Master

Security- und Privacy-Anforderungen für Health Data Intelligence Systems

Security and Privacy Requirements for Health Data Intelligence Systems

Motivation — English

To cope with widespread crisis situations such as the Corona pandemic, local action with overarching regulations has proven to be an effective strategy. Data is collected and processed in a decentralized manner. Public data on the incidence of infection, but also non-public health data on individual persons are processed by artificial intelligence methods. Since some of the data involved is highly sensitive data is processed and transmitted, especially in the internal and external relations of the BOS. There are high data protection and data security requirements for the associated trustworthy data-intensive systems. Developing such systems at short notice poses a particular challenge to those involved. Consequences of this could be observed at the beginning of the Corona pandemic in Germany: e.g., high development and and maintenance costs for the Corona warning app[1] or data protection concerns[2] despite good data protection in the Corona warning app[3].

Although this type of systems has common concerns regarding privacy and security, currently no common set of requirements is known and no reference architecture exists. The goal of this thesis is to propose a reference architecture for health data intelligence, that support their specific privacy and security requirements. You will therefore identify the privacy and security requirements from relevant sources for health data intelligence systems. These requirements will have their effect on all levels such as processes, architectures and applications. You will survey the concrete privacy and security requirements, considering data sources and flows, data, data processing locations and steps with relevant attack scenarios on these types of systems.

We provide the following research questions:

- RQ 1: Which are the relevant sources for privacy and security requirements for health data intelligence systems?
- RQ 2: What are common privacy and security requirements for health data intelligence systems?
- RQ 3: What are potential types of attack considering the identified requirements?
- RQ 4: How can these requirements be considered in a reference architecture?

Knowledge required to carry out the work: None special needed
Helpful knowledge: Requirements Engineering, Health Domain, Software Architecture

Organisatorisches

Kontakt:
Dr. Marco Konersmann <konersmann@uni-koblenz.de> (Main Contact)
Dr. Qusai Ramadan<qramadan@uni-koblenz.de>

Literatur

[1] As introduction: The “Regulation” Section of Wikipedia’s topic “Artificial Intelligence in Healthcare” `https://en.wikipedia.org/wiki/Artificial_intelligence_in_healthcare#Regulation`

[2] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data,

[1] `https://www.tagesspiegel.de/wirtschaft/69-millionen-euro-warum-die-corona-warn-app-so-viel-kostet/25929302.html`, accessed 2020-11-03

[2] `https://www.zeit.de/digital/2020-07/corona-warn-app-technische-probleme-vertrauensverlust-gesundheitsschutz-corona-eindaemm` accessed 2020-11-03

[3] `https://www.haufe.de/compliance/recht-politik/orten-von-corona-infizierten-per-app-und-datenschutz_230132_511524.html`, accessed 2020-11-03

and repealing Directive 95/46/EC (**General Data Protection Regulation**) https://eur-lex.europa.eu/eli/reg/2016/679/oj

[3] ITU/WHO Focus Group on "Artificial Intelligence for Health" https://www.itu.int/en/ITU-T/focusgroups/ai4h/Pages/default.aspx