Identity Management and Authorization Infrastructure in Secure Mobile Access to Electronic Health Records

Supervisor: P. Fazendeiro   Co-supervisor: A. Ferreira

1   Abstract

Data related to health information systems are highly sensitive and subject to severe legal and regulatory restrictions that aim to protect the individual rights and privacy of patients and healthcare data custodians. To do this there is the need to provide the individual with a trusted digital identity composed of a set of personal data attributes that can be used to characterize a user.

The smartphone is recognized as essential for enhancing security and privacy and research has proved it plays a crucial role on more flexible user-centric architectures.

In a nutshell, we will address an interesting challenge in healthcare, which is to provide data transparency while still keeping it private by guaranteeing its socio-technical security, i.e., closer to the owner, reflecting policy and regulatory requirements, as well as providing for its integrity, verifiability and usability within cloud and big data paradigms.

The ongoing challenge is to propose a real time user-centric aggregation identity management and authorization infrastructure implemented within smartphones which are currently recognized as essential for enhancing security and privacy as well as providing flexible user-centric architectures, where it is vital to employ stronger cryptographic mechanisms.

2   Objectives and Tasks

T1 Review of the related literature

T1.1 Access control to electronic health record (EHR) data

T1.2 Identity management and authentication

T2 To collect the requirements and define system's architecture

T3 Identification of security requirements, threats and vulnerabilities regarding the access to Personal/Electronic Health records in a Health Records System via Smartphones

T4 Development of a mobile application's prototype addressing the identified security concerns

T5 Integration, test and validation of the approach

T6 To write up a MSc thesis and a scientific paper

3   Timetable

T1.1 1 month

T1.2 1 month

T2 1 month

T3 1 month

T4 1 month

T5 2 months

T6 2 months

4   Expected Results

- 1 journal paper

- 1 MSc thesis

5   References

Ram Krishnan. Access Control and Privacy Policy Challenges in Big Data. NSF Workshop on Big Data Security and Privacy. 2014.

Mont, Marco; Pearson, Siani; Bramhall, Pete; Towards Accountable Management of Privacy and Identity Information: Computer Security ESORICS; Lecture Notes in Computer Science; Springer Berlin / Heidelberg; Isbn: 978-3-540-20300-1; page:146- 161; Volume: 2808. 2003.

Ana Ferreira and Gabriele Lenzini. Can transparency enhancing tools support patients accessing electronic health records? 3rd World Conference on Information Systems and Technologies. Advances in Intelligent Systems and Computing, 2015. 353: 1121-1132.