16-124-836
Marcel Matti ZAUDER

Chapter 1

Privacy

PRIVACY concerns information about individuals or groups of people. Those should be able to be hidden or to hide the information of themselves. PRIVACY also allows to release information selectively and for a certain purpose.

1.1 CONTEXT of information

The CONTEXT is defined to be the domain, setting, or the interaction in which information is transferred. Its elements are the people, relationship and trust, traditions, values, purposes and goals, time and place, and laws.

1.2 INFORMATIONAL NORM

The INFORMATIONAL NORM concerns an information flow and is defined by the following five elements:

- sender
- recipient
- subject
- information type (attributes)
- transmission principle (circumstances of the information flow)

This norm can be one of two types:

1. **Normative**
   How the actors should behave
2. **Descriptive**
   Practice of the actors

1.3 CONTEXTUAL INTEGRITY

PRIVACY as CONTEXTUAL INTEGRITY means that an information flow respects the information norm of its context.

Chapter 2

Principles of Computer Security

2.1 Access Control

A Reference Monitor is a logical concept to model if requests from subjects to objects are permitted. The associated policies define the permitted operations for each subject-object pair.

Chapter 3

Tracking

3.1 Active Tracking Methods

3.1.1 Cookies

Because HTTP is stateless a method must be provided to enable continuity and sessions. Cookies address this problem by being set by the servers in a browser saving personalization, logins, and tracking information. The browser sends this cookie with every request it makes to that server.

1st-Party Cookie

Set by the server in URL from which the DOM originates.

3rd-Party Cookie

When DOM includes some information from 3rd-party servers the original server requests this information and the response might contain a 3rd-party cookie which is primarily used for tracking.

3.1.2 Tracking Pixels

Typically 1x1 transparent images included by an external server via the DOM. Most often used on websites or in e-mails.

3.1.3 Identifiers on device or browser

More often used for mobile devices like IMSI, GAID, or IDFA-ID. For desktop PCs this is not very common.

3.1.4 Evercookie

Using other methods for storing a cookie in browsers. The goal is to recreate the same cookie on every visit. For example Flash, local and session storage, or ETags (HTTP element to facilitate coding).

3.1.5 Cookie Syncing

Correlate 1st-party cookies sent by different servers, across domains.
Domain **A** places cookie and makes the browser to include some content from another Domain **B** via personalized URL, which includes the tracking data. Domain **B** can associate this with identifier used by **A**. All domains that are using this cookie merge all data collected individually.

3.2 Passive Tracking Methods

The client doesn't need to take any action. These trackers are not visible on the client and are usually called fingerprinting.

Chapter 4

Data Anonymization

Chapter 5

ϵ-Closeness