Trust and Privacy in IoT

How to design, implement and operate a privacy ensured and trustful IoT – System

Privacy and Trust is a wide field. There are many concepts, technologies, implementations and also regulation and laws outside that are dealing with the privacy of individuals or groups and trust in systems or organizations. Most of the approaches clearly distinguish between personal identifiable information (PII) that can be linked to a certain person and other arbitrary data.

But Privacy and Trust becomes crucial in the Internet of Things because even an arbitrary data, like a temperature might be related to a user when it's combined with other data like location or it is profiled of a certain time period. A very drastic example is the ability to determine what kind of TV-Program a user is watching just from measuring the energy consumption with very frequent probs like described in a paper of Greveler et. Al [1]

The following text is a start to collect basic principles, design strategies or technical methods that can be taken into account while designing a IoT system in order to protect user privacy and in order to increase the trust in a system:

ISO/IEC/IEEE 42010:2011 defines a template where so called concerns are described to frame an architecture viewpoint:

- **Data minimization** – Concerned with collecting, transmitting and processing only a minimal set off data that is really necessary to fulfill a certain function in an IoT system.

  Even if it is sometimes easy to collect "interesting data that can be used "later" for other services keep in mind that these data might be a potential privacy risk when they are leaked or misused.

- **Transparency** – Concerned with providing an overview of data transactions, data access attempts or data process steps conducted by different stakeholders while operating an IoT system.

  It is often necessary to process or transmit data that can be easily linked to a person. But make this very clear to a user. No hidden mechanisms. Be open and state clear what you do with the user data. Transparency is a source for trust in a service or organization.

- **Consent** – Concerned with providing stakeholders means to agree or disagree whether certain (potential sensitive) data are collected, transmitted or processed in an IoT- system.

  User consent is important. In many legislations user consent makes things easier. It enables to process and transmit data. The Kantara Initiative Information Consent & Information Sharing Work Group works on a framework for handling user consent. The idea is to give users means to manage their consent. A user gets a consent receipt. This is an advantage for both users and service providers. The user gets an overview of given consent and can extend or revoke it. A company has a legal safe way to manage and to proof the possessing of user consent.

- **Revocation** – Concerned with means to revoke granted access rights or consent

  Once Access rights are granted there should be also a way to revoke this right. This lets the user in control of the process.

- **Intervene** – Concerned with providing means to interrupt or stop collecting, transmitting and processing any data at any time.

  This is a kind of red button.

- **Aggregation** (over time, over sources) – Concerned with providing the possibility to aggregate traces over a certain time or certain sources before transmission or processing and thus to hide detailed information.

  Aggregation is a very important method.

- **Anonymity** – Concerned with providing means to transmit or process data without revealing the identity of the receiver or/and the recipient.

- **Pseudonymity** Concerned with using and managing other identifier than real names

- **Unobservability** – Concerned with providing means to disguise to an observing parties the transmission of data.

- **Unlinkability** – Concerned with providing means to disguise that two or more entities or even messages belonging together.

- **Deletion of Data** – Concerned with providing stakeholders with the ability to delete all data belonging to a certain device, user or service on demand or automatically as soon as they are not needed anymore

Trust related concerns:

- **Identity proofing** – Concerned with trusting a certain identity by proofing that it was authenticated according to a certain level of confidence.

- **Trust elevation** – Concerned with adapting the level of confidence in an identity according to a required level

- **Compliance** – Concerned with trust in complying with data protection legislation.

- **Data Ethics** – Concerned with handling data in privacy ensured way going further than just being conform ?.

- **Data usage** – Concerned with using data just for an intended purpose.
- **Data integrity** – Concerned with using data that are not changed during the transmission process.

[1] Ulrich Greveler, Benjamin Justus, and Dennis Loehr, “Multimedia Content Identification Through Smart Meter Power Usage Profiles“