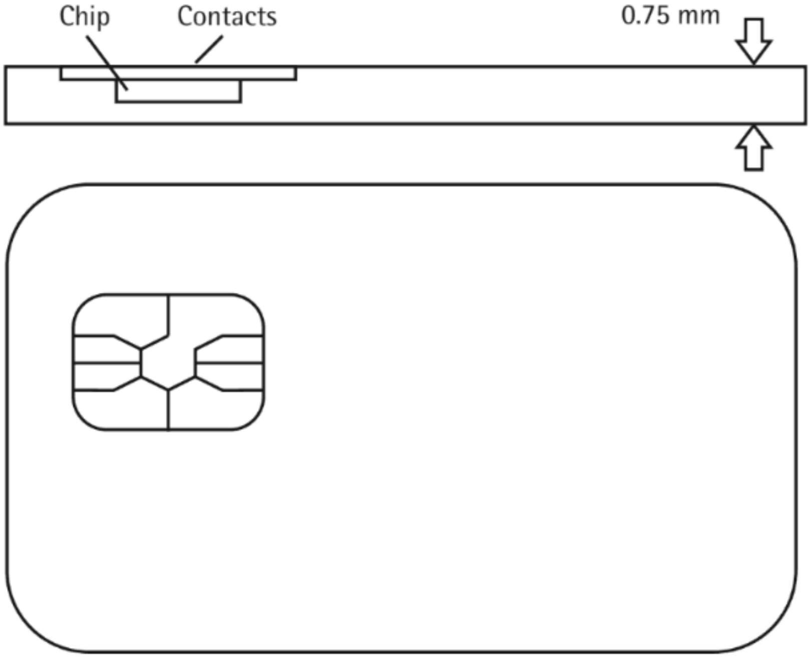
Abstract—Smart card are a secure way of transferring data, but security has not been properly handled in numerous applications, such as in public transportation systems. In this project, a methodology to reverse engineer and detect security flaws has been practiced. Specifically, the protocol of a smart 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.



Although smart cards are a secure method of data transport, they are susceptible to many dangers. Smart card security may be threatened by several factors, including logical and physical attacks like malware and tampering and cloning. Smart card technology may also be vulnerable due to problems with the creation, use, or administration of the cards.

Many countermeasures, like as encryption, authentication protocols, access control systems, and physical security measures, can be used to minimise these dangers and vulnerabilities. Furthermore, it is possible to create and use smart card operating systems and apps to lower the danger of assaults.

Reverse engineering examines the transmission between the smart card and the reader or host device at the protocol level. This can be accomplished through the use of passive or active techniques like eavesdropping, message interception, modification, or injection. The smart card application protocol data unit (APDU), the common means for exchanging data between smart cards and readers, can be revealed using these techniques in terms of its structure, content, and semantics. These techniques, though, are dependent on the implementations, standards, and protocol specifications, and they can be stopped by security mechanisms like authentication, encryption, and integrity checking.

The protocol level of smart card technology is how the smart card and the reader exchange data using the application protocol data unit (APDU) format. There are different types of contacted and contactless intelligent card protocols, such as T=0, T=1, Type A, Type B, etc. These protocols define the physical interface, transmission mode, error detection, and anti-collision methods. Standard protocols ensure interoperability and security, while proprietary protocols may have some advantages or disadvantages.