University of Southern California

CSCI531 Applied Cryptogrophy
Final Project

EHR Audit System

Student: Hallgrimur David Egilsson
USC ID: 6059-2639-79

Professor: Dr. Tatyana Ryutov

April 25, 2022

I have read the Guide to Avoiding Plagiarism published by the student affairs office. I understand what is expected of me with respect to properly citing sources, and how to avoid representing the work of others as my own. The material in this paper was written by me, except for such material that is quoted or indented and properly cited to indicate the sources of the material. I understand that using the words of others, and simply tagging the sentence, paragraph, or section with a tag to the copied source does not constitute proper citation and that if such material is used verbatim or paraphrased it must be specifically conveyed (such as through the use of quotation marks or indentation) together with the citation. I further understand that overuse of properly cited quotations to avoid conveying the information in my own words, while it will not subject me to disciplinary action, does convey to the instructor that I do not understand the material enough to explain it in my own words, and will likely result in a lesser grade on the paper.

Signed: Hallgrimur David Egilsson

1 Workspace

For simplicity of this PoC (Proof of Concept) the system will only support 5 hard-coded patients and 2 hard-coded audit companies. The patients in the systems will be:

Alice, Bob, Carol, David, Eve

The first audit company is USC and should be able to audit the EHR records of Alice, Bob and Eve.

The second audit company is UCLA and should be able to audit the EHR records of Carol and David.

Python pajsonckage setup follow recommendations at: https://packaging.python.org/en/latest/tutorials/packaging-projects/

EHR id generation: * Explain the chance of generating two ids that are the same.

Database file: * current: linux/ MAC OS lockin with /tmp/ehr_db.json

EHR REST API: * POST data should always be in application/json

User IDs are just names for simplicity, we assume everyone has a uniqe name.

2 Introduction

3 System architecture

Describe the system components (e.g., authentication server, audit server, etc.), their functionality, and communication patterns. Clearly describe how your system meets the five goals discussed above.

4 Cryptographic components

discuss appropriate choice of specific cryptographic primitives to ensure the system supports the goals outlined above.

Describe the concrete encryption schemes and key management approaches to be used in your system

5 Limitations of the system

Which challenges were not addressed?

6 Example section

Example citation [1]

6.1 Example subsection 1

6.2 Example subsection 2

References

[1] C. Neuman, "Challenges in security for cyber-physical systems," in *DHS workshop on future directions in cyber-physical systems security*, pp. 22–24, Citeseer, 2009.