Taming The Wild Card for Mobile Payment

Mastooreh Salajegheh
Computer Science
University of Virginia,
Charlottesville, VA
negin@virginia.edu

Bodhi Priyantha
Microsoft Research
Redmond, WA
bodhip@microsoft.com

Jie Liu
Microsoft Research
Redmond, WA
liuj@microsoft.com

ABSTRACT

Mobile wallets promise to allow people to easily manage their accounts and to carry less cards. However, the slow adoption of contactless point of sales (POS) terminals by merchants limits the potential of Near-Field Communication (NFC) based payment devices. In this paper, we discuss Wild Card, a secure and backward compatible way to make mobile payment through conventional magnetic stripe based POS terminals. The device resembles a traditional credit card in its physical dimensions and stays in the phone case. It can be programmatically set by a NFC-enabled mobile phone to any card number that the user owns. The key technologies that enables Wild Card are a fully programmable magnetic stripe, an energy harvesting system that allow the card to be charged and programmed by the phone through NFC, and a security mechanism that makes card information resilient to attacks on mobile devices. With a prototype, we evaluate the feasibility of Wild Cards in terms of functionality and energy budget.

INTRODUCTION

How thick is your wallet? According to estimates from Census Bureau, there are more than 1.4 billion credit cards in the US [19], most of which are contact magnetic stripe credit cards and a smaller fraction of the cards are contactless (e.g. RFID-enabled). A typical person also carries debit/bank cards, membership cards, discount cards and loyalty cards in the wallet. Again, majority of them are magnetic stripe cards.

Smart phones have successfully assimilated many personal objects in our daily life, such as cameras, music/video players, GPS, calendars, web access, and game consoles. More recently, mobile wallets promise to push the integration further to reduce the thickness of actual wallets or to replace them altogether.

The concept of mobile wallets is quite broad, largely including:

- Account Management: Our credit card, debit card, or membership accounts can be stored in mobile devices for easy access. Examples include Wallet apps in Android and Windows Phone devices, various bank and Paypal apps, as well as apps like Card Star that simply stores bar codes for membership, shopping, and frequent flier numbers.
- Mobile Payment Acceptor: These are credit card reader devices, such as Square and Paypal readers, as smart phone peripherals that allow smart phone owners to accept payment made from regular magnetic stripe credit cards.
- Mobile Payment Issuer: These are mobile devices that can make a money transaction via specially designed terminals. While bar codes have been used for small transactions, like in Starbucks, the widely referenced example is contactless card emulators via Near Field Communication (NFC). A NFC equipped mobile phone can emulate a contactless credit card (e.g. PayPass from Master Card and PayWave from VISA) and make payment at terminals that supports NFC.

This paper focuses on the mobile payment issuer cases. Although NFC has experienced fast growth in recent years, the adoption is still slow compared to the massive payment infrastructure around conventional magnetic stripe based credit or debit cards. According to market research reports [4, 17], there are about 150,000 contactless point-of-sales (POS) terminals in US in 2011, and the growth rate is about 17% from 2011 to 2015, or doubling in 5 years. In comparison, there are over 13 million VISA payment terminals alone. It has been widely recognized that the high cost of contactless POS terminals and the lack of incentives for merchants to upgrade existing payment infrastructure pose great challenges to the wide adoption of NFC-based mobile payment systems [17].

Can we design a mobile payment device that is compatible with conventional infrastructure yet allows us to enjoy the convenience of mobile account management?

Imagine a single "credit card" that can be pulled out of a smart phone. The card can be programmed by the smart phone into any magnetic stripe based card that one owns, and be swiped at any magnetic stripe card receivers at merchants' POS terminals. The card account information is managed by the phone, taking advantage of its UI and network connectivity. For example, account balances and rebate programs can be easily accessed when making a payment decision; coupons can be pushed to the phones and redeemed electronically; and with the support from credit card issuers, one can request a one-time-use card number at the POS for just

Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. To copy otherwise, or republish, to post on servers or to redistribute to lists, requires prior specific permission and/or a fee.
UbiComp '13, Sep 8-Sep 12, 2013, Zurich, Switzerland.
Copyright 2013 ACM 978-1-4503-1770-2/13/09...$10.00.

one transaction to avoid card number being stolen. One can even program the card so it can only be swiped once, in situations when the card must be handed to a third person (e.g. a waiter) to be swiped out of sight. We call this type of card a *Wild Card*.

Recent advancements in low-power electronics and energy-harvesting techniques enable boundless ubiquitous applications. Our goal in the paper is to show that it is technically feasible to build a new ubiquitous application, a Wild Card that is backward compatible with magnetic stripe readers, forward compatible with mobile wallets, and secure. There are several challenges to achieve this goal. Among them, the most profound one is to achieve a fully programmable magnetic stripe. That is, to design a mechanism that the card can programmatically produce the same magnetic stripe signals when swiping through a reader, within the physical dimension of a credit card, especially the 0.7mm thickness. Furthermore, the card can communicate with a smart phone to receive the numbers that user chooses. All has to be within an energy budget that can be obtained and stored by the card with normal usage patterns. The card has to protect the security and privacy of user date.

The main contributions of our Wild Card design can be highlighted as:

- A multi-track dynamic magnetic stripe emulated by rows of ferrite-core inductors. Instead of laying out the magnetic components to meet the bit-level dimension of magnetic materials on conventional cards, our card detects the reader head position and "plays back" the stripe content sequentially. The magnetic stripe emulator is driven by a low power microcontroller, which receives card information from a mobile phone.

- A NFC-based charging and communication interface to smart phones. We show that a card, normally stored in the sleeve of a NFC-enabled phone, can harvest enough energy to charge a thin-film battery to power a day-long card usage, even after the phone is out of battery.

- We design a security framework that allows card numbers to be handled securely even when the mobile phone or the card are stolen.

Although limited by the manufacturing process to integrate the pieces into a full package, we evaluate each subsystem to show that technologies are ready for Wild Card.

The rest of the paper is organized as follows. We first report the results from a user study on the Wild Card concept and to motivate the goals in our design. Then, we give an overview of conventional magnetic stripe and its reading mechanisms, and describe our design of the stripe emulator. We design a security framework that is adapted to the limited computation and memory resources of card microcontrollers. Finally, we discuss the energy harvesting and storage subsystem and evaluate the energy consumption of the card components using our prototype. We show that we can harvest enough energy from mobile phones to power the card for its daily use.

MOTIVATION

There are good reasons that people keep multiple cards in their wallet and use different ones in different situations. Card acceptance, rebate programs, credit limits, and damage containment (when information of a single card is stolen), are common considerations when choosing one card versus others. Mobile payment systems promise to make the card management experience simpler. With mobile phones managing multiple cards in the same app, one can select which card to use from a single interface. Once selected, the payment device (primarily NFC-enabled phones today) is programed to use the corresponding account.

Our goal here is to replace all magnetic stripe based cards, most notably credit cards, bank cards, and loyalty cards by a single, programmable device that resemble the physical size of a credit card. So users can enjoy mobile-managed payment without merchants changing the existing payment receiving infrastructure. To understand how people will accept this idea, we conducted a user study.

User Study

The user study is conducted with 201 people, including 88 male and 113 female, from age 18 to 84. It is part of a larger study, which is designed to evaluate a set of new technologies and is deliberate to hit a broad and balanced set of demographics. For example, 50% of users in the study have smart phones, 42% have basic phones that cannot access internet or download apps, and the rest 8% do not have a mobile phone at all. Among the users, 68.7% carry at least one credit card everyday, while 78.6% carry at least a debit card.

In particular, we are interested in "tech trendsetters" (TT) who are identified by having strong agreements (over 80%) with the following statements: 1) "I embrace technology and social media (e.g., blogs, Twitter, Facebook, etc.) to connect with others and express myself in new, interesting, and fun ways"; 2) "Technology is important to me for staying organized (e.g., scheduling, planning, etc.)"; and 3) "It is important for me to have internet access when I am on-the-go—away from home or work." There are 30 tech trendsetters in the survey, among roughly equal numbers of "Go Getters", "Home Honchos", "Savvy Socials", "Game Gurus", "Media Moderates", "Avid Avoiders", and "Common Casuals". Due to the page limit, we do not enumerate the questions asked to derive these classes, rather we use these terms based on common senses. The reason we separate out tech trendsetters is because these are early adopters of latest technologies, such as smart phones in 2007 and tablets in 2010.

To evaluate the concept, we show all users a picture shown in Figure 1, with the following description:

A universal smart card that syncs with your phone so you do not have to carry individual credit, debit, and frequent shopper cards. How it works:

- *Download an app to your phone and tell it which cards you want to use.*

- *When you go to make a purchase, use the app to select*

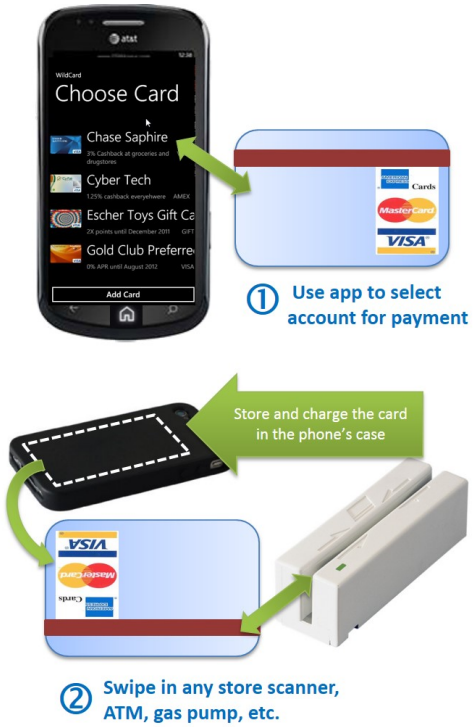

Figure 1. A visual description of Wild Card used in the user study.

which account to use.

- *In some stores you will have an option to pay directly from your phone with NFC. In all stores you can pull out the card from its slot in the back of the phone's case and use it in any conventional card reader.*

We told users that the potential benefits for such a card are:

- Convenience: Eliminates the need to carry individual cards and locate them each time one pays.
- Security: When done right, the account numbers cannot be copied or stolen because the phone can request a unique number from card issuers for each transaction. Both the phone and the universal card are useless if lost or stolen.
- Cost Savings: The phone can automatically recommend the best card to use for a transaction, optimizing card discounts, interest rates and/or reward programs and applies store coupons and discounts.
- Information Advantage: See your balances prior-to and following transactions.

We then asked users the following questions and assign numerical values from 0 to a maximum point from 4 to 9, based on answers like disagree / not exciting / dislike to strongly agree / very excited / strongly preferred.

- Like(0-6pts). Which statement best describes how much you think you would like or dislike this idea?

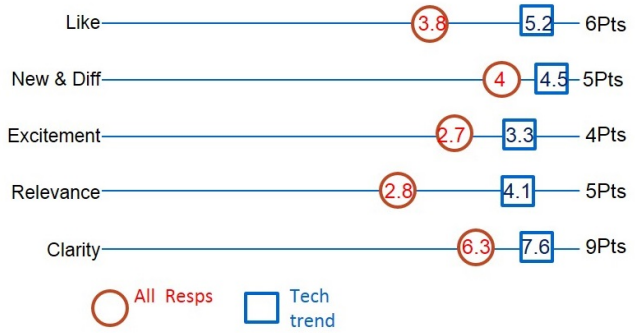

Figure 2. User study results in term of different features of the concept.

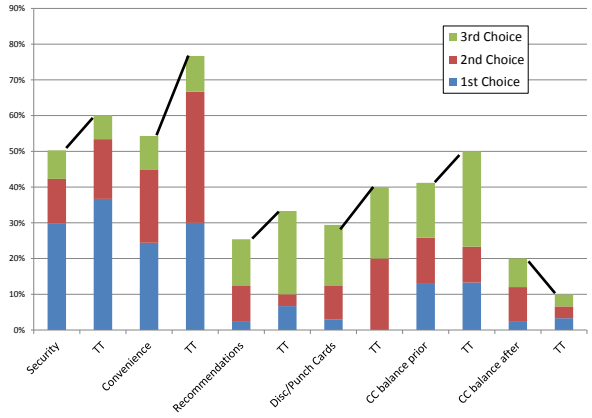

Figure 3. The distribution of the top three reasons a use would like the use the card.

- New & Diff (0-5pts). Which of these phrases best describe how new and different you think this idea is from other things that are available?
- Excitement (0-4pts). How exciting do you find this idea?
- Relevance (0-5pts). Assuming the idea you have seen was available today, how likely would you be to use it yourself either for work, school or personal use?
- Clarity (0-9pts). To what extent do you believe you know what to expect from this idea?

Study Results

The score of the user study is shown in Figure 2. We can see that while the average population found the concept attractive, it is especially preferred among the tech trendsetters. Figure 3 further plots the top reasons that users select to use the card. Each pair of the bars shows the distribution of general users and tech trendsetters (TT) who give the corresponding choices. Clearly, security (i.e. being able to request a unique number for every swipe) and convenience are the top reasons that people like the concept.

As part of the study, we also allow users to give written comments on the top reasons and top concerns of universal credit

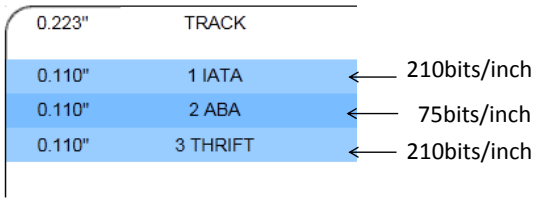

Figure 4. The dimension and bit density on card magnetic stripes.

cards. Here we quote some examples of concerns given by the users: 1) "*Cell phones are unreliable as phones—I would not want to be stuck without my credit cards too if there was an emergency.*"; 2) "*One mugging and all your information is gone and your credit rating can be wrecked.*"; 3) "*My phone shouldn't have that much information about my personal stuff*". Clearly, many concerns are around that the phone may be compromised, either physically or through cyber-crimes. At the same time, the credit card should work even when the phone runs out of battery. For the rest of the paper, we focus on discussing the Wild Card designs that overcome these challenges.

MAGNETIC STRIPE CARDS: BACKGROUND

In order to make magnetic stripe cards programmable, let us first review the conventional cards and reader mechanisms.

A standard credit card is of dimension 86mm x 54mm x 0.76mm (or 3.375in x 2.125in x 0.03in). The magnetic stripe on it is 0.33 inches wide, split into three tracks, as shown in Figure 4. Bits are encoded serially on the magnetic stripe using a series of magnetic materials and the changes of N-S poles cause magnetic flux transitions in the reader (Figure 5). The data encoding uses a F2F (Frequency–double frequency) mechanism. There are essentially long and short magnets pasted on the stripe, each with a flip of polarization from the previous one. When a reader go through the boundary of the magnets, it can detect the flip of the magnetic field. A *zero* bit is represented by a long magnet, while a *one* bit is represented by two consecutive short magnets. Typically, the length of a zero bit is 0.0047619 inches for track 1 and track 3 and 0.013333 inches for track 2. The shorter length zero bits allows for higher information density in a track.

The F2F encoding allows self-clocking of the data which means the encoded data can be extracted from the data signal without a need to present another extra signal for the clock. The self-clocking feature is especially helpful in the case of the cards because the card is passed through the reader by human hand and it works regardless of how fast or slow the card swiping is. To help the reader estimate the swiping speed and generate an internal clock to match the card frequency, at two ends of the card, there is a sequences of 1's serving as the clock reference.

Card information is usually encoded on the first two tracks of the card. The usage of the third track is not uniform among card issuers. Track1 contains 7-bit (6 plus odd parity) alphanumeric characters while track2 and 3 provide 5-bit (4

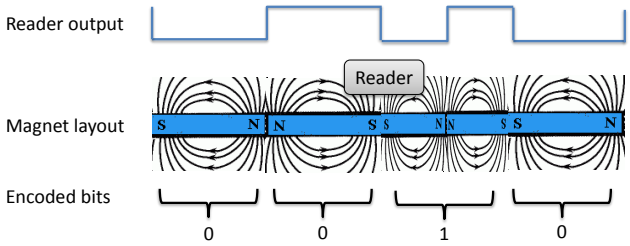

Figure 5. Bit encoding on stripes using longer and shorter magnets.

plus odd parity) numeric characters [9]. Figure 6 shows the typical layout of contents on track 1. There are 62 bit of clocking signals on each end (so the card can be swiped from either direction), a start sentinel(% symbol), up to 76 character of data, an end sentinel (? symbol), and error checking code LRC (Longitudinal Redundancy Check).

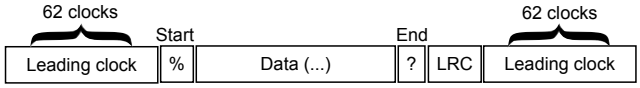

Figure 6. All three tracks of the magnetic stripe have a similar data format. They start with leading clocks to allow enough time for the reader to detect the card. Then a start symbol (%) is followed. The data segment is alphanumerical for track1 and only numeric for track2 and track3.

DESIGN OF THE Wild Card

At a high level, the card has the following components, as shown in Figure 7. As a mobile phone peripheral, the card is normally stored in a phone case. It communicates with the phone and get charged by the phone through near-field communication (NFC) interface. A magnetic stripe emulator allows it to produce magnetic fields that can mimic those from real magnetic stripes. There may be buttons or displays on the card for user interaction. A microcontroller on the card controls the energy harvesting, NFC communication, card emulation and UI.

In the rest of this section, we explain the key technologies that enables the Wild Card – magnetic stripe emulation, energy harvesting, and the security framework.

Dynamic Magnetic Stripes

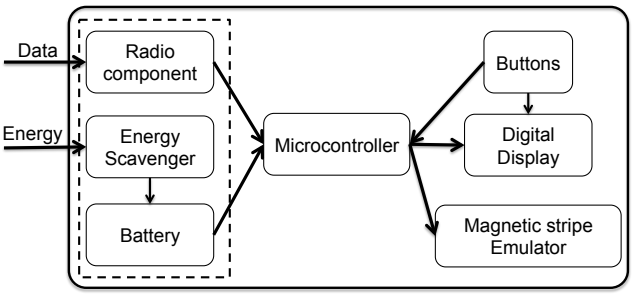

Figure 7. The high level design of a programmable card that interacts with a phone.

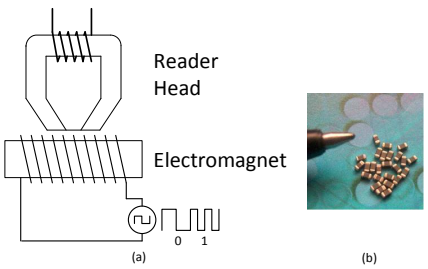

Figure 8. Emulating the magnetic stripe of payment cards using an electromagnet energized by a waveform representing the encoded bit pattern. (a) The principle of electromagnetics. (b) Examples of tiny inductors.

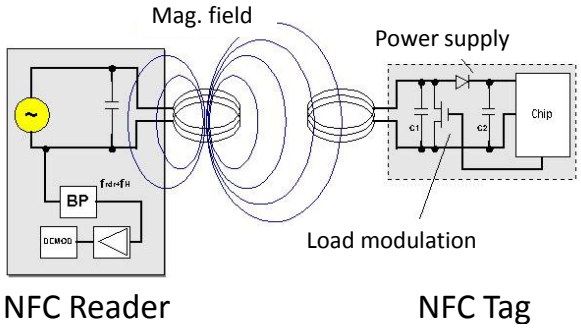

Figure 9. NFC reader and passive NFC tag functional block diagram.

The goal of a programmable card is to represent more than one card data on the magnetic stripe; this requires a *dynamic* magnetic stripe that can generate the appropriate magnetic field corresponding to the data on *any* given card.

While a conventional magnetic strip is composed of a number of tiny fixed magnets to generate alternating magnetic fields at the magnetic reader's head when the card is moved across the head, it is impossible, or likely to be very expensive, to line up tiny electromagnets with the same density and controlled by a microcontroller. Instead, Wild Card uses a single (or an sectional array of) electromagnet to *play back* the varying magnetic field over time, mimicking card swiping motion.

Consider from the point of view of a reader head, when a conventional card swipes across it, it reads alternating magnetic field over time. The same effect will hold, if we keep the reader stationary and use an electromagnetic to generate the fields (Figure 8 (a)). Empirically, we observe that it typically takes 100 to 200 milliseconds for a card to swipe through a reader. Given the 553 bits on the densest magnetic stripe, or about 1106 field flips, it means the electromagnetic field has to run at a frequency up to 10KHz. Of course, the electromagnetic component has to fit in the physical card dimension. Many small inductors can meet the frequency and size requirements.

A challenge for sequential playback is to detect the position of the reader head, since we want to keep the swiping experience that users are familiar with. Our solution leverage the fact that reader heads are made of metal materials, has a flat curvature at the center, and is mounted on a spring for reliable reading of conventional card. If we expose two conductive terminals on Wild Card, the reader head will short circuit it, which can be used as an interrupt to the microcontroller.

Energy Harvesting

Being an active device to drive the dynamic magnetic stripe card and to communicate with a smart phone, the energy source of a Wild Card becomes a challenge. There are thin-film batteries that can easily fit into a credit card dimension. However, requiring a user to charge the card periodically is unacceptable. Our key observation is that smart phones are portable energy sources, and people are used to charge them every day. As NFC becomes ubiquitous on smart phones, our goal is to leverage the same NFC interface for both communication and energy transfer purposes. The NFC energy harvesting is built into the NFC communication link implemented on the Wild Card; hence, the energy scavenging functionality does not incur extra hardware cost.

One of the capabilities for NFC on mobile phones is for RFID reading. Passive RFID systems depend on the RFID reader generating enough energy to power passive tags. UHF RFID tags that operate at 900MHz frequency band receive power through the RF field, while NFC (more specifically HF) tags operating at 13.56MHz receive power through magnetic coupling. Figure 9 shows a block diagram of an NFC reader and passive NFC tag.

The NFC reader generates a magnetic field using an inductor and capacitor circuit tuned to 13.56MHz, the tag also has a similar circuit tuned to the same frequency. When the tag is within close proximity to the reader, the magnetic coupling between the two coils generates voltage at the tag coil. This voltage is used to supply power to the tag. Unlike the magnetic coupling used in electric transformers, the magnetic coupling of tuned coils enables efficient energy transfer over short distances (typically several centimeters in NFC).

A NFC reader transmits data to the tag by varying the amplitude of the generated magnetic field; while, the tag transmits data back to the reader using *load modulation*, where the tag changes the electric load seen by the reader by turning on and off a capacitor across the tag's tuned coil.

Since an NFC-enabled phone need to communicate with passive tags, the phone generates a strong magnetic field that enables a significant amount of energy harvesting using a tuned coil placed next to the phone.

There are two distinct opportunities for energy harvesting from the magnetic field generated by the phone. First, when the phone generates NFC messages, such as when communicating with the Wild Card, the NFC reader generates the magnetic field. Second, as reported by previous work, the phone generates a periodic magnetic field with 10% duty cycle under unlocked screen while searching for NFC enabled devices in the background [2]. As we show later, Wild

Card can scavenge enough energy during these operations for continued operation under typical usage, without draining extra battery from the phone. If necessary, it is possible to scavenge even more energy using the *subcarrier generation* technique described in [2].

Apart from communicating with passive tags, NFC also supports a peer-to-peer communication mode where both endpoints actively generates the magnetic filed in turn when transmitting data. Unlike passive tag mode, the active peer-to-peer mode incurs a high energy consumption due to the need for generating a magnetic field on both ends . Typically, a device with peer-to-peer capability can also acts as a passive tag when operating in the *tag emulation* mode. In our design, it is suffice for a Wild Card to serve as a passive tag.

Security

Security is a major concern when handling mobile payments. Our goals when designing the security framework of Wild Card are:

- it should have at least the same security level as conventional cards, and
- it should not make stealing other people's card numbers easier than today.

In particular, we do not trust the network nor the mobile phone host. Network packets can be eavesdropped, and the mobile phone may contain malware that steals memory contents. We only trust the Wild Card issuers (WCI) and the cards themselves.

The keys for our security framework are a unique ID (called a CardID) on each Wild Card and an associated secret key (called a CardKey) that is only shared between the WCI and the Wild Card. A WCI is an entity that is trusted by credit issuers, such as banks. When a user obtains a Wild Card, the WCI links person's identity to the CardID. We separate our discussions between managing newly issued cards and importing existing cards.

New Accounts

When a bank issues a new credit account to a user, it generates a credit card number and associated information to appear on typical magnetic stripes, which will be what it expects to receive from the merchants to finish a transaction. The bank contacts WCI, which encrypts the card information using the Wild Card's secret CardKey. The encrypted message is sent to the user and uploaded to the mobile payment app. A side advantage of the design is that the banks no longer need to mail new cards physically to users.

At the time of use, a user start from selecting a card from the smart phone. When the card is selected, the corresponding encrypted card information is sent to the card. The microcontroller in the card decrypts the message and obtains the magnetic stripe contents, which will be played out when user swipes the card. Since only the card has the decryption key, even other cards or sources obtained the encrypted card information, they cannot create the right magnetic stripe contents.

Existing Accounts

To import existing accounts, the WCI must verify that the user is the real owner of the account. Otherwise, the Wild Card can be used to steal anyone else's credit card number. To achieve this, upon receiving an importing request, the WCI will make a few small transactions to the card account. The user is expected to verify the transactions with the bank, and report the exact the transaction amounts. This is the same mechanism that some online payment system, such as PayPal, validated registered credit cards.

Once validated, the WCI will encrypt the card information and send it to the user, similar to the procedure for new accounts.

Lost Phone or Card

Losing the phone or the Wild Card should not be worse than losing one's wallet or a card today. The mobile app itself can be protected by a password (similar to other banking mobile apps). Additional security measured can be added to the card. For example, the card can have buttons so that the user must unlock it with a pin. The information on the card can expire after a fixed number of swipes. In addition, when a user realizes that the card is missing, a single phone call to WCI can invalidate all accounts associated with it, comparing to numerous phone calls today to each card issuers.

In summary, the card is protected in the following sense:

- If the phone is stolen, requests for a new card will not be authenticated because the attacker does not have the right pin for accessing the mobile app.
- If the attacker buys a new Wild Card, she cannot program the Wild Card with a valid card number (clone a card) without authenticating herself to the bank first and encrypting the data with the card secret key. This prevents the wild card from becoming a universal credit card generator.
- If the adversary steals someone's Wild Card, the information on the card is safe if the Wild Card is locked with a pin code. The card is still safe even if the phone and card are both stolen since the adversary needs the pin for both the phone and the card. Even without a pin on the card, the attacker can only use the card for a small number of times, so the damage is contained.

The technical challenge for protecting security of the card is to choose a cryptography system that imposes minimum overhead on the energy budget of the card. The card data has to be processed before it is presented on the magnetic stripe. For example, it has to be verified and decrypted and then it has to be translated into 0 and 1 signals. Due to the energy limitations of the card, a low-power microcontroller with small amount of RAM and storage is the best fit, similar to other low-power designs [11, 12, 20]. Therefore, the

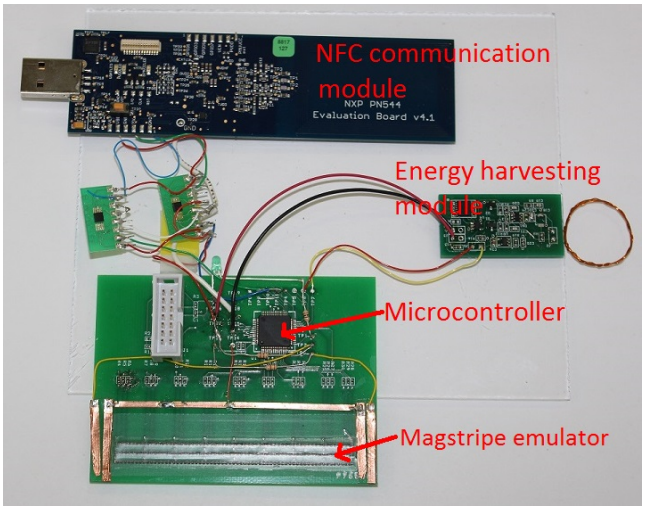

Figure 10. Wild Card prototype showing the NFC communication module, energy scavenging module, the microcontroller, and the magnetic stripe emulator

.

crypto system has to be chosen carefully to fit within the computational capabilities of the card. We discuss our implementation choice in the next section.

PROTOTYPE IMPLEMENTATION

Without an manufacturing process for full integration, we have implemented and tested the key features of Wild Card on custom made hardware. A conventional multi-track swipe-through card reader successfully read the card and received the stored information on two tracks of the card. Figure 10 shows how the Wild Card is implemented in hardware based on the architecture we explained before.

Hardware Components

Our prototype of the Wild Card included the following components:

Low-Power Microcontroller: We chose MSP430F2418 from Texas Instrument [18] to process the data and send the corresponding signal to the dynamic magnetic stripe. This microcontroller has 8 KB of RAM, 116 KB + 256 B of flash memory. The MSP430F2418 is ultra low-power and consumes $365\mu A$ in active mode when operating at 1MHz, and consumes only 0.1μA in the deep sleep mode.

NFC Controller: Our prototype uses the PN544 NFC controller from NXP. This is an NFC controller typically used as the NFC reader chip on mobile phones. However, as we described later, Wild Card uses the NFC tag emulation mode for communication. The processing and hardware functionality needed for tag emulation mode is almost identical to the resource requirements of the IC used in a passive NFC tag. The physical size of these tag ICs enable them to be seamlessly integrated in to paper-thin RFID tags. For example, the NTAG210/212 passive NFC tag IC from NXP has a 0.6 mmx0.5 mm area and is 0.075 mm thick, which makes it possible to easily integrate these tags in the Wild Card.

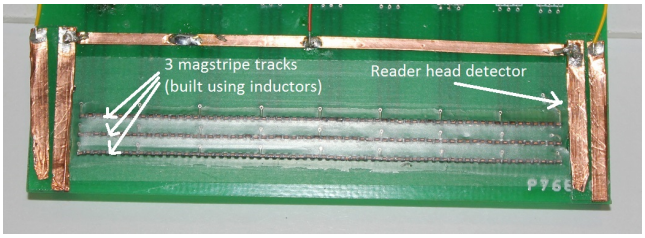

Figure 11. The prototype magnetic stripe emulator showing the reader head detector and the three magnetic stripe tracks. The tracks are implemented by connecting a number of miniature inductors in series

.

Battery: The energy harvested through NFC is stored in two MC201 rechargeable batteries from Infinite Power Solutions [16]. Each battery has a 1 mAh capacity, and can support up to 40 mA discharge current at 4.1 V and 7.5 mA. Since a single battery cannot accommodate the current requirements for driving the magnetic stripe, we use two batteries connected in parallel. The two battery stack occupies a 12.7mm x 12.7mm area and has a thickness of 0.34mm. This thickness is well suited for embedding in the 0.7mm thick Wild Card.

Power Management: Various power management functions, such as battery charging, and voltage regulation are handled by a MAX17710 energy harvester IC. In addition managing the battery charging, this IC has a dual-mode voltage regulator optimized for both heavy and light loads. Under the heavy load mode, this chip consumes 0.75 μA while under light load mode it consumes only 0.15 μA.

While the Wild Card is not playing back the magnetic bit pattern or not actively communicating with the phone, the microcontroller enters a deep sleep mode while putting other submodules such as the power manager into low-power mode. In this low-power mode, the Wild Card consumes < 1 μA. However, as soon as the swiping at a payment terminal starts, the microcontroller must wake up and start playing back the magnetic bit pattern. Since the microcontroller and the rest of the submodules can wake up within several milliseconds once an interrupt is detected, we use a head detection circuit at either end of the wild card to detect the presence of the reader head. Figure 11 shows the current prototype implementation where two exposed copper strips are short circuited as the reader head moves over them. A production version of the Wild Card could use tactile dome switches for reader head detection (e.g. the *P-series* tactile dome switches from Snaptron).

Magnetic Stripe Emulator

We implemented a magnetic stripe emulator prototype consisting of all the three tracks that can fits inside a standard sized payment card. We face two challenges when implementing the prototype: First, the magnet has to be thin enough to fit in 0.7mm thick card, while generating a strong enough magnetic field that ca be detected at the reader head. Second, the closely placed magnetic stripes should be magnetically isolated, so that they do not cause interference among each

other. We built a prototype that meets these criteria using a string of ferrite-cored inductors connected in series. We use 0402AF-561XJLU miniature wire-wound inductor from Coilcraft. These inductors have a 0.66 mm x 1.12 mm area and a 0.66 mm maximum thickness. This small thickness enables them to be embedded in the 0.76 mm thick Wild Card.

Figure 11 shows a picture of our prototype where a series of closely-spaced inductors were hand soldered to emulate a single long inductor spanning the entire length of the card per track. During evaluation, we observe that the discontinuities in the magnetic field due to imperfect fitting of individual inductors causes reader bit errors, we can reduce the impact due to these imperfections by covering the magnetic strip with a thing ferrite sheet; however, the ferrite sheet reduces the magnetic field strength since it absorbs some of the magnetic field.

We note that a large scale manufacturing of the Wild Card would use custom built, long, narrow, ferrite-cored inductors which would prevent the performance degradations due to these imperfections.

The two endpoints of each inductor string (corresponding to a single track) are connected to two GPIO pins of the microcontroller. To generate the magnetic filed, the GPIO pin connected to one end is set to output log 1, while the other end is set to output logic 0. To switch the direction of the magnetic field, the logic levels of the two ends are reversed. When the stripe is not active, the two GPIO pins are configured as inputs to save power.

The playback of the card content is driven by a timer interrupt. Since track 2 is 3 times less dense than track 1, the timer interrupt is set to the rate of playing back track 1 in 150ms. Track 2 is activated for every 3 interrupts. We obtained the credit card contents from a standard card reader. Since it does not report the error checking LRC code, we also generate the code in software.

NFC Communication Channel

We implemented the NFC communication using PN544 [1] development boards, one in the initiator mode (to emulate the phone) and one in target mode (on the card side).

Once the initialization for both initiator and target chips is done, the initiator tries to discover and activate the remote NFC target. When the NFC target has been activated, the initiator receives a message about this event (NXP_EVT_NFC ACTIVATED). Then, the two chips create and open a communication channel (pipe) between each other and the target informs the initiator that it is ready to receive messages (NXP_EVT_NFC_RCV_DATA). The code for target side was tested on the TI MSP430F2418 and the initiator code was run on a PC and the two chips could successfully communicate. The NFC initialization took about 150 ms and the data exchange between the two chips was about 600 ms at the data rate of 106 kbps.

EVALUATION OF THE WILD CARD

Wild Card is powered by the energy scavenged from the phone's NFC transmissions. Here we examine the feasibility of operating the Wild Card entirely from the scavenged energy. When at deep sleep, Wild Card consumes $< 1\mu$A of power, while it consumes $simeq$ 70mA during mag stripe emulation. A single magnetic stripe emulation lasts $simeq$ 150ms.

With power scavenging coil of 2.5cm diameter, Wild Card can scavenge 30mW at the scavenging coil when the phone screen is unlocked. Since the background NFC tag scavenging has a 10% duty cycle. The effective average power scavenged drops to 3mW. Assuming a worst case efficiency of 50% due to voltage regulator power loss and power loss during battery charging and discharging, the energy scavenging delivers an average effective power of 1.5mW. With a 4.2V battery, this translates to a charging current of 0.35mA.

Based on a recent survey, a person interacts with their phone $simeq$ 2.5 hours per day. Assuming only 1 hour of interaction, Wild Card scavenges 0.35mAh of energy per day. A leakage current of 1μA results in 0.024mAh energy consumption per day. Which leaves 0.3mAh of energy for magnetic stripe operation.

With each card emulation requiring 0.003 mAh of energy, with 0.3mAh Wild Card can support up to 100 card emulations per day. Given that this is larger than the typical usage, the rechargeable battery will gradually fill up. A fully charged battery (2 x MC201 batteries) has 2mAh capacity. hence, the Wild Card can perform $simeq$600 card emulations.

Cost of Security

The RC5 [13] algorithm has been implemented on low-power and even battery-less platforms before and it has been shown that it is an energy efficient choice [7]. For example, data decryption consumes 5.56μJ for 64-bits of data and 16 bytes of secret key [3] and the one time key setup would require 25.75μJ.

However, we note that the security operations on Wild Card happen during the interaction with the phone. During this interaction, Wild Card continues to scavenge power from the NFC at $simeq$ 100% duty cycle. Further, these interaction happen only when the user adds new card information to Wild Card, which is an infrequent activity. Hence, the security related energy overhead does not impact the overall performance of Wild Card.

Physical Implementation Feasibility

The 86 mm x 54 mm x 0.76 mm credit card creates a physically constrained space when implementing Wild Card. In this section, we discuss if full Wild Card functionality can be implemented on a credit card size device.

We successfully demonstrated that the 3 magnetic strip tracks can be embedded on a credit card using off the shelf components. It would be relatively straight forward to implement

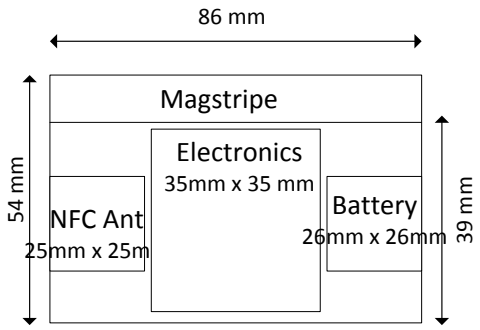

Figure 12. Approximate allocation of Wild Card physical area for implementing different HW features.

a customized solution within the same space constraints. In addition to the space occupied by the magnetic stripe, the credit card has 86 mm x 39 mm area for implementing the rest of the Wild Card features (Figure 12). The NFC antenna takes 25 mm x 25 mm, while the battery takes 26 mm x 26 mm area. The antenna will be implemented using a thin metal sheet, similar to the paper-thin antennas used in HF RFID tags. The two batteries are stacked on top of each other with a total thickness of 0.34 mm. Hence both the antenna and the battery can fit within a 0.74mm thick card.

This leaves 35 mm x 35 mm area for the rest of the electronics. off the shelf electronic components are typically thicker than 1mm, hence exceed the card thickness. However, for large scale manufacturing, these components are available in much smaller sizes. One example is the SimFi [14] radio module that contained full functional WiFi radio within a Mini-SIM module of 0.76 mm thickness. Given the electronics in a WiFi module (radio, baseband processor etc.) is much more complex than those required for Wild Card, and the area available is larger than the size of a Mini-SIM module, all the electronics should easily fit inside the 35 mm x 35 mm area.

USABILITY DISCUSSIONS

Our prototype and evaluation only includes the stripe emulation and NFC parts. There are several other features a commercial Wild Card need consider.

- Display. There is information on a physical credit card that is not on the magnetic stripe, for example, the CCA code. This allows the credit card processor to validate the presence of the card at the time of transaction. Other contents, such as bank logos, card designs, and network logos, are important parts of a card identity. E-ink type of displays is mature for this purpose. The advantages of E-ink displays are their thickness, flexibility, and energy efficiency. Once programmed, while the Wild Card is with the phone, the display does not require any energy to maintain the images. The back of the card can have an authorized signature, like conventional cards.

- Buttons. The card can embedded a number of buttons within its thickness. They can be used to enter user pins to unlock the card, or to select among a few commonly used cards without programming it every time.

- Contactless mode. Since the Wild Card already has a NFC circuit, it is easy for it to emulator a contactless card just like the mobile phones. So, a Wild Card can be forward compatible if the societal payment infrastructure moves to contactless.

All these features can be easily supported by the energy budget on the card.

RELATED WORK

Mobile Payment Systems

Recently, there are many mobile payment systems being developed that use NFC for payment (e.g. Master Card PayPass, VISA PayWave, Isis Mobile Wallet™, and Google Wallet) and make payment at terminals that supports NFC. However, contactless *mobile wallets* are not backward compatible and cannot be used where NFC terminals are not supported. iCache Inc.[1] recently developed the iCache Geode Mobile Wallet that uses a phone case to program payment cards into one physical card. Protean Inc.[2] has a similar product called Echo. Both of these products require an additional device, like a magnetic stripe writer, to program the magnetic stripe for each new card. The Wild Card is self-contained and uses a microcontroller to program its dynamic magnetic stripe emulator. Dynamics ePlate™ [3] is another programmable payment card that uses a mobile app to allow selection of two cards at once. The card runs a battery that is expected to last three years but it is rechargeable by phone. None of the other solutions offer a centralized security framework. Account management systems (*wallet apps*) such as PayPal and Starbuck app that enable online payments but do not interact with merchants' terminals. The wild card allows for managing cards online but making payments in the conventional form when needed.

Security of payment systems and low-power devices

Fu et al. [6] discuss the weakness of RFID-enabled credit cards and show that the card information such as name and expiration time are communicated in plain text and It is fairly easy for an adversary to clone a RFID-enabled card. The programmable microcontroller of the wild card makes it simple to implement, improve, and test various security techniques designed for credit cards. Madlmayr et al. [8] analyze the Security and privacy of NFC devices and propose a set of guidelines to improve the current devices. The improvements must be done in the NFC architecture layer and implementing them would improve the security of the wild card which is build upon the NFC modules. Eisenbarth et al. [5] discuss different lightweight cryptography systems are designed for low-power RFID tags and smart cards. These systems are the right candidates for implementing encryption and message authentication schemes for the wild card considering its energy limitations.

[1] http://www.icache.com/
[2] http://getprotean.com/
[3] http://www.dynamicsinc.com

Energy Harvesting

Many forms of energy scavenging exist. The work closes to our technique is RF-based energy scavenging. Intel WISP [15] is a battery-less sensing device that harvests its energy wirelessly from a 915MHz RF signal using a multi-stage voltage multiplier. The UMass Moo [20] uses a similar technique for energy harvesting. Both of these systems are designed for UHF RFID communication, the wild card uses HF communication. Parks et al. [10] prototyped an energy scavenging system to harvest energy from a broadcast transmitter and a local cellular tower. They are able to harvest energy to power up a sensing device (with light and temperature sensors). Ambient RF energy scavengers if miniaturized enough can improve ubiquitous applications such as Wild Card.

CONCLUSION

This paper discusses the concept and technologies for the Wild Card, a programmable universal payment card. The Wild Card interacts with a mobile phone to receive both data and energy through NFC. To make the Wild Card programmable, we designed a magnetic stripe emulator that can be driven by a microcontroller to produce the magnetic field that is expected by card reader. We designed a security framework so the card information is safe and they cannot be used to steal other credit card contents. The backward compatibility and security of Wild Card makes it distinguishable from other mobile payment systems. Our evaluation of the Wild Card shows that the card can be swiped up to 100 times with just one charge from the phone. Our new mobile payment method allows people to manage their accounts easier and paves the road to replacing wallets all together.

REFERENCES

1. NXP NFC controller PN544 for mobile phones and portable equipment.
2. Hidden for blind review. Technical report, 2013.
3. H.-J. Chae, D. J. Yeager, J. R. Smith, and K. Fu. Maximalist cryptography and computation on the WISP UHF RFID tag. In *Proceedings of the Conference on RFID Security*, July 2007.
4. D. Contini, M. Crowe, C. Merritt, R. Oliver, and S. Mott. Mobile Payments in the United States: Mapping Out the Road Ahead. http://www.bos.frb.org/bankinfo/payment-strategies/publications/2011/mobile-payments-mapping.htm.
5. T. Eisenbarth and S. Kumar. A survey of lightweight-cryptography implementations. *Design Test of Computers, IEEE*, 24(6):522–533, Nov.-Dec.
6. T. S. Heydt-Benjamin, D. V. Bailey, K. Fu, A. Juels, and T. OHare. Vulnerabilities in first-generation RFID-enabled credit cards. In *Proceedings of Eleventh International Conference on Financial Cryptography and Data Security, Lecture Notes in Computer Science, Vol. 4886*, pages 2–14, Lowlands, Scarborough, Trinidad/Tobago, Feb. 2007.
7. C. Karlof, N. Sastry, and D. Wagner. Tinysec: a link layer security architecture for wireless sensor networks. In *Proceedings of the 2nd international conference on Embedded networked sensor systems*, SenSys '04, pages 162–175, New York, NY, USA, 2004. ACM.
8. G. Madlmayr, J. Langer, C. Kantner, and J. Scharinger. Nfc devices: Security and privacy. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pages 642–647, March.
9. R. T. I. . MAGTEK. I/O interface for TTL magnetic stripe readers technical reference manual, December 2003.
10. A. Parks, A. Sample, Y. Zhao, and J. R. Smith. A wireless sensing platform utilizing ambient rf energy, 2013.
11. J. Polastre, R. Szewczyk, and D. Culler. Telos: enabling ultra-low power wireless research. In *Proceedings of the 4th international symposium on Information processing in sensor networks*, IPSN '05, Piscataway, NJ, USA, 2005. IEEE Press.
12. B. Priyantha, D. Lymberopoulos, and J. Liu. Enabling energy efficient continuous sensing on mobile phones with littlerock. In *Proceedings of the 9th ACM/IEEE International Conference on Information Processing in Sensor Networks*, IPSN '10, pages 420–421, New York, NY, USA, 2010. ACM.
13. R. L. Rivest. The RC5 encryption algorithm. In B. Preneel, editor, *Fast Software Encryption*, pages 86–96. Springer, 1995. (Proceedings Second Int'l Workshop, Dec. 1994, Leuven, Belgium).
14. Sagem and Telefnica. SIMFi, a SIM Card With Built-In Wi-Fi Hotspot. http://tinyurl.com/ydn4aw6, 2010.
15. J. R. Smith, A. P. Sample, P. S. Powledge, S. Roy, and A. Mamishev. A wirelessly-powered platform for sensing and computation. In *Proceedings of the 8th international conference on Ubiquitous Computing*, UbiComp'06, pages 495–506. Springer-Verlag, 2006.
16. I. P. Solutions. THINERGY MEC225 solid-state, flexible, rechargeable thin-film micro-energy cell. http://tinyurl.com/apsmkxu, 2012.
17. Technavio. Global NFC PoS Terminal Market 2011-2015. http://www.technavio.com/content/global-nfc-pos-terminal-market-2011-2015.
18. Texas Instruments Incorporated. MSP430 Ultra-Low Power Microcontrollers. http://www.ti.com/msp430.
19. M. Valles. How has the number of credit cards per US household changed since 2008? http://tinyurl.com/bwum52y, 2012.
20. H. Zhang, J. Gummeson, B. Ransford, and K. Fu. Moo: A batteryless computational RFID and sensing platform. Technical Report UM-CS-2011-020, Department of Computer Science, University of Massachusetts Amherst, Amherst, MA, June 2011.