SafePay: Protecting against Credit Card Forgery with Existing Magnetic Card Readers

Yinzhi Cao[†], Xiang Pan[‡] and Yan Chen[‡]
[†] Lehigh University, Bethlehem, PA
[‡] Northwestern University, Evanston, IL

Abstract—**Existing magnetic cards adopt plain text to store confidential information, thus being vulnerable to an untrusted credit card reader or a skimming device. To tackle the problem, researchers have proposed several new techniques such as integrated circuit card (IC card) and mobile wallet applications [1]; however, none of them can support existing magnetic card readers thereby facing backwards compatibility issue.**

In this paper, to combat such credit card information leakages and remain backwards compatible, we propose SafePay, a system that transforms disposable credit card information to electrical current and drives a magnetic card chip to simulate the behavior of a physical magnetic card.

We have implemented a prototype system of SafePay by a mobile phone and a prototype magnetic card chip. In the evaluation, we show that the current cost is about $0.5 excluding the phone, and the cost can be even lowered if manufactured in large scale. We also evaluated the prototype in experimental environment such as oscilloscope and real-world scenarios such as vending machines. The results show that the physical signal in oscilloscope is the same as the theoretical value, and meanwhile, we can successfully buy products in all the tested real-world scenarios.

I. Introduction

Existing magnetic credit cards adopt plain text to store all the confidential information, thus being vulnerable to an untrusted magnetic card reader[1]. For example, as reported by New York Times on October 2012, attackers have stolen customers' credit card information at 63 Barnes & Noble stores by hacked credit card readers [2]. For another example, in November 2013, credit and debit card information of 70 million customers has been stolen during a large-scale data breach of Target stores [3]. Meanwhile, it has been reported that fake credit card readers have been used by illegal merchants in China to steal customers' credit card information [4]. In total, as reported by the analyst firm Aite Group, the incurred loss of such cases in the U.S is huge, adding up to over $8 billion dollars per year [5].

To deal with the credit card information leakage problem, researchers have proposed using integrated circuit (IC) cards [6], also known as Europay, MasterCard and Visa (EMV) cards, with strong security authentication to replace the old magnetic cards. However, IC cards face backwards compatibility issues, and therefore all existing IC cards still have a magnetic stripe on it to maintain backwards compatibility. Consequently, a malicious merchant can simply inform the customer the absence of IC card readers, force him to use the magnetic strip on IC cards, and steal credit card information. Moreover, attackers can still use skimming devices to steal customers' information from places where IC card readers are not installed [7], or gain access to systems where chip technology is not deployed, *e.g.*, hotel room key system and subway fare system [8].

Besides IC cards, people have also proposed mobile wallet applications [1, 9]–[13] with new techniques, such as QR codes and Near Field Communication, for financial transactions. However, such technology is even less adopted than IC cards, and it is costly[2] and time consuming for the merchants to make changes. As quoted from a Wall Street Journal article [14] on April 2013, "mobile wallets can make things a lot simpler for shoppers. But they can leave retailers confused".

Therefore, we believe that a striking solution to the problem should address the following **challenges**:

- **Leakage Resilience.** A new solution should prevent information leakage through a fake magnetic card reader or a skimming device plugged into a legitimate reader.
- **Backward Compatibility and Low Cost.** A new solution should be compatible with the existing magnetic card readers. Meanwhile, a new solution should impose low cost to banks, merchants, and credit card holders.
- **User Friendliness.** A new solution should be easy to use without special knowledge.

In this paper, we propose SafePay, our novel technique protecting users' credit card information and being compatible with existing magnetic card readers. The whole system has a bank server application, a mobile banking application and a magnetic card chip. First, the user downloads and executes the mobile banking application communicating with the bank server. Then, during transactions, the mobile application acquires disposable credit card numbers from the bank server, generates a wave file, plays the file to generate electrical current, and then drive the magnetic card chip via an audio jack or Bluetooth. To address the aforementioned challenges, we have the following components:

- **Disposable Credit Card Information.** Disposable credit card information, also known as virtual credit card number, expires after a limited time or number of usage (*e.g.*, one

[1] In this paper, if not otherwise stated, a card reader or a credit card reader refer to a magnetic credit card reader.

[2] "It can often run around $200 for a QR-code reader and $100 for an add-on to an existing terminal for Near Field Communication, says Chris Gardner, co-founder of Paydiant." [14].

time). Even if the information is leaked to an attacker, he cannot further utilize it for future transactions. Such techniques have been adopted by existing systems like EntroPay [15] and PayPal [16] to protect online transaction.

- **Magnetic Credit Card Chip.** Magnetic credit card chip serves the same functionality as a magnetic card stripe on a physical credit card. Therefore, it is completely backwards compatible with existing readers. In the evaluation, we show that the cost of magnetic card chip is about $0.5, and the price could be even lower if manufactured in large scale.
- **A Mobile Banking Application.** To make the whole system user friendly, we make a mobile application to connect with the magnetic credit card chip via an audio jack or Bluetooth. The mobile application automates all processes communicating with the bank and the chip. In the evaluation, we successfully perform several real transactions using all components of SafePay in real-world scenarios such as a vending machine.
- **A Proxy Support.** To protect a credit cardholder with a card issued by a bank that does not adopt SafePay, we also provide a proxy support that relays the communications between the cardholder and the bank.

Broadly speaking, our SafePay is related to Cyber-Physical System (CPS), a system consisting of computational elements controlling physical entities. The computational elements in SafePay consist of a mobile device and a server or a proxy distributing disposable credit card numbers. Meanwhile, the physical entity is the magnetic credit card chip controlled by the mobile application residing in the mobile device.

The rest of the paper is organized as follows. We introduce the background of credit card in Section II and then our threat model in Section III. Overall architecture and server-side deployment model are given in Section IV. Next, we present the design of SafePay in Section V ,prototype implementation in Section VI, and security analysis in Section VII. SafePay is evaluated in Section VIII. Some questions and related works are discussed in Section IX and X respectively. In the end, the paper concludes in Section XI.

II. Background

In this section, we introduce the background of credit cards from two aspects: physical layer format and stored data format.

Physical Layer Format. The physical layout of a magnetic stripe on a credit card is similar to the one on a magnetic tape, consisting of a sequence of magnetic particles. Each magnetic particle is a tiny magnetic bar with its axis of magnetization parallel to the magnetic stripe, facing either right or left. To store data on the stripe, the direction of those tiny magnetic particles are changed based on the stored value by a magnetic stripe data encoder.

When the credit card is swiped over the credit card reader, the header of the reader can sense each of the tiny magnetic fields produced by magnetic particles and a current will be generated. The direction of the current will change, if a magnetic reversal, *i.e.*, the north pole of a magnetic particle next to another magnetic particle's north pole or vice versa, is sensed.

Data Format. A magnetic card consists of three tracks. Only track 2 is used during credit card transaction, and therefore introduced in the paper. Track 2 use four-bit binary-coded decimal (BCD) data format plus a fifth bit odd parity to encode data. For example, a sequence of four zeros and a parity bit one means a digit 0.

Track 2 starts with a sentinel, a fixed ";" character, followed by a primary account number up to 19 digits of the credit card holder. The primary account number consists of a six-digit issuer identification number (IIN) denoting the bank, an individual account identifier of up to 16 digits, and a single check digit by the Luhn algorithm [17]. Then, a field separator "=" follows. The information after the separator shows some additional data such as expiration date and bank specific information. An end sentinel "?" and longitudinal redundancy check (LRC) ends the whole data.

III. Threat Model

There are three entities involved in the threat model, *i.e.*, a bank, a customer, and a merchant. A bank in the context of our paper is a financial institute capable of issuing credit cards to customers and authenticating credit card information from merchants. A customer owns credit cards issued from one or multiple banks, and swipes his cards at merchants to buy products. Then, a merchant who owns a credit card reader acquires the credit card information from a customer and authenticates the information with the bank.

In this threat model, users and banks are benign, while the merchants are potentially malicious. A malicious merchant can be one itself, or hacked by an outside attacker through a credit card skimmer, a device that is attached to a normal reader and fraudulently gathering credit card information [18]. In order to distinguish our threat model from other attacks, we list several credit card related attacks. However, those are *out of scope* of this paper.

Fraud over Internet. During transactions over the Internet, credit card information can be sniffed by attacks including but not limited to cross-site scripting attacks, insecure transaction channels like HTTP, and compromised browsers. Among all the aforementioned attacks, neither physical cards nor card readers are involved in the transaction, therefore excluded from the scope of the paper. We believe a web site administrator or a browser vendor could adopt existing defenses [19]–[21] to secure transactions over Internet.

Lost/Stolen Cards. In the case of a lost or stolen card, the attacker can easily read all the information from the credit card without a fake or compromised card reader. In SafePay, we do not have a physical card, but we do discuss similar case about stolen or lost devices of SafePay in Section VII. No additional damages are made in SafePay.

Compromised Servers. In the case of a compromised server, such as a Chase bank server and/or an Amazon web server stored with users' credit card information, an attacker can

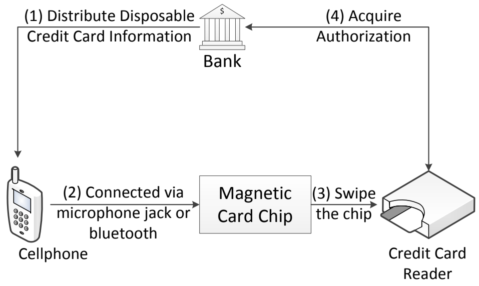


Fig. 1. Overall Architecture.

acquire all the stored information. Again, since neither physical cards nor card readers are involved, the attack is excluded from the scope of the paper. Similarly, a web site administrator could adopt server-side approaches such as Balzarott et al. [22] to defend such attacks.

IV. Overview

In this section, we introduce the overall architecture of SafePay in Figure 1. A cell phone application installed by the user first authenticates itself with the bank application, and then fetches disposable credit card information from the bank. The fetched information is transformed into a wave file on the cell phone, which is played by a media player and converted to an electrical current. The current serves as an input to the magnetic card chip issued by the bank, which simulates the behavior of a physical card. Next, when the user swipes the chip through a credit card reader presented by the merchant, the information, *i.e.*, those generated by the magnetic card chip, is parsed by the card reader and sent to the bank for authentication. Within the overall architecture of SafePay, there are two types of deployment models: bank deployment, where a bank protects all its users, and proxy deployment, where a user relies on a third-party proxy to protect all his credit cards.

Bank Deployment. If SafePay is deployed at a bank side, the transaction process is as follows. First, the user swipe our magnetic card chip, and the information is sent to a credit card association, which contacts the real bank deployed with SafePay. Then, the bank recognizes that the registered user's disposable credit card number and associates it with the user's real account. In the end, a success (or failure in the cases like that the amount exceeds the user's credit limit) notice is sent back to the credit card reader, and the transaction finishes.

Proxy Deployment. If a user wants to protect his or her account but the bank has no deployment of SafePay, he can rely on a third-party provider to protect his credit card information as follows. First, the user registers his bank account or credit card number at a trustable third-party provider (a proxy). Then, when he swipes the magnetic card chip at a magnetic card reader, the reader sends the information to a credit card association. The association redirects the information to the proxy, which contacts the bank with the user provided information. In the end, after acquiring approval or denial from the bank, the proxy redirects the notice back to the association and then the card reader.

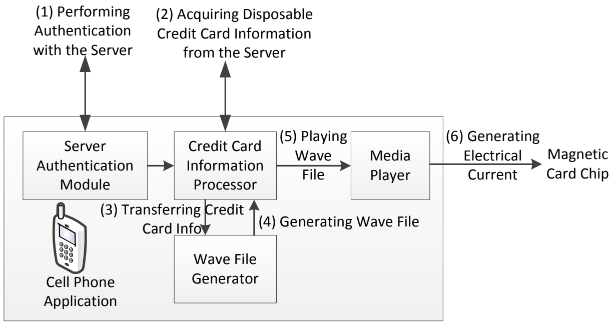
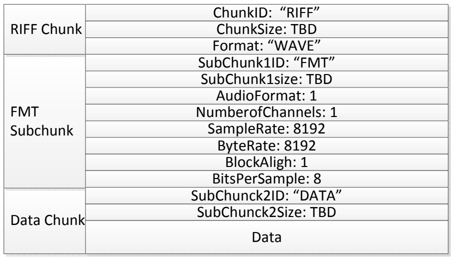


Fig. 2. Cell Phone Application.



RIFF Chunk	ChunkID: "RIFF"
	ChunkSize: TBD
	Format: "WAVE"
FMT Subchunk	SubChunk1ID: "FMT"
	SubChunk1size: TBD
	AudioFormat: 1
	NumberofChannels: 1
	SampleRate: 8192
	ByteRate: 8192
	BlockAligh: 1
	BitsPerSample: 8
Data Chunk	SubChunck2ID: "DATA"
	SubChunck2Size: TBD
	Data

Fig. 3. Wave File Format.

V. Design

In previous section, we give an overview of the architecture of SafePay. Next, in this section, we introduce the details of each individual module separately.

Cell Phone Application As shown in Figure 2, the cell phone application consists of four components: server authentication module, credit card information processor, wave file generator, and media player. First, the server authentication module contacts the server and authenticates the user. Then, credit card information processor fetches disposable credit card information from the server and passes it to wave file generator. When the wave file is ready, it will again be passes to media player. Figure 3 shows the format of a wave file consisting of three parts: RIFF chunk, FMT sub-chunk, and data sub-chunk. RIFF chunk describes the file information, FMT chunk describes some specifications of the current wave file, and data chunk provides the real wave data. According to credit card specification [23], the real wave data starts with several zeros denoting the clock and then real information encoded by zeros and ones. In one period, a constant low or high voltage denotes zero, a switch between low and high voltage denotes one. Each five digits including four digits and a parity represent a character as specified by Aiken Biphase encoding [23]. Once all the information for the wave are produced, a wave generator will write all the details sequentially in binary mode.

Magnetic Card Chip. As shown in Figure 4, a magnetic card chip contains three components: an amplifier, a low pass filter, and a solenoid. When an electrical current comes to a magnetic card, the amplifier first increases its energy to make sure that the current can stimulate a magnetic field. Then, the low pass filter gets rid of high frequency noise that may lower the accuracy

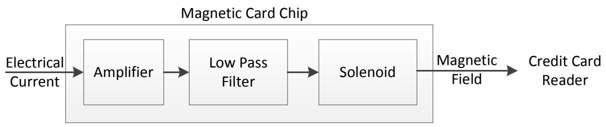


Fig. 4. Magnetic Card Chip.

of a credit card reader. In the end, the processed current is fed into the solenoid to stimulate magnetic field.

Server-side Application. As discussed in Section IV, there are two types of deployment: bank side deployment and proxy deployment, and therefore we are introducing them separately.

- *Bank Application.* A bank application needs to contact both the user with a mobile application and a merchant with a valid credit card reader. The overall process is as follows. When a mobile application installed by a user first communicates with the bank application, the bank application authenticates the mobile user and associates the mobile device with the user's account. Then the bank application distributes disposable credit card information to the mobile application and stores the information associated with the user's account in the database. Next, during a real transaction, when a credit card reader contacts the bank application with disposable credit information, the bank application looks up the user account associated with the information and then perform transactions on the user's account.
- *Proxy Application.* A proxy application needs to contact three entities: a mobile application installed by users, banks, and a merchant with a valid credit card reader. This is how the proxy application works. When a mobile application installed by a user communicates with the proxy application, the proxy application authenticates the user through user name and password. Then, the proxy application obtains the user's card information and contacts the bank to validate the information. Next, the proxy application distributes disposable credit card information, and associates the disposable information with the user's real credit card information. During transactions, when a credit card reader contacts the proxy application, the proxy application first looks up the database to fetch the real credit card information, and then contacts the bank for transactions. If the bank validate the transaction, the proxy application will also generate a validation of the disposable information to the card reader. Otherwise, the proxy application will reject the transaction.

VI. Prototype Implementation

We have implemented a prototype of SafePay as shown in Figure 5. Now, we introduce the prototype implementation of mobile application, magnetic card chip, and server-side application respectively.

Magnetic Card Chip. To implement and debug magnetic card chip, we directly play wav file sound from a desktop media player and feed the output to an old speaker for amplification.

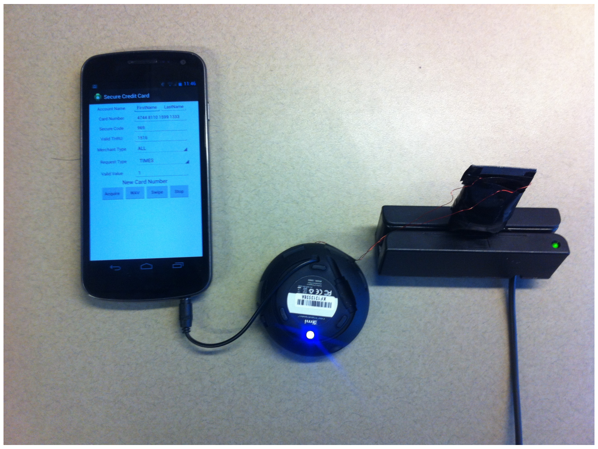


Fig. 5. A Picture of Our Prototype System (In real-world implementation, the amplifier and the solenoid can be combined together into one single chip, which can be directly plugged into the audio jack without a wire or connected with the phone through bluetooth).

The output is restricted between 4V and 5V so that it can stimulate magnetic field. Next, because the sound output contains some high frequency noise, we add a simple low pass filter with a resistor and a capacitor between the amplifier and the solenoid. The cut-off frequency of the low pass filter follows this equation: $f_c = \frac{1}{2\pi RC}$. Since the frequency of our square wave is set to be 8192Hz, if we choose $1\mu F$ as the capacitor, the resistor should be 383Ω. As an approximation, 100Ω resistor is used in the experiment.

After the low pass filter, the output is fed into a solenoid. We mimic the methods described in [24] to make a solenoid in square. An illustration is shown in Figure 6. Resistor wire is twisted on a square shape iron sheet and the front part of the iron sheet is bigger so that it can swipe through a card reader. In practice, we find that since resistor wire is weak and iron sheet is sharp, it is very easy to cut off electric varnish on the resistor wire leading to a short cut. After several failures, we have to put double layers of electric insulation tapes on the edge of the iron sheet to prevent possible short cut. We monitor the resistor between the iron sheet and each end of the resistor wire and find that it is larger than 1MΩ.

Mobile Application. We write a prototype android application with 869 lines of codes to serve as the mobile part. The server communication module is written as Client2Server java class in which it will communicate with the server in an SSL channel defined by *javax.net.ssl*. The client information processor module is written as ClientProcessor java class receiving information from Client2Server class and dealing with UsersDBHandler class that temporarily stores disposable credit card information into a database defined by *android.database.sqlite.SQLiteDatabase* at client side. ClientProcessor class also communicates with WavGenerator generating wav files and WavPlayer class that plays sound by *android.media.SoundPool*. Finally, ApplicationUI class implements a simple UI with login interface and a swipe card button playing sound once pressed.

Server-side Application. As a prototype, we implement a bank

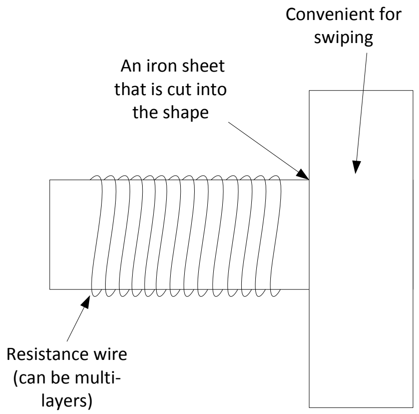

Convenient for swiping
An iron sheet that is cut into the shape
Resistance wire (can be multi-layers)

Fig. 6. Solenoid in the Magnetic Card Chip.

application with 367 lines of codes. The client authentication module is written in a Server2Client java class that acquires and authenticates user information including user name and password through an SSL channel. Then, our implemented credit card information distributor connect to a database using ServersDBHandler java class to store and fetch disposable credit information. Since we have not contacted credit card association, we implemented a fake credit card authentication module by CardAuthenticator class that accepts credit information through network, looks it up through ServersDBHandler class, and then returns the authentication result.

VII. Security Analysis

We analyze the security of SafePay by comparing the new credit card system proposed in this paper with the traditional magnetic credit card system. Then, we mainly focus on what has been changed in the new system and analyze possible security issues. The traditional system consists of three entities: the bank, the cardholder, and the merchant. The bank sends a physical card to the cardholder, authenticates him, and then activates the card. Then, the cardholder swipes his card through a card reader provided by the merchant.

Security of Communication between the Bank and the Card Holder. We are discussing two security issues in the communication between the bank and the credit card holder:

- *Authenticity.* Authenticity solves the problem of how to recognize the cardholder and associate his account with the credit card. In old credit card system, when the cardholder receives the physical credit card, he needs to call the bank, provide his own information like last four digits of social security number, and then activate the card. In the SafePay system, the cardholder needs to register an account by providing his own information and then obtain a user name and password. The process of such a registration has been widely used in online banking systems, and therefore, we believe the process of authentication is mature and safe.
- *Confidentiality.* Confidentiality solves the problem of leaking the credit card information during communication. In old credit card system, the physical card is secured in a sealed envelope during delivery to the cardholder, and therefore an outsider cannot acquire the information without tampering it. In our new credit card system, the disposable credit card information is sent through an encrypted SSL channel that cannot be decrypted without acquiring the private key.

Next, the physical card at the cardholder is replaced by a mobile application installed on a physical phone and a magnetic card chip. We discuss the security of those two separately.

Security of the Mobile Phone at the Card Holder. We focus on the *integrity* part of mobile phone and the credit card application, and then discuss the following two cases:

- *Lost Phone.* A lost phone can enable an attacker to swipe the physical device as the identity of the cardholder. Similarly, in the old credit card system, a lost magnetic card can lead to the same damage. The latter one is even severe because those who find the magnetic card can directly use it, but those who find the phone also need to break authentication mechanism provided by the phone such as PIN.
- *Exploited Phone.* An exploited phone can enable an attacker to break the mobile application and acquire credit card information. However, given the prevalence of mobile banking applications on phones, researchers have proposed many security approaches to prevent information leakages, such as sandboxing a bank application inside a virtual operating system [25]. Meanwhile, we has encrypted the database used by the bank application and therefore the information cannot be read out directly.

Security of the Magnetic Card Chip at the Card Holder. We discuss two security issues for the magnetic card chip:

- *Fake Device.* A fake magnetic card chip could reveal the credit card information to a third party by additional communication channel with an attacker. To avoid using such a fake magnetic card chip, the credit card holder should obtain the magnetic card chip from an authorized bank.
- *Sniffing.* An attacker can sniff the signal emitted by the magnetic card chip and acquire the card information. In SafePay, since the card information is disposable, the acquired information is actually useless. At the same time, we also lower the power of our magnetic card chip so that an attacker cannot sniff the information from ten centimeters away to further minimize sniffing attacks.

Security of the Communication between the Merchant and the Bank. In the case of a malicious merchant, the merchant can read the one-time credit card number, stop submitting it to the bank, and fake a denied transaction. However, because the mobile application at the card holder will verify the denial of transaction, the bank can easily void this one-time credit card number.

VIII. Evaluation

In this section, we first introduce our evaluation methodology in Section VIII-A. Then, we evaluate the correctness of SafePay in Section VIII-B, robustness in Section VIII-C, scalability in Section VIII-D, and cost in Section VIII-E.

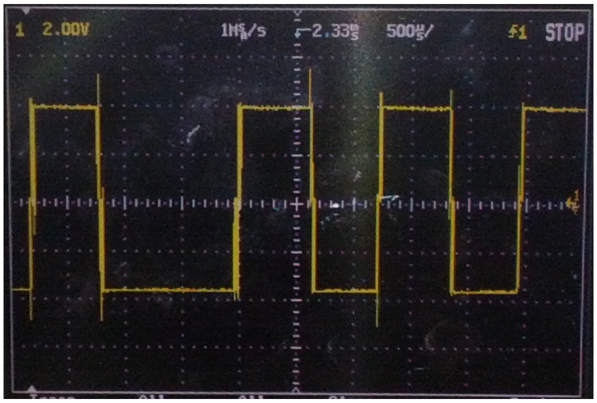


Fig. 7. Unfiltered Outputted Wave at Magnetic Card Chip.

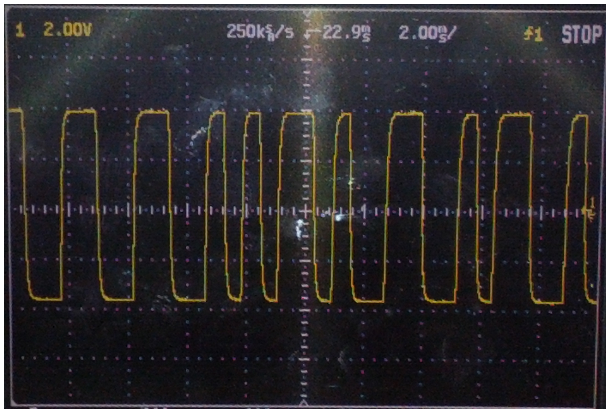


Fig. 8. Filtered Outputted Wave at Magnetic Card Chip.

A. *Methodology*

All the evaluations are performed on Android 4.0.4 of a SumSung Galaxy Nexus phone with 700MHz CPU, 16GB external storage, and 704MB RAM. The server side application is running in a Linux machine with 8 Core 2.5GHz CPU and 16GB memory. We evaluate SafePay on the following metrics:

- **Correctness.** We first want to make sure that SafePay is technically sound by performing two sets of experiments: physical signal analysis and real-world experiment. In the physical signal analysis, we use oscilloscope to monitor the wave outputted from SafePay, and in real-world experiment, we use SafePay in real-world environment.
- **Robustness.** We evaluate the robustness of the magnetic card, server-side application and mobile ones by recruiting people to use it.
- **Scalability.** We evaluate the scalability of SafePay by investigating the future usage if applied to a big community.
- **Cost.** We evaluate the cost of SafePay by calculate its component and adding them together.

B. *Correctness*

To evaluate the correctness of SafePay, we first perform a physical signal analysis to monitor the wave through an oscilloscope, and then test SafePay in real-world environment.

Physical Signal Analysis. In the physical signal analysis, we use Hewlett-Packard 54616C Oscilloscope to monitor voltages before and after filtering at two points. We define *Vout1* as the voltage before the low pass filter, and *Vout2* as the voltage after the low pass filter and before the solenoid. The mobile phone repeatedly plays the same credit card information and we use *Stop* functionality provided by the oscilloscope to record the wave. Then, we manually resemble all the pieces on the oscilloscope screen together, and compare the output voltage with the theoretic wave as shown in Figure 3. Since the oscilloscope does not have an Internet or USB interface, a camera is used to record the screen.

In Figure 7, we show the voltage of *Vout1*. The positive part of the square wave is almost +4V, and the negative part of the wave is -4V. The amplification of the wave is large enough to stimulate a solenoid. However, the switch of positive and negative has lots of noise as large as 8V (not shown in the figure), which lows the accuracy of SafePay. Therefore, we add a low pass filter and show the voltage of *Vout2* in Figure 8. The noise in Figure 7 is greatly mitigated.

Meantime, we also compare those combined pieces (only one is shown in Figure 7) with the original generated wave file. We start with the synchronization clock and end with the check sum. The result is that the output wave monitored by oscilloscope exactly matches the generated wave file.

Real-world Experiments. To evaluate the correctness of our magnetic credit card chip in real world, we perform three experiments on a vending machine, a gas station, and a university coffee shop. During the experiments, we adopt our bank application, cell phone application, and magnetic credit card chip. The disposable credit card information is acquired from ShopSafe [26] by registering several disposable credit card information with a Bank of America credit card from the authors' group. Since the disposable credit card only has a "valid through" setting instead of the number of valid times, our server-side application needs to invalidate the "valid through" date in the Bank of America system automatically, after the disposable credit card number is used.

At the vending machine, the cell phone is on Wi-Fi mode. By swiping our magnetic credit card chip, we successfully buy a coffee. At the gas station, the cell phone is on 4G mode, and we perform similar actions and successfully fill gas into a car. At the university coffee shop, we tell the staff about the purpose of our research and let him to swipe the chip. By doing this, we successfully buy a cup of yogurt. In sum, the three aforementioned experiments show that SafePay does work in real-world environment.

C. *Robustness*

We evaluate the robustness of SafePay by examining magnetic card chip and both the server and mobile application below.

- *Magnetic Card Chip.* To evaluate the robustness of our prototype chip, we randomly select twenty people within our department, give them our credit card reader and SafePay, and tell them how to install the mobile client at their own cell phone. We ask them to swipe the magnetic card chip ten times and record the number of successful swipe. Out of twenty people, nineteen of them all get ten times correct swipe. We investigate the only one who cannot swipe the chip correctly and find that the volume of his cell phone is not large enough to stimulate magnetic field. We let him increase the volume and he can swipe SafePay correctly too.

- *Server and Mobile Application.* To evaluate the robustness of our prototype implementation of server and mobile application, we let the server-side application generates ten thousands credit card number and let the reader to read it. Then, we calculate the number of successfully read numbers. The results show that all ten thousands generated credit numbers are correctly read, indicating that server-side application can generate correct credit card information and mobile application can convert it into electrical current.

D. Scalability

The disposable credit card information faces the problem of capacitor since every day every one may acquire several credit card numbers. As shown in the specification of Section II, a normal credit card like visa and master card number includes six-digit issuer identification number, one-digit checksum, and account number up to sixteen digits. Adding four-digit expiration date to the account number, we have thirteen digits that can be used for disposable credit card numbers. Assuming that there are one billion[3] people using the service, each person can have 10 million disposable credit card number at a time, which is enough for a normal person to purchase merchandises even for a whole year.

E. Costs

We evaluate the cost of magnetic card chip in this subsection. As discussed in Section V, a magnetic card chip consists of three components: an amplifier, a low pass filter, and a solenoid. The price of an operational amplifier is $0.35 in Amazon [29], and the price of one resistor is $0.02 [30]. Therefore, the whole amplifier is $0.37. A low pass filter consists of a resistor and an electric capacitor. Both resistor and capacitor are about $0.01 each [30, 31]. In the end, resistor wire used in solenoid is $1 per 10 kilograms [32]. We only use less than 100 grams in solenoid, which is again about $0.01. Iron sheet is also about $0.1. Adding all of them together, we have less than $0.5 for the magnetic card chip. We believe that it is affordable, and the price could be even lower if manufactured in large scale.

IX. Discussion

We discuss the following questions in this section.

What if there is no wireless communication? SafePay needs to contact the server through a wireless communication to acquire disposable credit card information. However, Wi-Fi network is not always available and mobile network like 3G and 4G usually costs money. In the case that a wireless network is not available, the mobile application can pre-fetch several disposable credit card numbers and store them in the phone. Therefore, the mobile application still works even if there is no Internet connection.

Does the usage of disposable credit card number hinder the process of returning items? No, because disposable credit card numbers are associated with the customer's real credit card account, the bank that receives a refund for a disposable credit card number can return the refund to the customer's real credit card account. Similarly, for will-call scenarios, the disposable credit card number can serve as the authentication of the customer.

What is the additional gain of SafePay other than the security aspect? One additional gain of SafePay is that banks do not need to issue a new card once the old credit card that belongs to a cardholder expires, since we actually use a new card during each transaction. The advantage first saves cost since both a new card and delivery costs additional fees. Second, it also saves a lot trouble for the cardholder to receive and activate a new card, which may bring possible interruption of the credit card usage.

What if the phone loses power? First, we believe that a phone with power is a key factor for many mobile applications, such as mobile banking applications, news applications, and mobile games. It is a separate and hot topic for researchers to boost the capability of batteries.

Second, actually, a mobile phone is also involved in traditional credit card forgery protections. For example, if a transaction happens at a unusual place, the bank that issues the credit card will call the cardholder to make sure the success of that transaction. In that case, if the mobile phone loses power, the transaction cannot succeed either.

X. Related Work

We first introduce direct solutions to credit card forgery in Section X-A. Then, two techniques in SafePay used for other purpose are introduced in Section X-B. We are aware that most of our cited works belong to commercial systems. The reason is that practically the credit card forgery problem is significant and draws attentions from many real-world commercial vendors, while in the academic area, the problem is relatively new and rarely being studied. One of the purposes of the paper is to draw the attentions of the academic world and shed a light for future researchers to study the problem.

A. Solutions to Physical Credit Card Forgery

We divide existing solutions to physical credit card forgery into two categories: client-side deployment and server-side deployment. Client-side deployment includes IC cards, two-factor authentication, and mobile wallets applications. Server-side deployment mainly refers to behavior based detection.

IC Cards. Integrated circuit (IC) cards or smart cards are those with embedded integrated circuits providing identification and

[3] The population of the U.S is approximately 300 million [27], and according to statistics, there are 609.8 million credit cards held by U.S. consumers in the year of 2010 [28].

authentication. With IC cards, strong security authentication can be provided to ensure communication security. There are two types of IC cards, namely contact IC cards and contactless IC cards. Contact IC cards without embedded batteries adopt ISO/IEC 7810 [33] and ISO/IEC 7816 [34] standard and get power from the reader. Contactless IC cards communicate with and are powered by the reader through wireless technology at transmission speed of 106-848 Kbit/s. The same as contact IC cards, contactless IC cards capture power from wireless signal, and drive its embedded circuit. As discussed in the introduction, IC cards face backwards compatibility issues, and therefore all existing IC cards still have a magnetic stripe on it to maintain backwards compatibility. Consequently, a malicious merchant can simply inform the customer the absence of IC card readers, force him to use the magnetic strip on IC cards, and steal credit card information.

Two-factor Authentication, such as PIN, CSC and Location. Personal identification number (PIN) is usually a four to six digit number known by the cardholder only to identify and authenticate transactions. During transaction, the cardholder needs to input the number through a PIN pad concealed from the merchant. There are no needs to add PINs to a magnetic strip, because any reader can read any contents on a magnetic strip.

Card security code (CSC), card verification value (CVV), card verification code (CVC), or some other similar names are usually three to four digit number printed on the physical card on the back (visa and master card) or on the front (American express card). It is designed to combat card-not-present forgery where a transaction needs to be verified together with a CSC number. In our threat model, because at physical positions, the cardholder needs to present the physical card to the merchant who can see the CSC clearly, a CSC number cannot prevent such attacks.

Mobile Wallets. LevelUp [1] is a start-up company that provides credit card authentication services that read generated QR Codes through another phone's camera. First, both the user and the merchant need to download LevelUp applications and register their services. The user inputs his own credit card information into LevelUp database and then LevelUp provides him a randomly generated QR code representing his account. The merchant installs the merchant part of LevelUp application on a cell phone and treats the cell phone as a card reader. During the transaction, a user presents his QR code to the merchants cell phone camera, which reads the information and sends to LevelUp server. The server authenticates the pre-stored credit card information and tells the merchants that the transaction succeeds or fails. Similarly, services provided by Paydiant Inc. [10] and Square Wallet [9] also adopt QR Codes. In particular, Paydiant Inc. provides a special software designed for a certain version of magnetic card readers to display an QR code for customers. Square Wallet [9] additionally uses geo-fencing to locate a user and display customers' name and photo on merchant reader's screen.

In addition, Google Wallet Application [12] adopts Near Field Communication (NFC) that allows a user to tap his cell phone near a special designed device and proceed the transaction. The two devices talk to each other through radio communication and exchange information. Meanwhile, TagPay Wallet [11] developed by Tagattitude adopts Near Sound Data Transfer (NSDT) that allows a cell phone to communicate with another cell phone or special designed device such as "Mobile Payment Terminal" (MPT) through its speaker and microphone via sound channel.

However, the same as IC card, a mobile wallet service requires changes at merchants' side by introducing a cell phone, a hardware, and/or a software. The number of such solutions is so large that a merchant may not have the specific solution that a customer uses, and therefore they have to use magnetic card readers facing skimming attacks.

Behavior based detection together with replacing card. To deal with credit card forgery, many issuers adopt complex detection methods for an abnormal usage of credit cards [35]–[37]. For example, credit card companies record the place that a credit card is normally used, and if the credit card is used at a different place or country, the transaction will be denied. Similarly, if a credit card is consumed at an untrusted merchant rated by the company, the credit card company will also deny the transaction. After the denied authentication, the credit card company usually informs the credit card holder about the information leakage and issues him or her new cards. However, compared with SafePay, there is a gap when the old card is invalid and the new one has not been sent to the cardholder through post mail service, triggering inconvenience for the cardholder. During that period, the cardholder cannot use his credit card. More importantly, those methods are hard to achieve 100% detection accuracy. For example, a cardholder normally performs transaction in U.S, but his travel to European countries with notification of banks may incur a denial of transaction and brings inconvenience for himself.

B. Disposable Credit Card Number, Card Spoofer and Others

Two parts of techniques used in SafePay, namely disposable credit card number and credit card spoofer, have been used for other purposes, and we present them below.

Disposable credit card number has been adopted by PayPal, American Express, EntroPay and so on for online usage. For example, EntroPay [15] allows depositing certain amount of money into a virtual credit card, the information of which is temporarily generated and changeable. Similarly, PayPal also invents virtual credit card number working in the same way [16]. All the existing disposable (virtual) credit number have been used for protecting clients from online credit card fraud but not physical card forgery, because it is impossible and costly to issue the cardholder a physical card each time.

Credit card spoofer has also been invented for fun and hackers only but not legitimate and protection purpose. As shown by [24], they have invented a credit card spoofer to open a door system protected by a magnetic card. The magnetic card chip part of our works has been largely inspired by their system. However, we also make changes by adding a low pass filter to increase the success rate of credit card reader. Similarly, coin [38] is another implemented credit card spoofer.

Comparing with existing techniques, we believe that we are the first to include both two techniques in one system and automate the whole process by a mobile application and a server-side application to solve a significant problem, physical magnetic card information leakage through a fake reader or a skimming device. That is the key contribution of the paper.

Other than the aforementioned related work, there is another interesting piece of work, Square Register [39], which is exactly the opposite of SafePay in the means that Square uses a chip to mimic a credit card reader, while we use a chip to mimic a credit card. Square is an ideal solution for a small or mobile business where a merchant does not need to carry a big credit card reader but a small chip with him. However, the purpose of Square and SafePay is different.

XI. Conclusion

In this paper, we propose a system protecting customers from credit card forgery and being compatible with existing magnetic card readers. First, the bank side generates disposable credit card information and delivers them to a mobile application installed on a cardholder's mobile phone. The mobile phone stimulates a magnetic credit card chip by playing sound through its audio jack. The cardholder can use the chip the same as previous physical card. We have implemented the whole system by a bank server, a mobile phone application, an amplifier, and a solenoid. In the evaluation, we successfully tested several real-world merchants such as vending machines and coffee shops. Meanwhile, we also estimate the cost of the whole prototype system without the mobile phone, which is about 0.5 dollar. If manufactured in large scale, the cost can be even lowered.

XII. Acknowledgement

This material is based upon work supported in part by Qatar National Research Fund under award ID SP0022512 and National Science Foundation under award number 1408790. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the authors and do not necessarily reflect the views of the funding foundations.

References

[1] LevelUp. https://www.thelevelup.com/.

[2] M. SCHMIDT and N. PERLROTH. Credit card data breach at barnes & noble stores. http://www.nytimes.com/2012/10/24/business/hackers-get-credit-data-at-barnes-noble.html?_r=1&adxnnl=1&adxnnlx=1363194210-f1jKgh5cVLKuz8egxYwCmw.

[3] S. Germano. Targets data-breach timeline. http://blogs.wsj.com/corporate-intelligence/2013/12/27/targets-data-breach-timeline/.

[4] S. Zhang. Five steps of making a fake credit card reader [in Chinese]. http://credit.cngold.org/c/2012-07-23/c1227945.html.

[5] L. Musthaler. U.s. clings to insecure magnetic stripe cards - whats the attraction? http://www.securitybistro.com/blog/?p=811.

[6] Smart cards [Wikipedia]. http://en.wikipedia.org/wiki/Smart_card.

[7] The unfortunate truth about your new chip credit card. http://www.huffingtonpost.com/creditcardscom/the-dirty-little-secret-y_b_5572081.html.

[8] MTA MetroCard. http://web.mta.info/metrocard/.

[9] Square wallet. https://squareup.com/wallet.

[10] Paydiant. http://www.paydiant.com/.

[11] Tagpay wallet. http://www.tagattitude.fr/en/applications/wallet.

[12] Google wallet. https://play.google.com/store/apps/details?id=com.google.android.apps.walletnfcrel&hl=en.

[13] Apple pay. https://www.apple.com/iphone-6/apple-pay/.

[14] J. ESPINOZA. Mobile wallets: A primer for retailers. http://online.wsj.com/article/SB10001424127887323826704578353812358723042.html.

[15] Entropay. Https://www.entropay.com/.

[16] Use paypal's free disposable credit card number to manage recurring charges. http://geardiary.com/2009/01/24/use-paypals-free-disposable-credit-card-number-to-manage-recurring-charges/.

[17] Secrets of the luhn-10 algorithm - an error detection method. http://www.ee.unb.ca/tervo/ee4253/luhn.shtml.

[18] Police briefs: Credit card skimmer found on pacific grove gas pump. http://www.montereyherald.com/ci_22753990/credit-card-skimmer-found-gas-pump?source=rss_viewed.

[19] M. Ter Louw and V. Venkatakrishnan, "Blueprint: Precise browser-neutral prevention of cross-site scripting attacks," in *30th IEEE Symposium on Security and Privacy*, 2009.

[20] P. Bisht and V. N. Venkatakrishnan, "XSS-GUARD: Precise dynamic prevention of cross-site scripting attacks," in *Proceedings of the 5th international conference on Detection of Intrusions and Malware, and Vulnerability Assessment*, ser. DIMVA '08. Berlin, Heidelberg: Springer-Verlag, 2008, pp. 23–43. [Online]. Available: http://dx.doi.org/10.1007/978-3-540-70542-0_2

[21] F. Nentwich, N. Jovanovic, E. Kirda, C. Kruegel, and G. Vigna, "Cross-site scripting prevention with dynamic data tainting and static analysis," in *In Proceeding of the Network and Distributed System Security Symposium*, 2007.

[22] D. Balzarotti, M. Cova, V. V. Felmetsger, and G. Vigna, "Multi-module vulnerability analysis of web-based applications," in *CCS: Conference on Computer and Communication Security*, 2007.

[23] C. Zero. Card-O-Rama: Magnetic Stripe Technology and Beyond or A Day in the Life of a Flux Reversal. http://www.phrack.org/issues.html?issue=37&id=6#article.

[24] Magnetic stripe card spoofer. http://www.instructables.com/id/Magnetic-stripe-card-spoofer/?ALLSTEPS.

[25] J. Andrus, C. Dall, A. V. Hof, O. Laadan, and J. Nieh, "Cells: a virtual mobile smartphone architecture," in *Proceedings of the Twenty-Third ACM Symposium on Operating Systems Principles*, ser. SOSP '11.

[26] Shopsafe online shopping security enhancement. https://www.bankofamerica.com/privacy/accounts-cards/shopsafe.go.

[27] U.S. population. https://www.google.com/search?newwindow=1&q=U.S+population&oq=U.S+population.

[28] B. Woolsey and M. Schulz. Credit card statistics, industry facts, debt statistics. http://www.creditcards.com/credit-card-news/credit-card-industry-facts-personal-debt-statistics-1276.php.

[29] LM358 power dual operational amplifier. http://www.amazon.com/Texas-Intsruments-Dual-Op-Amp/dp/B003O3PBRC/ref=sr_1_1?ie=UTF8&qid=1367939372&sr=8-1&keywords=LM358.

[30] Resistance price [in Chinese]. http://detail.cn.china.cn/provide/2282884381.html.

[31] Capacity price [in Chinese]. http://detail.cn.china.cn/provide/2051419632.html.

[32] Resistance wire price [in Chinese]. http://detail.cn.china.cn/provide/2121160801.html.

[33] ISO/IEC 7810. http://en.wikipedia.org/wiki/ISO/IEC_7810.

[34] ISO/IEC 7816. http://en.wikipedia.org/wiki/ISO/IEC_7816.

[35] E. Dumana and M. H. Ozcelikb, "Detecting credit card fraud by genetic algorithm and scatter search," *Expert Systems with Applications*, 2011.

[36] A. Srivastava, A. Kundu, S. Sural, and A. Majumdar, "Credit card fraud detection using hidden markov model," *IEEE Transactions on Dependable and Secure Computing*, 2008.

[37] C. Whitrow, D. J. Hand, P. Juszczak, D. Weston, and N. M. Adams, "Transaction aggregation as a strategy for credit card fraud detection," *Data Min. Knowl. Discov.*, 2009.

[38] coin. https://onlycoin.com/.

[39] Square register. https://squareup.com/register.