability and access to personal data in a timely manner in theevent of a physical or technical incident;
4. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Notification of a personal data breach to the supervisory authority

In the case of a personal data breach, the controller shall $(\cdots)$

- not later than 72 hours after having become aware of it $(\cdots)$
- notify the personal data breach to the supervisory authority.

Data Protection Officer

The **Data Protection Officer** is meant to ensure that the organization complies with privacy laws:

- Shall have direct communication with organization leaders who make decisions in privacy matters.
- Must perform audits of compliance, and work proactively.
- Protection from being layed-off.

Dark UI-patterns

Report: **Deceived by design** (Forbrukerådet, June 27th 2018).

Analyzed a sample of settings in Facebook, Google and Windows 10.

Dark UI-patterns

Report: **Deceived by design** (Forbrukerådet, June 27th 2018).

Analyzed a sample of settings in Facebook, Google and Windows 10.

“The findings include

- privacy intrusive default settings,
- misleading wording,
- giving users an illusion of control,
- hiding away privacy-friendly choices,
- take-it-or-leave-it choices
- $(\cdots)$”

Tracking

Tracking of peolpe's browsing is done using many different techniques:

- Cookies and web-storage
- HTML5 canvas finger printing.
- "Like"-buttons (even without pressing it)
- Web-beacons
- Analytics software
- Advertisement
- Cross-device tracking (ultra-sonic tracking)

Anti-tracking software: Focussed on blocking network requests to known tracker domains.

Onion Routing

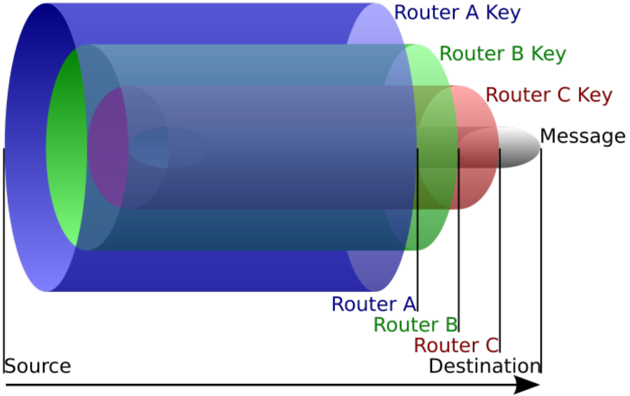
Mix networks

Mix-networks are networks where communication is redirected through several hosts before reaching its destination.

- A mix network is not useful if the data reveals information about source/destinaton

Onion routing solves the problem by using layers of encryption to hide source/destination of the message.

The idea


Router A Key
Router B Key
Router C Key
Message
Router A
Router B
Router C
Source
Destination

Onion routing

In onion routing the messages are wrapped in several layers of encryption.

- Each layer can only be decrypted by a specific relay
- The relay forwards messages to the next relay
- until the message reaches the final destination.

Tor

Tor is an implemenation of onion routing on the Internet.

- A network of nodes
- Three kinds of nodes:
  - Client
  - Relay
  - Out-proxy
- A central directory helps clients construct tunnels.

Attacks on Tor

- Timing attacks
- Browser fingerprinting
- Avoiding the proxy
- Malicious exit nodes
- Vulnerabilities in the browser
- ...

Tor browser

The Tor browser is a hardened version of Firefox, with Tor already set up.

- Designed to reveal as little information as possible.
- Use Tor for all connections.

Hidden services

Some websites, called **hidden services** live entirely within the Tor network.

- The servers running a hidden service are anonymous to their users.
- The users are anonymous to the server.

I2P

I2P is an implementation of anonymity using an onion routing like protocol (called garlic routing).

- Fully distributive and peer-to-peer (no central directory)
- Routing is unidirectional.
- All nodes participate in routing for other nodes.
- Each peer has a fixed number of client tunnels.
- Services have public input tunnels.

Anonymity vs Privacy

The following are different:

- Privacy (control over private information)
- Anonymity (absense of identification)
- Pseudonymity

Anonymity vs Privacy

The following are different:

- Privacy (control over private information)
- Anonymity (absense of identification)
- Pseudonymity

Question

Are there situations (in our everyday lives) where we want privacy, but not anonymity?

Privacy

Increasing use of software raises new privacy issues:

- Tracking people's activities in much more detail.
- Centralisation of data storage.
- New aggregation techniques.

Laws regulating personal information is taking form (GDPR). And users with techniqual know-how can mitigate some of the tracking.