University of Detroit Mercy
College of Engineering and Science
Department of Mathematics, Computer Science and Software Engineering

CSC-4540 Computer Security - Term Project-

Applying Cryptology to E-Visit

E-Visit is an interaction between a physician and a patient with regards to minor health problems. E-Visit is available 24 hours a day. Patients could ask their doctors questions regarding their health and obtain test results. The patient will contact a nurse online who verifies her/his information and then a doctor will interact with the patient. A number of problems exist here. The patient should ensure that she/he is connected to a nurse or a doctor but not intruders. The nurse and the doctor should also be convinced that they are interacting with a valid patient. There are also problems of accessing patient records which demands privacy. In this project, you are required to specify how various areas of Cryptology could be applied to E-Visit Security requirements. You are supposed to cover at least the following:

Project Plan

1. Collect and read a number of papers on E-Visits and Patient Records Security and Privacy including the Health Insurance Portability and Accountability Act (HIPPAA)
2. Specify Security/Privacy Requirements for E-Visit Systems
3. Validate these Requirements
4. Devise E-Visit Protocols (Cryptology Protocols) to meet the Security Requirements

Example[†] (Voting System)

The protocol for the security requirement "**Only authorized voters can vote**" is as follows:

1) Each voter encrypts her/his vote with the public key of a Central Tabulating Facility
2) Each voter sends her/his vote in to the Central Tabulating Facility
3) The Central Tabulating Facility decrypts the votes, tabulates them, and makes the results public

Deliverables

All your findings should be documented in a report. The report should be organized as follows:

Title page
Abstract
Chapter 1: Introduction
- E-Visit Systems

- security requirements
- cryptology areas needed for the project

Chapter 2: E-Visit Security/Privacy
Chapter 3: Security Requirements for E-Visits
Chapter 4: Application of Cryptology to E-Visit Systems
Chapter 5: Implementing E-Visit Protocols
Chapter 6: Conclusion
Chapter 8: Future Extensions
References

† *Bruce Schneier, Applied Cryptology, Second Edition, Wiley, 1996.*