CPSC 4200: Midterm Project Report

Ben Joye, Reagan Leonard, William Shope
Dr. Cheng

Literature Review

As per our project proposal, we set out to complete the literature review by October 16th. We completed this on the 18th, so we were running about two days behind in completing that. From this literature review, we have researched topics such as:

- Magstripe/chip history
- Magstripe functionality/weaknesses
- EMV chip card functionality/weaknesses
- Chip card global adoption
- Breaches of both types
- Etc...

Our pool of information comes from a total of over 30+ resources, and we will pick and choose from these resources which we would like to include in our research paper.

Paper

With our paper, we were planning on completing the rough draft of it by October 31st. We are roughly 40-50% complete in finishing it, and we have completed sections such as:

- Introduction
- General Information on Topic
- Relevance of Topic in Modern America
- Security Design of the Magstripe Card
- Security Design of the EMV Chip Card
- Rise of the EMV Chip Card
- Analysis of Fraud Data from Before vs. After EMV Chip Card

Introduction

From the inception of credit cards, security and fraud have always been a major issue. Since October 2015 in the United States, EMV chips have been required to be accepted by businesses or else they would be held liable if any fraudulent activity occurred [3]. This is because EMV chips in cards provide significantly more security than their chipless counterparts. Without a chip, thieves are able to steal card information very easily. Magstripe cards hold their data statically, and anyone with a magstripe reader is able to store that data and write it onto a blank card, creating an exact copy. Chips, however, uniquely encrypt the information on every transaction, which makes it much harder to intercept the data [4].

There are two main reasons why EMV cards are superior in terms of security to the classic magnetic-stripe cards that have been around since the 1960s: 1) fraudulent cards with EMV chips are much more difficult to make than fraudulent cards with magnetic stripes and, 2) "the data on chip cards is constantly changing making it extremely hard to isolate and extract" [1]. For obvious reasons, it is much more difficult for a thief to manufacture a fake chip card than one with a magnetic stripe, simply because of the hardware involved; they would need to manufacture the chips.

General Information on Topic

The origins of what has come to be known as the modern-day credit card began in 1946. A banker named John Biggins created the "Charg-It" card in Brooklyn, NY [5]. Any purchases made with a Charg-It card were forwarded to the bank Biggins owned. The bank then reimbursed the merchant and obtained payment from the customer. This model of triangular

Magnetic stripes, meanwhile, are simply what they sound like: a magnetized section of the card that essentially holds the card's ID number. This can be recreated much more easily than a chip because of the hardware involved in a chip. Furthermore, the software that a chip brings to the table—the sophisticated encryption that occurs on each and every transaction—provides another added level of protection to the cardholder that has made the EMV chip the obvious world leader in card payment technology [2]. This has inspired the electronic payment world to take a deeper look into how we can make e-payment even more secure through further innovations in card technology; NFC payment, and online payment via private applications.

Overall, this project will address the differences between the EMV chip card and a credit card with a magnetic strip and then transition to the remaining security vulnerabilities as well as potential solutions to those vulnerabilities. This will be done by conducting a thorough literature review from which these security vulnerabilities will be identified. One of these solutions that we devise will be extensively reviewed and form the main basis of the following scientific paper.

transactions was subsequently known as the "closed-loop" system. In the beginning phases of these types of cards, purchases could only be made locally and only bank customers could obtain a Charg-It card. Then, in 1951, Franklin National Bank, also out of New York, issued its first charge card to its loan customers [5].

Several years later, in 1958, American Express, which is now one of the largest and most successful credit card companies in the world, launched its first

credit card. In the years that followed, American Express would prove itself as one of the global competitors in this newly discovered credit card market. In 1959, they introduced the world's first plastic credit card, which quickly made the existing cardboard and celluloid cards obsolete. Five years later, there were over 1 million American Express cards in circulation and they were accepted at over 85,000 merchants, both in the U.S. and abroad [5].

Back when using credit cards was still a very manual ordeal, the process of paying for something with a card was much more intricate than it is nowadays. In order for a transaction to be completed, the merchant would call the cardholder's bank, then the bank would call the credit card company. Then the credit card company would have to have an employee manually look up the customer by name in order to check their available credit balance. This

was bound to be replaced by something more technologically advanced in the future. Of course, it was made obsolete by a computerized version of this process in 1973 which was designed and implemented by the first CEO of Visa, Dee Hock. Once this process was handled by computers, the transaction time went from an arduous several minutes to being able to be completed in under a minute.

Relevance of Topic in Modern America

As you can see from the description of the rise of the modern credit card, we have certainly come a long way in the innovation of credit card usage. We have also come a long way in the security of electronic payment. However, this does not mean that we do not still have a long way to go in improving the security of credit card

We plan to continue working on this and finishing the paper by the 31st so we can peer review each of our member's contributions to the paper.

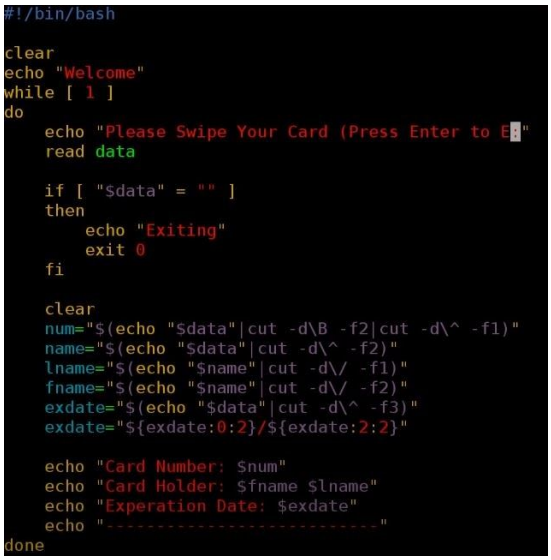
Hands-on Aspect

Our plan for a hands-on activity to go with our paper is to use a magstripe card reader with a usb connection so that we can connect it to our laptop. Our next step is to write a linux bash script that can parse the card's data to show how easily credit card fraud can be done with things like a fraudulent card reader placed over a gas station's card insertion.

We will show how the information could be reused for future purchases, and then explain how a chip card would prevent this.

Pictured below is the usb card reader that our group has purchased:

This is an example of a bash script that we can write to extract the user data:



```
#!/bin/bash

clear
echo "Welcome"
while [ 1 ]
do
    echo "Please Swipe Your Card (Press Enter to E:"
    read data

    if [ "$data" = "" ]
    then
        echo "Exiting"
        exit 0
    fi

    clear
    num="$(echo "$data"|cut -d\B -f2|cut -d\^ -f1)"
    name="$(echo "$data"|cut -d\^ -f2)"
    lname="$(echo "$name"|cut -d\/ -f1)"
    fname="$(echo "$name"|cut -d\/ -f2)"
    exdate="$(echo "$data"|cut -d\^ -f3)"
    exdate="${exdate:0:2}/${exdate:2:2}"

    echo "Card Number: $num"
    echo "Card Holder: $fname $lname"
    echo "Experation Date: $exdate"
    echo "--------------------------"
done
```