Vulnerabilities in First-Generation RFID-enabled Credit Cards*

Thomas S. Heydt-Benjamin[1], Daniel V. Bailey[2], Kevin Fu[1], Ari Juels[2], and Tom O'Hare[3]

[1] University of Massachusetts
Amherst, MA, USA
{tshb, kevinfu}@cs.umass.edu
[2] RSA Laboratories
Bedford, MA, USA
{dbailey, ajuels}@rsa.com
[3] Innealta, Inc.
Salem, MA, USA
tom@innealta.com

Abstract. RFID-enabled credit cards are widely deployed in the United States and other countries, but no public study has thoroughly analyzed the mechanisms that provide both security and privacy. Using samples from a variety of RFID-enabled credit cards, our study observes that (1) the cardholder's name and often credit card number and expiration are leaked in plaintext to unauthenticated readers, (2) our homemade device costing around $150 effectively clones one type of skimmed cards — providing a proof-of-concept of the RF replay attack for cards, (3) information revealed by the RFID transmission cross contaminates the security of non-RFID payment media, and (4) RFID-enabled credit cards are susceptible in various degrees to a range of other traditional RFID attacks such as skimming and relaying.

Keywords: RFID, credit cards, contactless, vulnerabilities

1 Introduction

An increasing number of credit cards now contain a tiny wireless computer chip and antenna based on RFID (Radio Frequency Identifier) and contactless smart-card technology. RFID-enabled credit cards permit contactless payments that are fast, easy, often more reliable than magstripe transactions, and require only physical proximity (rather than contact) between the credit card and the reader. An estimated 20 million RFID credit cards and 150,000 vendor readers [9] are already deployed in the U.S. According to Visa USA [9], "This has been the fastest acceptance of new payment technology in the history of the industry."

The conveniences of RFID credit cards also lead to new risks for security and privacy. Traditional credit cards require visual access or direct physical contact for retrieving information such as the cardholder's name and the credit-card number. By contrast RFID credit cards make these and other sensitive pieces of data available using a small radio transponder that is energized and interrogated by a reader.

Although RFID-enabled credit cards are widely reported to use sophisticated cryptography [4, 19, 23, 25, 41, 43], our experiments found several surprising vulnerabilities in every system we examined. We collected two commercial readers from two independent manufacturers and approximately 20 RFID-enabled credit cards issued in the last year from three major payment associations and several issuing banks in the U.S. We were unable to locate

* UMass Amherst CS TR-2006-055 under review. See www.rfid-cusp.org for the latest version.

public documentation on the proprietary commands used by RFID-enabled credit cards. Thus, we reverse engineered the protocols and constructed inexpensive devices that emulate both credit cards and readers. The experiments indicate that all the cards are susceptible to live relay attacks, all the cards are susceptible to disclosure of personal information, and many of the cards are susceptible to various types of replay attacks. In addition, we successfully completed a cross-contamination attack against the magstripe of one card. All but one of the other cards tested appear to be susceptible to the cross-contamination attack as well.

1.1 Background

Several large chains in the U.S. have deployed many thousands of RFID readers for credit cards: CVS Pharmacies (all 5,300 locations), McDonald's (12,000 of 13,700 locations), the Regal Entertainment Group of movie theaters, and several other large vendors [37, 42]. A vendor typically deploys an RFID-enabled credit card reader at each cash register. Each reader is continually polling for cards by broadcasting a radio carrier, and can speak with the major brands of RFID-enabled credit cards. A small number of manufacturers produce readers capable of speaking several proprietary protocols. In our collection of approximately 20 RFID-enabled cards issued in the last year, we have observed four semantically different protocols between the card and reader.

Scope of current deployment: Reports estimate the deployment of 20 to 55 million RFID-enabled credit cards in comparison to 398 million conventional credit cards [5, 9, 37]. In addition to traditional payment contexts, RFID-enabled credit cards are becoming accepted in other contexts such as public transportation [24]. The New York City subway [40] recently started a trial of 30 stations accepting an estimated 100,000 RFID-enabled credit cards [10]. A participant in this trial uses her credit card as a transit ticket as well as a credit card in place of the traditional magstripe-based dedicated subway tickets.

Integration of RF technology into existing credit-card infrastructure: The RFID payment cards that we examined seem to have been designed specifically for easy integration into the existing payment-authorization infrastructure. For instance, even though no magnetic stripes are read during an RF transaction, the RFID credit card readers that we examined reformat received RFID data into "Track 1 Data" and "Track 2 Data" before passing it along to point-of-sale terminals. In other words, data is presented to the charge-processing network in the same format regardless of whether the credit-card reader received the information from an RF transaction, or a traditional swipe of a magnetic strip.

Sometimes, as a defense against magstripe skimming, a human enters an additional piece of data: the card validation code (CVC), which is printed on the card but not contained in the magstripe. These data are sent to the back-end infrastructure, which returns an approve-or-decline decision.

Our work focuses on the first step in a long chain of system interactions: card presentation. Over years of operational experience, credit card issuers have gained expertise in detecting fraudulent transactions by tracking patterns of behavior [13]. Fraud detection and prevention mechanisms address many but not all of the concerns raised by exposure of credit card data. Detecting fraud is an effective defense against many types of financial risk, but is not effective against *preventing* invasion of privacy. Our study considers vulnerabilities to privacy that today's anti-fraud methods do not prevent.

Communications protocol used by RFID credit cards: The radio interface of all of our credit cards uses a communications protocol specified by the International Organization for Standardization in a series of documents titled ISO 14443-1 through 14443-4 [29]. There are two protocols specified in this standard, but our cards speak the B protocol.

All devices observed in our experiments begin each transaction with a standard layer-3 handshake. After this handshake is complete, further communication is at layer 4, the application layer. It is at this point that proprietary commands come in to play, as opposed to the commands that are specified in public standards. ISO 14443-4 can carry arbitrary commands at the discretion of the application designer, with each command wrapped in a layer 4 envelope broadcast over the ISO specified transport layer (layer 2).

2 Related Work

RFID-enabled credit cards share many of the challenges and approaches for security and privacy as other RFID-based authentication and identification systems.

2.1 RFID authentication and cloning

Several types of RFID tags merely emit static identifiers. Electronic Product Code (EPC) tags [27], which are designed in effect to serve as next-generation, wireless barcodes, are an example. Although proposed as an anti-counterfeiting tool for use in, e.g., pharmaceutical supply chains [17], EPC tags provide no explicit authentication features. In principle they are easy to clone: An attacker need merely create a radio device that emits the same static information as a target EPC tag. (With certain enhancements, however, EPC tags can offer some resistance to cloning [31].)

Certain types of proximity cards, the RFID-enabled cards that provide building access in lieu of physical keys, similarly do no more than emit static identifiers. Westhues has demonstrated a simple, inexpensive device that can skim proximity cards at a distance—even through walls—and then simulate them, thereby undermining their security functionality [46]. The VeriChip, a human-implantable RFID tag proposed for use as an authenticator, appears to operate in the same way and to be similarly vulnerable to cloning [20].

E-passports, a new form of passport being deployed this year, incorporate RFID tags as data carriers. As the technical specifications for e-passports make clear [26], and as a security consultant has recently demonstrated [48], the RFID tags in basic e-passports are also subject to straightforward cloning attacks. The data carried by e-passports, however, include digital signatures, so that while cloning of an e-passport is relatively easy, modification of its data contents is largely infeasible. Since e-passports include biometric information, such as facial images, copying does not directly permit impersonation, and therefore may not undermine system security in a general sense. On the other hand, the technical guidelines for e-passports allow a number of deployment options, and Dutch passports, for example, have proven vulnerable to eavesdropping due to poorly formed cryptographic keys. [33] provides an overview.

Certain RFID devices employ cryptographic operations as a countermeasure to cloning. Some, like the NXP (formerly Philips) Mifare DESfire [38] include strong, industry-standard ciphers which, in the absence of direct physical attack, render cloning largely infeasible. Contactless smartcards—effectively short-range RFID tags with ample processing power—can execute strong cryptographic primitives such as digital signatures.

Other RFID devices, however, incorporate less robust cryptography. For example, one of the first widely-accepted RFID payment systems in the U.S. is based on the Digital Signal Transponder (DST), a cryptographically-enabled RFID device manufactured by Texas

Instruments (TI). It is present in the ExxonMobil Speedpass, and still popular today. Over seven million customers possess Speedpass tokens. Additionally, the TI DST operates as a theft deterrent in over 150 million automobiles worldwide. Unlike the credit cards we examined, Speedpass does not carry personally identifiable information, e.g., the name of its owner.

In late 2004, researchers at Johns Hopkins University and RSA Laboratories reverse-engineered the proprietary, unpublished cipher in the DST [8]. Each individual DST device is programmable with a unique cryptographic key. As this key is only 40 bits in length, however, the researchers were able to demonstrate practical cloning attacks against the DST. By "skimming" a pair of challenge-response readings from a target tag, they were able to recover its cryptographic key by brute-force search in under thirty minutes using a small number of FPGAs.

2.2 Read ranges

Industry claims around the security of RFID devices often hinge on their short read ranges. Some cautionary notes are in order, however. As discussed in [32], RFID tags do not have a single, definitive read range. While the *nominal* read range of an RFID tag may be quite short, on the order of several centimeters, for example, a non-standard reader or large antenna can provide a significant boost in range at which an attacker can skim an RFID tag. Hancke [22] has recently demonstrated skimming ranges of over 20cm for RFID systems in which most readers operate at a distance of only several centimeters, while Kfir and Wool have hypothesized a possible skimming range of up to 50cm for ISO 14443-B [35]. Furthermore, while skimming requires that a reader power the targeted tag, an attacker performing passive eavesdropping on a session between a legitimate reader and RFID tag can potentially harvest tag data at a considerably longer range. Claims have surfaced of tests in which e-passports, which rely on ISO 14443-A and 14443-B, were read at a distance of 30 feet [47][4] and detected at a distance of 20 meters [15].

We make no claims in this paper about the read ranges of RFID-enabled credit cards beyond the fact that characterization of these ranges is not straightforward and constitutes an important open research question.

3 Threat Model

An RFID-enabled credit card implements one of at least four different over-the-air protocols. While all the protocols we observed have the same general intent – to deliver a string of data strongly resembling an ISO 7813 magstripe – the details vary somewhat. Our focus is on observing and manipulating these protocols, rather than the myriad other means of perpetrating financial fraud like physically probing the cards, analyzing side channels, or social engineering and phishing. While formal RFID threat models have already been well explored [7, 33], the application-specific nature of our work lends itself to informal scenarios specific to these RFID credit cards.

3.1 Attacks and scenarios

Our informal analysis considers five basic attacks against privacy and security: *Tracking*, *Skimming*, *Eavesdropping*, *replay and relay*, and *cross-contamination*.

[4] While the referenced report is short on details, it seems likely that the tests involved passive eavesdropping of some kind, rather than direct skimming.

Tracking: In this scenario, a legitimate merchant exceeds the expected use of their RFID credit card readers. For example, a merchant A may want to know whether a credit card C has been used with any other vendor since the last transaction between A and C. Avoine describes examples of how such attacks on the cardholder's privacy could be implemented [6, 7]. Some of the cards we examined allow this sort of attack by means of a transaction counter that could be co-opted.

Skimming: In this attack an unauthorized and potentially clandestine reader reads tags from either close proximity or from a distance. One such skimming attack we call the "Johnny Carson" attack. In a famous series of comedic skits, Johnny Carson's character Carnac the Magnificent used his mental powers to read the contents of sealed envelopes. Since containers that are visually opaque are not necessarily RF-opaque, security measures sufficient for traditional credit cards such as "security envelopes" must be re-examined in the context of RFID-enabled cards. The Johnny Carson attack on RFID credit cards occurs when an attacker has access to the physical mail stream to read RF data from credit cards in transit to their owners. This attack is particularly powerful because the adversary gains accessory knowledge such as cardholder address, and because physical access to postal mail is commonly easy in many areas (such as dormitory mailrooms and side-of-the-road mailboxes).

Many other skimming attack scenarios exist, such as the "bump-and-run" close range skimming of the contents of a victim's wallet while standing in a crowded line, elevator, or subway. Long range skimming attacks are even more diverse, but the absolute maximum read ranges for ISO 14443-B transponders have not yet been clearly established.

Even if the read ranges of RFID-enabled credit cards are short, their new uses and form factors will engender new opportunities for attack. Cards that support sufficient read range may tempt consumers to hold their wallets up to readers, rather than to remove their cards first. For instance, consumers are trained to present ATM cards to devices that look like ATMs [2]. A compromised reader at a parking garage could skim customers' credit-card information at the same time that they read the parking pass. Fob-type RFID credit cards are now available for attachment to key rings, exposing them to attack when consumers leave their keys unattended. This behavior is seen most often in valet-parking situations, or in gymnasiums where it is common for users to leave their keys together in an unsecured box by the door. The fact that such cards may not bear embossed numbers can create a false sense of security in addition to the fact that consumers are skilled at protecting their wallets, but as we have seen, often leave their keys exposed.

Eavesdropping: In an eavesdropping attack, an adversary uses an antenna to record the communication between a legitimate RF device and reader. Because the eavesdropping happens on live communication (e.g., during a purchase at a store), foil shielding does not help to prevent this particular attack. The eavesdropping feasibility depends on many factors, including read distance.

Replay and relay: In a replay attack, an adversary broadcasts an exact replay of the transponder end of the radio signal recorded from a past transaction between an RF device and a reader. Where mechanisms exist to foil simple replays (such as time stamps, one-time passwords, and challenge-response cryptography) a related but more sophisticated attack can frequently still succeed. This attack, commonly known as the relay attack, uses a man in the middle adversary to relay an ephemeral connection from a legitimate reader through one or more adversarial devices to a legitimate tag which may be at a considerable distance. The distance at which the relay attack can succeed is limited only by the latency which will be

tolerated by the attacked protocol. However, many portions of ISO-14443-B are extremely tolerant to latency.

Cross contamination: The cross contamination attack occurs when private information such as cardholder name, number, and expiration date learned by an adversary in an RF context are then used by the adversary in a different context. For example, the adversary could use this data to create a magstripe card, re-encode the stripe on an existing card, or use these data in a card-not-present transaction such as a telephone or online mail-order purchase.

4 Methodology and Experiments

Our experiments used two different kinds of commercial readers that read RFID credit cards and produce serial output compatible with standard charge-processing networks according to ISO 7813 [30]. This is the standard that is used for the magstripe data on a standard credit card. One of these readers was obtained used from a company at which it is the standard POS (Point Of Sale) interface at hundreds or thousands of locations nationwide. The other reader was obtained new, and is also of a common type used at POS locations.

Our conclusions are based on observations from a sample set of approximately 20 credit cards obtained in 2006. Several different issuing banks and the three largest payment associations in the U.S. are all represented.

4.1 Eavesdropping experiments

Our eavesdropping hardware consisted simply of a tuned 13.56MHz antenna connected to an oscilloscope. Using this setup we obtained oscilloscope traces of complete transactions between various RFID credit cards and our various commercial readers. The serial output obtained from the readers during these transactions was saved for later correlation.

The raw oscilloscope trace was sufficient for determination of carrier frequency and RFID protocol due to the characteristic 10% amplitude modulation associated with the ISO 14443-B [29] RFID protocol. Simple signal analysis software based on information in section 3 of the ISO 14443-B specification was used to process scope traces. This analysis revealed that all of the data transmitted by the credit card reader consisted of well-formed ISO 14443-B layer 3 and layer 4 commands. Since this ISO protocol specifies that a cyclic redundancy check be transmitted with each command, we were able to confirm the accuracy (no garbled bits) of our analysis of each command. BPSK demodulation of PICC transmissions revealed that all PICC communications also conform to the ISO-14443-B protocol.

Our hardware and software are able to capture and demodulate any data transmitted between RFID credit card readers and cards that are within a certain distance of the eavesdropping antenna. Since the focus of this work is not on extending read ranges, we did not try to achieve great range. But we did experimentally demonstrate that eavesdropping with our setup is effective through materials such as cloth, lending credence to the threat of clandestine eavesdropping, perhaps through clothing.

Examination of data obtained through these means immediately demonstrated the efficacy of the simple eavesdropping attack, since the full cardholder name and card expiration date were present in cleartext in all transactions. Other data such as credit card number are discussed in Section 5.

Fig. 1. Our assembled PICCAL credit card emulator

4.2 Skimming experiments

In our first skimming experiment we took a commercial RFID credit card reader described above and determined that when presented with an RFID credit card it produced serial output in conformance with the ISO 7813 Track 1 and Track 2 format. Since this is the exact data that is normally transmitted by a POS terminal to a charge processing network, we note that this extremely simple skimming attack is clearly sufficient for perpetration of certain kinds of financial fraud.

In order to perform more flexible active attacks against RFID credit cards, we built a device capable of impersonating our commercial RFID credit card readers. We required only the ability to send arbitrary bytes according to ISO 14443 layers 2 and 3, and we discovered that the Texas Instruments s4100 Multi-Frequency RFID reader possessed all of the hardware capabilities that we required. This hardware together with applications of our own design allows us to rapidly challenge cards at a rate far exceeding that observed on any commercial hardware. In addition, this same hardware combined with custom amplifiers provides the basis for some noteworthy read range extension experiments [36].

Using libraries of our own design, we wrote a program which simply sends the exact bytes that we captured from the commercial readers in our eavesdropping experiments. Eavesdropping on transactions between our credit card reader emulator and real RFID credit cards demonstrated that all of the RFID credit cards we tested responded to our emulator exactly as they respond to a commercial RFID credit card reader. This strongly suggests that cards operate in a "promiscuous mode" interacting with any reader, with no cryptographic or other secure mechanisms in use to authenticate an authorized RFID reader to a credit card before it releases sensitive information.

4.3 Replay experiments

An RFID credit card belongs to a class of RFID devices known in the ISO standard as a "proximity integrated circuit card" (PICC). Since the primary difference between our device and a traditional PICC is that ours uses actively powered logic circuitry as opposed to the passively powered (antenna powered) RFID credit card, we have named our device a PICCAL (Proximity Integrated Circuit Card with Active Logic).

Our PICCAL is a microprocessor controlled device capable of sending arbitrary bytes over the ISO 14443-B transport layer (layer 2). For ease of prototyping and flexibility of experimentation we chose the gumstix single board computer as the controller for our device. This computer is approximately the size and shape of its namesake stick of chewing gum, and incorporates an ARM PXA255 microprocessor [28]. Four General Purpose Input/Output pins (GPIOs) of the microprocessor are used to control simple radio circuitry of our own

Card Type	Payment Association	Privacy Invasion?	Relay Attack?	Cross-Contamination?	Replay Attack?
A	1	Yes	Yes	Yes	Yes**
B	2	Yes	Yes	Yes	Maybe
C	3	Yes	Yes	No	Maybe
D	1	Yes	Yes	Yes*	Maybe

Table 1. A summary of susceptibility to various attacks for the four semantic types of cards (A, B, C, D) from three payment associations (1, 2, 3). * This attack proven in the field. ** This card admits unrestricted replay, while the others induce a race condition.

design. The small size and low power requirements of this single board computer contribute the feasibility of clandestine use of a PICCAL.

Our analog front end is essentially a simple AM radio consisting of three integrated circuits, and a few capacitors and resistors. The integrated circuits are: a comparator used to demodulate AM commands from the PCD, a counter/divider to divide the input carrier into subcarrier and baud rate clocks, and an XOR to allow the microprocessor to accomplish phase shifting for the 14443-B layers 2 and 3 specified binary phase shift keying.

We programmed our PICCAL to expect the RFID credit card reader commands that we captured using our eavesdropping setup described in Section 4.1, and to transmit replies captured from real RFID credit cards during a skimming attack performed with the reader emulator described in Section 4.2. The output from our commercial RFID credit card readers is identical in the case where the reader is presented with a real versus PICCAL emulated credit card. Since the data thus output is the same data we would expect to be transmitted over the charge processing network, we cannot think of a scenario in which the charge processing network could distinguish a real card from a PICCAL unless additional elements are present that we have not been able to observe in the laboratory. But as noted above, many pieces of data go into an overall transaction approval decision including sophisticated risk-based fraud detection mechanisms on the backend. For this reason, a valuable future research direction would include field tests in which PICCAL initiated transactions are tested with complete purchases from real merchants.

5 Analysis and Results

To protect the identity of our cards, we label the cards A, B, C, and D based on semantic equivalence classes determined by observing behavior between cards and readers. Table 1 summarizes the vulnerabilities of four classes of cards.

5.1 RFID credit card protocols

In a traditional card-present transaction, data is read from the magnetic stripe of a credit card by a POS terminal. The format of this data is specified by ISO 7813.

In this section we shall explore some of the RFID credit card protocols that are in current deployment. We shall examine some of the conclusions that can be reached through examination of the ISO 7813 data output by the serial port of RFID credit card readers when presented with different types of credit cards. Where pertinent we shall consider in correlation with this serial output the raw RF data from the same transactions as captured by our eavesdropping apparatus.

In keeping with a philosophy of ethical attacks research, we have redacted several pieces of information from the following subsections in part due to a desire to prevent criminal misuse of our findings. Cardholder name and card number have been concealed. Additionally we

have obscured the number of digits in the card number in order to obscure which observations correlate with the products of specific payment associations and issuing banks.

Card A protocol: When presented (RF transaction) with any sample of a card of type A, our reader outputs serial data identical to the data contained on the magstripe of the same credit card. This finding was confirmed by comparison with output obtained with presentation of the magstripe rather than RF. When presented with the same card, the output is always the same: in the serial output there is no evidence of a counter, one-time-password, or any other mechanism for prevention of replay attacks.

Figure 2 shows a sample of this serial output, which includes all the usual components of an ISO 7813 magstripe. The first line represents Track 1. The start sentinel B is followed by the primary account number. Following the field-separator character, the cardholder name appears, followed by another field-separator and an "additional data" field. This field includes not only the card expiration date (in this case 06/2009), but also a long string of digits. The meaning of these additional digits is not clear, but since this field is static for card type A, it cannot be used to prevent a replay or cross-contamination attack.

The second line represents standard Track 2 data, which is largely similar to the Track 1 data. Track 2 does not contain the cardholder name, and contains less room for proprietary information.

```
Bxxxxxx6531xxxxxx^DOE/JANE^0906101000000000000000000000000000858000000
xxxxxx6531xxxxxx=09061010000085800000
```

Fig. 2. Serial output from a commercial reader after an RF transaction with a card from issuer A

Card B protocol: When presented with cards from issuer B, our commercial readers output data similar to that of the card A experiments, with a few important differences.

In the sample card B output shown in Figure 3 we note the presence of a counter, determined to be such because of monotonic incrementation with successive transactions. Additionally we observe three digits which change with each transaction in no pattern that we have identified. Because of the relatively high entropy of these three digits, we consider it likely that they are the output of some cryptographic algorithm which takes the transaction counter as an input. If this is the case, then the algorithm must also take a card-specific value like a cryptographic key as an input since we observe that different cards with the same counter value produce different codes. We speculate that these data may serve as a stand-in for the traditional CVC.

```
Bxxxxxx1079xxxxxx^DOE/JANE^0901101100000000000100000000000
xxxxxx1079xxxxxx=090110110000016 00221
Bxxxxxx1079xxxxxx^DOE/JANE^0901101100000000000100000000000
xxxxxx1079xxxxxx=090110110000074 00231
```

Fig. 3. Sample of reader serial output after RF transaction with a card from issuer B. In this sample we see a three digit code (shown in bold italic font), and a four digit counter (shown underlined).

Card C protocol: Card C's protocol differs from Card B's in a few crucial details:

1. its unique transaction codes are eight digits instead of three
2. its transaction counter, now located in the Cardholder Name field, displays only three digits instead of four
3. rather than sending the embossed card number over the air, it uses a fixed pseudonym

Shown in Figure 4 are transactions 017 and 018 from an issuer C RFID credit card. These transactions correspond to codes 10691958 and 40146036, seen both at the end of Track 1 and in different order at the end of Track 2. Note that the counter value in Track 2 is followed by a 0 instead of a 1, perhaps an indication to the back end processing network of a different algorithm.

Bxxxxxx2892xxxxxx^DOE/JANE 017^10011010***10691958***
xxxxxx2892xxxxxx=10011010***10691958***01700
Bxxxxxx2892xxxxxx^DOE/JANE 018^10011010***40146036***
xxxxxx2892xxxxxx=10011010***40146036***01800

Fig. 4. Sample output from an issuer C card differs from output of an issuer B. Transaction codes are shown in bold italic font, transaction counter is shown underlined.

Card D protocol: Card type D is similar to card type B in that some kind of counter and some kind of code are present. RF eavesdropping shown in Figure 5 indicates that a 16 bit counter and a 32 bit code of some sort are sent from a card of type D to a reader.

Card #1:
77 0F 9F 61 02 ***51 A0*** 9F 60 02 ***35 90*** 9F 36 02 04 19 90 00
77 0F 9F 61 02 ***C3 AF*** 9F 60 02 ***1D 5C*** 9F 36 02 04 1A 90 00

Fig. 5. These lines represent the raw bytes of the same command in two consecutive transactions transmitted over RF from a card of type D to an RFID credit card reader. In each case this command is the only PICC command in a complete transaction that differs by even a single bit. In this example a 16 bit counter can be seen incrementing (shown underlined). We also note the presence of a 32 bit code divided into two 16 bit words (shown in bold italics).

5.2 Analysis of some attacks as they pertain to RFID-enabled credit cards

Replay attacks: Replay attacks come in several flavors depending on what data are communicated from the credit card all the way to the back end charge processing network.

1. Unrestricted replay: A card that always reports the same data need be scanned only once. After that, the attacker can replay the captured data at will, and the processing network cannot detect any difference between a replay and successive transactions with a real card. Since we observed the serial output from real POS readers to always be static with respect to cards of type A, we conclude that cards of this type are susceptible to this attack.
2. Replay with Race Condition: A card that uses a transaction counter and rolling code poses more of a challenge if the back end processing network stores and checks counter values. In such a case, once transaction n has been accepted by the network, transactions

numbered less than n should be declined if presented. However, if an adversary skims a transaction from a card, perhaps with the Johnny Carson attack, and then replays that transaction to the network before the legitimate user has a chance to use their card, then the charge-processing network should accept the adversary's transactions, and actually decline the legitimate ones. Therefore, even if the counter and codes observed with cards of type B and C are cryptographically secure, these cards should still be susceptible to this attack. It's true that the attacker is faced with a counter synchronization problem, but these are far easier than the cryptographic problems on which we prefer to base our security whenever possible.

3. Counter rollover: If a transaction counter is the only changing input to a code, then the number of possible codes is clearly limited by the maximum possible transaction counter value. There are then two cases; in one the counter is permitted to roll over, repeating from the beginning, thus also repeating the codes from the beginning. In the other case the card refuses to engage in additional transactions after the counter is exhausted.
   In the first case, an adversary that enjoys sufficient time in proximity to a card can build a database of all possible counter values and their corresponding codes, and therefore can mimic all possible behavior of the target card. Cards of type B are susceptible to this attack.
   In the second case, denial-of-service can be perpetrated against the card if the attacker has sufficient time in proximity to exhaust the counter by repeated skimming. Our experiments determined that cards of type C exhibit this behavior.

Relay Attack: Even in the case of a card that combines a challenge-response protocol with a transaction counter, the relay attack may still succeed. In an example relay attack two adversaries M_1 and M_2 collude to perform a purchase at an innocent user A's expense. M_1 possesses a clandestine credit card reader emulator with a (non-RFID) radio link to M_2's clandestine credit card emulator. M_1 sits down or stands next to A, and M_1's device rapidly discovers A's credit card. M_2 receiving this signal approaches the POS terminal and initiates a purchase. M_2 presents his PICCAL to the POS terminal. The PICCAL receives commands from the POS terminal and relays them to M_1's device, which transmits them to A's credit card. A's card's responses are likewise relayed through M_2's device and are broadcast from M_1's PICCAL to the POS terminal. The purchase should succeed, and the cost will be charged to A. Observe that even with application-layer challenge-response or transaction-counter protocols, this attack will still succeed, as protocol messages will simply be relayed between the card and reader.

Cross-contamination attack: To analyze the feasibility of a cross-contamination attack, we took a credit card of type A, placed it in a sealed envelope, and performed a Johnny Carson attack by reading the card through the envelope using our custom programmed TI s4100 reader.

We combined the data thus obtained with address and telephone information looked up in the telephone directory given the cardholder name transmitted through the envelope (for postal mail, the attacker already knows the cardholder address!). Using only this information we placed an online purchase for electronic parts from one of our major research-parts suppliers. Our purchase was successful, and we conclude that the cross-contamination attack is effective for cards of type A – and we believe the attack would also work against cards of type B and D. With the exception of card type C, we have no reason to believe that it would not be effective against any merchant that doesn't require a CVC.

Of course, the processing rules of the payment associations vary. Since type C uses a different card number over RF than is printed on the face or encoded onto the magstripe

it should be possible for the charge processing network to distinguish between RF and traditional use of the card. Therefore some kinds of cross-contamination attacks on card type C can be prevented if the processing network declines transactions in which the RF card number is presented in other contexts, such as an online purchase. Whether or not this check is actually performed should be easy to test, but owing to legal concerns, we did not perform this tempting experiment.

Privacy Invasion and Tracking: Our eavesdropping transcripts show that personally-identifying information is broadcast in cleartext by every RFID-enabled credit card we have examined.

This must be considered a privacy vulnerability in that automated, full identification of a person carrying an RFID credit card is easily demonstrated in the lab, and should be feasible in the field. This vulnerability is compounded by the fact that an adversary could use the full identity disclosure of the RFID credit card to build up a database of associated pseudonyms based on other RFID tags with longer read range that a user may commonly carry. For example, item-level tagging is increasingly used especially in the apparel and footwear supply chains. An EPC tag embedded in a shoe may transmit only a serial number, but if this number can be correlated with a user's name just once, then the shoe serial number can be used to identify the same user later. Since some kinds of RFID tags have much greater read range than others, this kind of attack is worthy of consideration.

In addition, the transaction counter found in some of the cards could be exploited by a vendor: by storing the transaction counter, a retailer could tell how often the card was used to purchase goods from others. Heavy card-users might be targeted for specific advertising, for instance.

6 Countermeasures

In addition to fraud detection to limit financial risk, several other countermeasures could significantly reduce risk of fraud and invasion of privacy.

Shielding and blocking: One countermeasure to some cases of skimming and relay attacks is to ensure that credit cards are unreadable when not in use. A Faraday cage is a physical cover that assumes the form of a metal sheet or mesh that is opaque to certain radio waves. Consumers can today purchase Faraday cages in the form of wallets and slip-cases to shield their RFID-enabled cards against unwanted scanning [12]. Note that this countermeasure is useless when the card is in use, since a card must be removed from a shielded wallet before an RF purchase can be made. It is clear, however, that credit card companies should at least ship cards through the mail enclosed in a Faraday cage to obviate the dangers of the Johnny Carson attack.

A slightly more sophisticated approach to preventing attack against dormant RFID devices is to disrupt ambient RFID communication. A *blocker* tag [34] is a device that exploits RFID anti-collision protocols in order to simulate a vast collection of non-existent RFID devices, thereby obscuring real RFID tags in its vicinity. In principle, a consumer could confer protection on RFID-enabled credit cards in an ordinary wallet or purse by positioning a blocker tag near them. On removal from the protected environment, a credit card would then operate normally. Or perhaps the blocker could contain a button or other means for a consumer to authorize card use.

Signaling cardholder intent: As an alternative approach to protection, it is possible, of course, to modify the credit cards themselves so that they activate only on indication of user intent. A simple push-button [44] would serve this purpose, but more sophisticated sensors might serve the same purpose, such as light sensors that render cards inactive in the dark, heat sensors that detect the proximity of the human hand, motion sensors that detect a telltale "tap-and-go" trajectory, etc. Ultimately, credit-card functionality will see incorporation into higher-powered consumer devices, such as NFC-ready mobile phones, and will benefit from the security protections of these host devices, such as biometric sensors and increased computational capacity [11].

Better cryptography: Contactless smart cards capable of robust cryptography have long been available. These techniques have already been applied to payment cards in the EMV standards, detailed in Section 7. If personally identifiable data can only be decrypted by authorized readers, then the danger of many of the attacks discussed in the paper are obviated.

7 Discussion

Comparison with other types of fraud: In most cases a financially motivated attacker has easier avenues to exploit than RF based attacks in order to perpetrate financial fraud. For example the alarming rise in phishing attacks enables attackers without physical presence to defraud merchants and cardholders. It is hard to directly compare the security of traditional magstripe cards and RFID-enabled cards. RFID-enabled cards are only more secure than their traditional counterparts against *certain kinds* of attacks. For example some traditional card reading mechanisms, such as taking a physical carbon copy of the face of the card, leave a physical image of the card in the hands of a possibly adversarial merchant or clerk. In fact, the use of a magstripe generally means handing one's card to a clerk who may have nefarious intent. By contrast, an RFID transaction leaves behind no physical carbon copy; in fact the card never leaves the cardholder's hands. Certainly, the effort required to obtain an RF copy of the transaction is greater in this case.

Additionally some RFID-enabled cards include a unique code for each transaction replacing the static data in a magstripe. This mechanism protects against some kinds of attacks, but creates opportunities for new types of attackers which cannot be easily addressed by traditional fraud control (such as cardholder tracking attacks).

The most important difference between RFID-enabled cards and traditional cards is perhaps the difference in cardholder control. Whereas a traditional magstripe reveals one's name and card number only when the artifact is physically handed to a merchant, an RFID enabled card is in some sense "always on." The card can be scanned and privacy can be compromised remotely and without the knowledge or consent of the cardholder.

The nominal read range of these cards, which is frequently cited as a source of security, is indeed short. However, that achievable read range is quite different from nominal read range. The exact range available for ISO 14443-B transponders seems to be hotly debated in press accounts [43]. Experiments conducted by Royal Dutch Shell of Canada [43], for example, indicate a read range of 26 inches, but unfortunately we have no details of the experimental setup used to obtain this result. Academic colleagues have demonstrated read ranges of 15cm against devices for which some standard readers achieve only 2cm [21, 22]. We have not explored this area in detail, but these types of attacks only improve with time and the development of more-specialized equipment.

Comparison with other electronic cards: The relationship between the cards we examined and the EMV series [14] of standards is unclear. Certainly in Europe, EMV techniques like the UK's "Chip and PIN" are seeing wide deployment and analysis [1, 3, 45]. But based on our observations, the protocols used by the U.S. contactless cards do not appear in the EMV standards, which have a sharp focus on public-key techniques.

Though extensive use is made of public-key cryptography, the EMV standards allow for cards that merely store digitally-signed data in addition to those that calculate fresh signatures. These latter cards use a technique called Dynamic Data Authentication (DDA) where the card digitally signs a random challenge issued by the reader. The use of DDA is motivated primarily by the need to support offline readers. But given the availability of EMV hardware with its support for public-key cryptography, it's not clear why the associations chose not to implement this existing standard and gain the higher security levels. Instead, they chose to develop a new system that primarily relies on symmetric-key cryptography and online verification.

We can surmise that this choice was motivated by the prevalence of online readers in the U.S., a focus on contactless operation and a desire to reduce costs. A card that doesn't need to implement a public-key accelerator will require fewer logic gates and cost less as well as offering longer range and shorter transaction times. But recent media reports suggest that contactless EMV transactions can be completed in "a fraction of a second [18]." The article doesn't specify if these were static or dynamic transactions, but perhaps we'll see an eventual harmonization of these payment cards and the EMV standards. As of this writing, the EMVCo website does not have such a specification publicly available.

Policy and regulation: Several state legislatures have recently considered bills on RFID. For instance, Gov. Schwarzenegger recently vetoed California's SB 768, which would have required interim protections for RFID cards, especially cards carrying personally identifiable information, and a process for figuring out long-term protections [16, 39]. The information made available by the cards, including name and card number are called personally identifiable information (PII) in the parlance of that bill [39]. If signed into law, ID cards issued by the state government carrying PII would have been required to implement mutual authentication and encryption to release the data. It's true that these cards are not state ID cards, but as time goes on we can expect more RFID-related legislation like SB 768 to be introduced.

Beyond regulation, it is an important open problem how best to incentivize all custodians of personal data to take adequate precautions. The core of the financial industry is risk management. However, we have yet to find a satisfying definition of privacy for the equation of risk management. How do we quantify user privacy when different users place different values on privacy? In hard figures, how does this value affect the business proposition of personal-data custodians?

New Technologies: Many new technologies and form factors are on the horizon. Smarter cards can offer greater security, including the possibility for mutual authentication: a card that releases personal information only to authorized readers. A promising platform for these features is the cellular telephone. A recent article in EETimes [11] dissects an NFC-enabled phone faceplate to show its parts. This emerging standard allows for a device to play the role of a tag, reader, or both. To that end, the faceplate includes an ISO 14443-A passive tag and what amounts to minimal electronics for a reader, including a 13.56 MHz transceiver.

One could imagine a faceplate that supports ISO 14443-B which could play the part of an RFID payment card. The faceplate offers greater power and computation and so therefore could perform more-robust cryptographic operations including EMV transactions. A more

tightly-integrated faceplate could in principle receive a Certificate Revocation List using its cellular data connection – and therefore know which readers are legitimate payment terminals and which have been revoked. To only a still-legitimate reader should a "card" reveal any personal information. Several technological hurdles stand in the way of this model of mobile payments, but in time, these too will be surmounted.

8 Conclusion

Despite the millions of RFID-enabled payment cards already in circulation, and the large investment required for their manufacture, personalization, and distribution, all the cards we examined are susceptible to privacy invasion and relay attacks. Some cards may be skimmed once and replayed at will, while others pose a modest additional synchronization burden to the attacker. After reverse engineering the secret protocols between RFID-enabled credit cards and readers, we were able to build a device to mount several advanced replay attacks in laboratory conditions. While absolute security and privacy in a contactless-card form factor is difficult to achieve, we hope that next-generation RFID-enabled payment systems will protect against the vulnerabilities that our study identifies.

Acknowledgments

We thank Russell Silva for his assistance in implementing Linux drivers for RFID devices as part of his undergraduate research project. We thank Robert Jackson and Prashant Shenoy for sharing laboratory equipment. We further thank Simson Garfinkel, Yoshi Kohno, David Molnar, and Adam Stubblefield for early reviews of this manuscript. This research was supported in part by grants from the National Science Foundation CNS-052072 and CNS-0627529.

References

1. Adida, B., Bond, M., Clulow, J., Lin, A., Murdoch, S., Anderson, R., Rivest, R.: Phish and chips: Traditional and new recipes for attacking EMV. Technical report, University of Cambridge Computer Laboratory (2006) http://www.cl.cam.ac.uk/~mkb23/research/Phish-and-Chips.pdf.
2. Anderson, R.: Why cryptosystems fail. In: Proceedings of the 1st ACM conference on Computer and Communications Security (CCS), New York, NY, USA, ACM Press (1993) 215–227
3. Anonymous: Chip and spin (2006) http://www.chipandspin.co.uk/problems.html Last Viewed October 11, 2006.
4. Associated Press: Wave the card for instant credit (2003) Wired News http://tinyurl.com/yc45ll Last Viewed October 16, 2006.
5. Averkamp, J.: ITS Michigan: Wireless technology and telecommunications (2006) http://www.itsmichigan.org/ppt/AM2005/Joe.ppt Last Viewed October 11, 2006.
6. Avoine, G.: Privacy issues in RFID banknote protection schemes. In: International Conference on Smart Card Research and Advanced Applications – CARDIS. (2004) 33–48
7. Avoine, G.: Adversary model for radio frequency identification. Technical Report LASEC-REPORT-2005-001, EPFL (2005)
8. Bono, S., Green, M., Stubblefield, A., Juels, A., Rubin, A., Szydlo, M.: Security analysis of a cryptographically-enabled RFID device. In: 14th USENIX Security Symposium. (2005)
9. Bray, H.: Credit cards with radio tags speed purchases but track customers, too (2006) Boston Globe, August 14, 2006 http://tinyurl.com/lmjt4.
10. CardTechnology: Paypass subway trial starts in New York (2006) http://tinyurl.com/uya3k.
11. Carey, D.: NFC turns phone into a wallet. EE Times (2006) http://tinyurl.com/yyxk28 Last Viewed October 8, 2006.

12. DIFRWear: Faraday-Caged Apparel. (2006) www.difrwear.com Last Viewed October 6, 2006.
13. Dougherty, G.: Real-time fraud detection (2000) MIT Applied Security Reading Group http://pdos.csail.mit.edu/asrg/02-28-2000.html http://pdos.csail.mit.edu/asrg/02-28-2000.doc.
14. EMVCo: EMV Integrated Circuit Card Specifications for Payment Systems. (2004) http://tinyurl.com/oo663 Last Viewed October 11, 2006.
15. EPIC: Mock point of entry test findings (2005) Page 48 of http://www.epic.org/privacy/us-visit/foia/mockpoe_res.pdf.
16. Ferguson, R.: Schwarzenegger quashes RFID bill (2006) eWeek DATE http://tinyurl.com/y29z6s.
17. Food, U.S., Administration, D.: Combatting counterfeit drugs: A report of the Food and Drug Administration (18 February 2004) Referenced 2006 at http://www.fda.gov/oc/initiatives/counterfeit/report02_04.html.
18. Gauthier, D.: Watch out, EMV is coming in contactless too (2005) Contactless News http://tinyurl.com/y7p3xs Last Viewed October 11, 2006.
19. Greenemeier, L.: Visa expands contactless card efforts (2006) Information Week http://tinyurl.com/ykzo4t.
20. Halamka, J., Juels, A., Stubblefield, A., Westhues, J.: The security implications of VeriChip cloning. Journal of the American Medical Informatics Association (2006) To appear.
21. Hancke, G.P.: A practical relay attack on ISO 14443 proximity cards. Technical report, University of Cambridge Computer Laboratory (2005) http://www.cl.cam.ac.uk/~gh275/relay.pdf Last Viewed October 12, 2006.
22. Hancke, G.P.: Practical attacks on proximity identification systems (short paper). In: Proceedings of IEEE Symposium on Security and Privacy. (2006) 328–333 http://www.cl.cam.ac.uk/ gh275/SPPractical.pdf.
23. Harper, J.: RFID wiggles its way into credit cards? (2005) http://lists.jammed.com/politech/2005/05/0038.html.
24. Heydt-Benjamin, T.S., Chae, H.J., Defend, B., Fu, K.: Privacy for public transportation. In: Proceedings of Privacy Enhancing Technologies workshop (PET 2006). (2006)
25. HowStuffWorks, Inc.: How blink works (2006) http://money.howstuffworks.com/blink1.htm Last Viewed October 8, 2006.
26. ICAO, I.C.A.O.: Document 9303, machine readable travel documents (MRTD), part I: Machine readable passports (2005)
27. Inc., E.: Class 1 generation 2 UHF air interface protocol standard version 1.0.9 (2006) Referenced 2006 at http://www.epcglobalinc.com/standards_technology/EPCglobalClass-1Generation-2UHFRFIDProtocolV109.pdf.
28. Intel: PXA255 Processor. (2006) http://tinyurl.com/y7fh2m Last Viewed October 12, 2006.
29. ISO: ISO/EIC 14443, proximity cards (PICCs). Technical report, ISO (2006) http://wg8.de/sd1.html.
30. ISO: ISO/EIC 7813:2006, identification cards – financial transaction cards. Technical report, ISO (2006)
31. Juels, A.: Strengthing EPC tags against cloning. In: ACM Workshop on Wireless Security (WiSe), ACM Press (2005) 67–76
32. Juels, A.: RFID security and privacy: A research survey. IEEE Journal on Selected Areas in Communication **24**(2) (2006)
33. Juels, A., Molnar, D., Wagner, D.: Security and privacy issues in e-passports. In: IEEE/CreateNet SecureComm. (2005) Referenced 2006 at http://www.cs.berkeley.edu/~dmolnar/papers/papers.html.
34. Juels, A., Rivest, R.L., Szydlo, M.: The blocker tag: selective blocking of RFID tags for consumer privacy. In: Proceedings of the 10th ACM conference on Computer and Communications Security (CCS '03). (2003) 103–111
35. Kfir, Z., Wool, A.: Picking virtual pockets using relay attacks on contactless smartcard systems. In: IEEE/CreateNet SecureComm, IEEE (2005) Referenced 2006 at http://eprint.iacr.org/2005/052.
36. Kirschenbaum, I., Wool, A.: How to build a low-cost, extended-range rfid skimmer. Cryptology ePrint Archive, Report 2006/054 (2006) http://eprint.iacr.org/.

37. Koper, S.: Contactless acceptance made easy for business payment systems (2006) BPS 2006 Summer Conference, Las Vegas, NV http://tinyurl.com/sjte6.
38. MIFARE DESfire: Nxp product description (2006) Referenced 2006 at http://www.nxp.com/products/identification/mifare/desfire/.
39. Molnar, D.: Personal communication (2006)
40. New York City Transit Authority: NYC MetroCard Fares. WWW (2006) http://tinyurl.com/y5egfd.
41. O'Connor, M.C.: Chase offers contactless cards in a blink (2005) RFID Journal http://tinyurl.com/yzy9u5.
42. O'Connor, M.C.: At McDonald's, ExpressPay fits the bill (2006) RFID Journal http://tinyurl.com/yc58sa.
43. Schuman, E.: How safe are the new contactless payment systems? (2005) eWeek June 20 http://tinyurl.com/y9a525.
44. Selker, E.: Manually-operated switch for enabling and disabling an RFID card. Technical report, MIT (2003) Patent #20030132301.
45. UK Chip and Pin: Chip and pin (2006) www.chipandpin.com Last Viewed October 11, 2006.
46. Westhues, J.: Hacking the prox card. In Garfinkel, S., Rosenberg, B., eds.: RFID: Applications, Security, and Privacy. Addison-Wesley (2005) 291–300
47. Yoshida, J.: Tests reveal e-passport security flaw (2004) EE Times August 30 http://tinyurl.com/surgr.
48. Zetter, K.: Hackers clone e-passports. Wired News (3 August 2006) Referenced 2006 at http://www.wired.com/news/technology/0,71521-0.html.