Cryptographically Strong Authorization and Identity Management in eHealth Portals

Daniel SLAMANIG\textsuperscript{a,1}, Christian STINGL\textsuperscript{a}, and Thomas KURMANN\textsuperscript{a,b}

\textsuperscript{a} School of Medical Information Technology, Carinthia University of Applied Sciences, Klagenfurt, Austria

\textsuperscript{b} Siemens AG Austria, Department of Medical Solutions NLG, Graz, Austria

Keywords: eHealth, Security, Cryptography, Privacy, Archival-repository systems for medical records-EPR-CPR-EMR, Identity Management

In recent years many countries have installed eHealth initiatives and working groups in order to develop strategies to harmonize the exchange of health related information using open environments. A central aspect of eHealth is called the electronic healthcare record (EHR) which integrates all relevant medical information of a person. Considering eHealth, one can recognize an alteration to a patient centric approach of health care. This is accompanied by the fact that privacy of patients is of utmost importance in many European countries, e.g. Austria, Germany, etc. Hence, these EHRs should be moderated by the patients themselves or a confidant of the patient (e.g. relative, general practitioner). By virtue of their sensitive character it is crucial that medical data can only be accessed by the patient herself and persons who are directly involved in the treatment of the patient. Since eHealth portals are available on the Internet, additional privacy issues arise that have to be considered carefully. In order to protect privacy, transmission encryption is often considered to be sufficient. However, an internal attacker (insider) or a hacker can easily acquire plaintext data even if transmission encryption is used. Therefore, documents need additionally to be encrypted at the application layer to prevent unauthorized access to the content of the documents at the eHealth portal. Since an eHealth portal constitutes a central access point we want to point out there exist additional attacks which can expose potentially compromising data of a person. It must be emphasized that even if content encryption is used the sole observation of the metadata of an eHealth portal can violate the privacy of users, and thus, there emerges the need for methods that improve the user’s privacy. Especially when considering the metadata of a system there exist possible attacks and privacy aspects which are either rarely discussed or not discussed at all in the literature so far. Besides, since the EHR of a person can be accessed time and location independent a person can be asked or even forced to present it, e.g. at a job interview. Although the enforced disclosure would be illegal the disclosure attack could be highly realistic in our opinion. In this work we present a novel concept of identity management that helps to reduce utilizable metadata and thus enormously improves the patient’s privacy. It must be mentioned, that the security of this concept does not depend on any trust assumptions in the provider and is provably secure.

\textsuperscript{1} Corresponding Author: Daniel Slamanig, Carinthia University of Applied Sciences, Primoschgasse 10, 9020 Klagenfurt, Austria. E-Mail: d.slamanig@cuas.at