Abstract—Smart card are a secure way of transferring data, but security has not been properly handled in numerous applications, such as in public transportation systems. In this project, a methodology to reverse engineer and detect security flaws has been practiced. Specifically, the protocol of a smart card was analyzed. By applying the methodology with a tool, it was possible to access private information to capture tag-reader communications, and even emulate both tags and readers.

Introduction

Smart cards are tiny plastic cards with a microprocessor chip inside that can store and process data. These cards are used for electronic payments, access control and authentication. The microprocessor chip on the smart card is used to handle tasks such as encryption, creating of digital signatures and for securing the data. The smart card communicates with the card readers by contact or contactless interfaces by which the transfer of data is possible. Also, they provide a second level of authentication and protection, so they are used for security purposes for the protection of data. These smart cards are used in sectors like healthcare, transportation, banking etc. as they can securely store and transfer data such as medical records, tickets used in transportation, credit card numbers etc.

Diagram

Description automatically generated