CSCI 531 Spring 2022 Semester Project

Designing a Secure Decentralized Audit System

1. The nature of the assignment

The semester project gives each student the opportunity to use and illustrate the concepts from the course in an applied manner. Based on information you gather and review, you are to report your design, analysis, and prototype of a secure electronic voting system.

In this project, you will have an option to either concentrate more on the on the detailed design of the system or on the implementation of the system prototype.

In not less than 7 and no more than 10 pages prepare a report in PDF format with a font size between 10 and 12. Figures, tables, screenshots and the like are not included in the 10-page maximum page count, but text beyond the 10-page limit will not be considered in grading. There are no specific requirements related to the formatting of your report. Submit the report and your code in electronic form on DEN D2L.

2. Project description

Electronic health record (EHR) systems have gradually replaced traditional paper-based health record systems in the United States. Audit logs serve multiple functional and regulatory purposes in EHR systems. When patient records are accessed for some reason, the history of all such events must be recorded in a log file for later audit on access histories. The log file is used for reconstructing the past state of medical records, and it can be used as a legal evidence in medical malpractice cases.

Your job is to produce design and prototype a system that meets the following goals:

1. *Privacy*. Patient privacy should be maintained. Unauthorized entities should not be able to access audit records.

2. *Identification and authorization*. All system users must be identified and authenticated. All requests to access the audit data should be authorized.

3. *Queries.* Authorized entities should be able to query audit records.

4. *Immutability*. No one should be able to delete or change existing audit records without detection. Any modifications/deletions of the audit records should be detected and reported.

5. *Decentralization*. The system should not rely on a single trusted entity to support immutability.

The description of the system is deliberately underspecified so that you have the intellectual freedom to consider various possibilities for how such a system should operate.

Some useful references are listed on the last page. You may use web sites and other aids to help you with this project, be sure to list your references in your report.

3. Deliverables

Based on information you gather and review, you are to report the design and prototype of a secure decentralized audit system.

This project will let you explore the implementation of software for a simplified electronic audit system. Limit your system to just five patients and two audit companies who attempt to access the audit data.

You do not need to implement a component that guards access to EHR data and generates the audit data when the EHR data is accessed. You can assume that the audit data is given in clear (unencrypted) as input to your system. Audit record content includes:

- Date and time of logged event
- Patient ID whose record was accessed
- User ID who performed the logged event
- Action type (create, delete, change, query, print, or copy)

Implementation of a practical audit system should be scalable and distributed and run over the network. However, we do not expect everyone interested in applied cryptography to have network programming experience. For that reason, your implementation can run on a single machine and we do not require socket programming. Message exchange can be implemented by writing and reading to/from a file. You can implement the required functionality as a library that can be called from a client or a server. However, you need to implement client and server stubs to demonstrate the required functionality.

You need to prototype some of the system components discussed in your system design. You can use a programming language of your choice. You are also allowed to use code developed by others.

You must clearly specify which parts of your implementation were developed by you and which parts you acquired from some sources (e.g., GitHub). You must provide explicit references to the code you obtained from the external sources (including all imported packages) as well as description of functionality the external code implements. Do not use any proprietary code in this project!

Required prototype implementation:

- Implement routines that support “Privacy” goal. In particular, confidentiality and integrity protection of sensitive data in transit and at rest.
- Implement routines to support “Queries” goal. Patients can query the system to monitor usage of their EHR data. Audit companies can query the system to monitor usage of HER data for a set of patients.
- Implement routines to support “Immutability” goal. Demonstrate how your system enforces immutability buy implementing a scenario where an attacker tampers with some audit data and the system reports the attack. For this task just detection of tempering is enough.

You must provide a comprehensive written description of the design of your system. The report should include the following:

- **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.
- **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.

You must provide a detailed written description of the design of your programs and a screen capture of a session demonstrating that your programs work. Clearly explain how your programs can be executed, describe expected inputs and outputs.

Finally, you need to describe limitations of your system. In particular, discuss security challenges were not addressed.

You can choose one of the two options to complete the project:

1. Explore applicability of various cryptographic schemes (e.g., homomorphic encryption, zero knowledge proofs, etc.) to improve the system security properties.

2. Implement extended prototype. In particular:

   - Implement routines to support “Identification and authorization” goal.
   - Implement routines to support “Decentralization” goal.

You need to decide which of the two options you prefer by March 15th. If you chose option 1, you have to describe your plans: submit a one-page description the topics you plan to explore along with the preliminary references.

4. Grading

You need to demonstrate that your proposed system meets the outlined requirements. Clearly state your assumptions and discuss limitations of the system. We will not require rigorous proofs of correctness.

The total of 100 points for the project will be allocated to four areas as follows:

1. [20 points] System architecture.
2. [30 points] Discussion of cryptographic components.
3. [40 points] Prototype implementation.
4. [10 points] Discussion of assumptions and system limitations.

Completion of the semester project is to be an independent, individual effort for each student. Communication with fellow students for this assignment, attempting to benefit from work of another student, past or present and similar behavior that defeats the intent of an assignment is unacceptable to the University. Such behavior will be treated as a violation of USC academic integrity standards, which are summarized in the on-line tutorial available at http://www.usc.edu/libraries/about/reference/tutorials/academic_integrity/index.php

References

Charalampos Stamatellis, Pavlos Papadopoulos, Nikolaos Pitropakis, Sokratis Katsikas, William J Buchanan, A Privacy-Preserving Healthcare Framework Using Hyperledger Fabric, arXiv - CS - Cryptography and Security, 2020.

D Tith, JS Lee, H Suzuki, W Wijesundara, N Taira, T Obi, N Ohyama, Application of Blockchain to Maintaining Patient Records in Electronic Health Record for Enhanced Privacy, Scalability, and Availability, Healthcare Informatics Research 26 (1), 3-12, 2020.

M. M. Madine et al., Blockchain for Giving Patients Control Over Their Medical Records, in IEEE Access, vol. 8, 2020.