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

CSSE-5700 Computer Security - Term Project-

Applying Cryptology to Vehicle Infotainment System

Vehicle Infotainment Systems deliver entertainment and information content. Some tasks that can be carried out by in-vehicle infotainment system include controlling and playing audio content, providing navigation, furnishing rear-seat entertainment, such as movies, games, and social networking, sending and receiving SMS text messages, making phone calls, and acquiring traffic conditions, sports scores and weather forecasts. In this project, you are required to specify how various areas of Cryptology could be applied to secure vehicles' Infotainment Systems.

Project Plan

1. Collect and read a number of papers/articles on Vehicle Infotainment Systems and their Security
2. Devise Security Requirements for Vehicle Infotainment Systems
3. Validate these Requirements
4. State the security protocol in natural language as in the example below.
5. Devise Vehicle Infotainment Systems security protocols (Cryptographic Protocols) to meet the Security Requirements.

Example† (Voting System)

The protocol for the security requirement "**Only authorized voters can vote**" is written 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

- Vehicle Infotainment Systems Systems

  - Security requirements
  - Cryptography areas needed for the project

Chapter 2: Vehicle Infotainment Systems Security
Chapter 3: Security Requirements for Vehicle Infotainment Systems
Chapter 4: Implementing Vehicle Infotainment Systems Protocols
Chapter 5: Conclusion
Chapter 6: Future Extensions
References

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