Vulnerabilities in first-generation RFID-enabled credit cards

Thomas S. Heydt-Benjamin, Daniel V. Bailey, Kevin Fu, Ari Juels, and Tom O'Hare

Introduction

An increasing number of credit cards now contain a tiny wireless computer chip and antenna based on RFID (radio frequency identification) and contactless smart card technology.[1] The RFID-enabled credit cards permit contactless payments that are fast, easy, and often more reliable than magnetic stripe card transactions, and only physical proximity (rather than contact) is required between this type of credit card and the reader. An estimated 20 million RFID-enabled credit cards and 150,000 vendor readers are already deployed in the U.S. (Bray, 2006). According to Visa USA, "This has been the fastest acceptance of new payment technology in the history of the industry" (Bray, 2006).

The conveniences of RFID-enabled credit cards also lead to new risks for security and privacy. Traditional (magnetic stripe) 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-enabled credit cards make these and other sensitive pieces of data available using a small radio transponder that is energized and interrogated by a reader.

Experimental results

Although RFID-enabled credit cards are widely reported to use sophisticated cryptography,[2] 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 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 the credit cards and readers. The experiments indicate that all the cards are susceptible to live relay attacks (in which an attacker relays verbatim a message from the sender to a valid receiver of the message), all the cards are susceptible to disclosure of personal information, and many of the cards are susceptible to various types of replay attacks (a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed). In addition, we successfully completed a proof-of-concept cross-contamination attack.

Given the size and diversity of our sample set, we believe that our results reflect the current state of deployed RFID-enabled credit cards; however, card issuers continue to innovate and will likely add new security features. Our findings are not necessarily exhaustive, and there may exist cards that use security mechanisms beyond what we have observed.

Background

In this section, we provide some background on the current state and standards of RFID technology and its deployment throughout the United States.

Thomas S. Heydt-Benjamin is a former graduate student at the University of Massachusetts Amherst. Daniel V. Bailey is a senior research scientist at RSA Laboratories in Bedford, Massachusetts. Kevin Fu is an assistant professor in the Department of Computer Science at the University of Massachusetts Amherst. Ari Juels is a chief scientist and director at RSA Laboratories. Tom O'Hare is an employee of Innealta Inc. in Salem, Massachusetts. The authors thank Russell Silva for his assistance in implementing Linux drivers for RFID devices as part of his undergraduate research project at the University of Massachusetts Amherst. They thank Robert Jackson and Prashant Shenoy for sharing their laboratory equipment. They further thank the anonymous reviewers, Simson Garfinkel, Yoshi Kohno, David Molnar, and Adam Stubblefield for reviewing earlier manuscripts. This research was supported in part by grants from the National Science Foundation (award Nos. CNS-052072 and CNS-0627529).

Scale of current deployment

Several large chain stores 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 (Koper, 2006; and O'Connor, 2006). Reports estimate that 20 million to 55 million RFID-enabled credit cards are in circulation, which is 5 percent to 14 percent of all credit cards (Averkamp, 2005; Bray, 2006; and Koper, 2006). In addition to traditional payment contexts, RFID-enabled credit cards are becoming accepted in other contexts such as public transportation (Heydt-Benjamin, Chae, et al., 2006). The New York City subway (Metropolitan Transit Authority, 2006) recently started a trial of 30 stations accepting an estimated 100,000 RFID-enabled credit cards (SourceMedia Inc., 2006). A participant in this trial uses her credit card as a transit ticket as well as a credit card in place of the traditional magnetic-stripe-based dedicated subway tickets.

Integration of radio frequency technology into existing credit card infrastructure

In a typical deployment, an RFID-enabled credit card reader is attached to a traditional cash register. Each reader continually broadcasts a radio signal to which RFID-enabled credit cards can respond. The RFID-enabled 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-enabled credit card readers that we examined reformat the received RFID data into "Track 1 Data" and "Track 2 Data" before passing them along to point-of-sale (POS) terminals. In other words, data are 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 stripe.

Our work focuses on the first step in a long chain of system interactions: card presentation. When considering the potential impact of the vulnerabilities we have observed in RFID-enabled card presentation, one must take into account the expertise credit card issuers have gained in detecting fraudulent transactions by tracking patterns of behavior (Dougherty, 2000). While detecting fraud is an effective defense against many types of financial risk, it does not *prevent* invasion of privacy. Our study considers vulnerabilities to privacy that today's antifraud methods do not prevent.

Communications protocol used by RFID-enabled credit cards

All of the credit cards we tested use a communications protocol specified by the International Organization for Standardization (ISO) in a series of documents titled ISO 14443-1 through 14443-4.[3] Our experiments indicate that the cards use the B version of this protocol, with an additional proprietary communications layer carried over ISO layer 4.

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. We discuss some of these here.

RFID authentication and cloning

Many types of RFID tags merely emit static identifiers, making them easy to clone. These tags are sometimes used in inappropriate contexts such as building access control. Westhues (2005) has demonstrated a simple, inexpensive device that can skim many types of cards at a distance—even through walls—and then simulate them. (Skimming is the theft of credit card information used in an otherwise legitimate transaction.) If unclonability is a security assumption, then this is a security break.

More sophisticated tags do not emit static data, but use cryptography to emit different data during different transactions. For example, the Texas Instruments' digital signal transponder (DST) is present in the ExxonMobil Speedpass (a keychain RFID device), and is also part of a common theft deterrent system for automobiles. These systems have been shown to be vulnerable because of faulty cryptography (Bono et al., 2005). In contrast with the RFID-enabled credit cards we examined, the DST uses cryptography to increase the difficulty of cloning, but it does not carry personally identifying information, for example, the name of its owner.

Read ranges

Industry claims around the security of RFID devices often hinge on their short read ranges. Some cautionary notes are in order, however: RFID tags do not have a single, definitive read range (Juels, 2006). While the *nominal* read range of an RFID tag may be quite short, a nonstandard reader or large antenna can increase the range at which an attacker can skim an RFID tag. The credit cards we examined are ISO 14443-B cards with a nominal range of 4–5 centimeters. Skimming ranges of over 20 centimeters have been demonstrated for cards of this type (Hancke, 2006), and ranges of up to 50 centimeters are hypothesized in the literature (Kfir and Wool, 2005). 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 where e-passports, which rely on the same ISO standard as credit cards, were read at a distance of 30 feet (Yoshida, 2004)[4] and detected at a distance of 20 meters (EPIC, 2005).

Our study makes no claims about the read ranges of RFID-enabled credit cards beyond the observation that characterization of these ranges is not straightforward and constitutes an important open research question.

Methodology and experiments

The following discussion highlights our methodology for testing the security of RFID-enabled credit cards against eavesdropping, skimming, and replay. A more detailed version is available in our technical report (see Heydt-Benjamin, Bailey, et al., 2006).

Eavesdropping experiments

In our eavesdropping experiments, we observed transactions between readers and cards with an oscilloscope attached to an antenna. Examination of data thus obtained demonstrated the efficacy of this simple attack, since in all transactions the cardholder's full name and card expiration date were present in "cleartext" (that is, this information was in a form that was immediately comprehensible to a human being without additional processing, implying a lack of cryptographic protection). A majority of cards examined transmitted the credit card number in cleartext, while a minority broadcast a separate (but static) credit card number apparently reserved for wireless transactions. We provide further details in the analysis and results section.

Skimming experiments

In our most simple skimming experiment, we took a commercial RFID-enabled credit card reader and presented it with each of our experimental cards, obtaining in each case ISO 7813 (magnetic stripe style) data. Since these are the exact data normally transmitted by a POS terminal to a charge-processing network, this most naive of skimming attacks is sufficient for perpetration of certain kinds of financial fraud.

We programmed an RFID reader not intended for credit card use to emulate an RFID-enabled credit card reader. Eavesdropping on transactions between our credit card reader emulator and real RFID-enabled credit cards demonstrated that all of the RFID credit cards we tested responded to our emulator exactly as they respond to a commercial RFID-enabled credit card reader. This strongly suggests that cards do not use any secure mechanism to authenticate an authorized RFID reader before releasing sensitive information.

Replay experiments

Our credit card emulator is a microprocessor controlled device with a simple radio, permitting broadcast of arbitrary bytes over the ISO 14443-B transport layer.

We programmed our credit card emulator to expect the RFID-enabled credit card reader commands that we captured during eavesdropping experiments and then to transmit replies captured from real RFID-enabled credit cards during a skimming attack performed with the reader emulator. In our experiments, commercial readers were unable to distinguish between our emulated card and the real card upon which it was based.

Since the output from the card emulator is identical to that of the real card from which it was skimmed, a simple replay attack using this device would succeed. As noted previously, many pieces of data go into an overall transaction approval decision, including sophisticated risk-based fraud detection mechanisms on the back end. For this reason, valuable future research would include field tests in which a credit card emulator is used to perform a purchase in a retail location rather than in a laboratory.

Analysis and results

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

Observations of RFID-enabled credit card protocols

This section explores some of the RFID-enabled credit card protocols that are in current deployment. The analysis is based on the ISO 7813 (magnetic stripe format) data output by the serial port of RFID-enabled credit card readers when presented with different types of credit cards. Where pertinent, our analysis compares this serial output with 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 to prevent criminal misuse of our findings. The cardholder's name and the card number have been concealed. Additionally, we have obscured the number of digits in the card number in order to obscure which observations

TABLE 1

Vulnerabilities of three classes of cards

Card type	Payment association	Privacy invasion?	Relay attack?[a]	Cross-contamination?	Replay attack?
A	1	Yes	Yes	Limited[b]	Yes[c]
B	2	Yes	Yes	Limited	Limited
C	3	Yes	Yes	No	Limited

[a] Because the cards have no shielding or notion of time, all the cards are susceptible to relay.

[b] This attack is proven in the field, but is limited to certain merchants.

[c] This card admits unrestricted replay for the readers we tested, while the others induce a race condition.

Notes: This is a summary of susceptibility to various attacks for the three semantic types of cards (A, B, C) from three payment associations (1, 2, 3). A relay attack is one in which an attacker relays verbatim a message from the sender to a valid receiver of the message. A replay attack is a form of network attack in which a valid data transmission is maliciously or fraudulently repeated or delayed.

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 magnetic stripe of the same credit card (see figure 1). 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.

Card B protocol

The sample card B output in figure 2 demonstrates the presence of a counter, determined to be as such because of monotonic incrementation with successive transactions. Additionally we observe three digits that 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 that 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 card verification code (CVC).

Card C protocol

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

- Its unique transaction codes are eight digits instead of three;
- Its transaction counter, now located in the cardholder's name field, displays only three digits instead of four; and
- Rather than sending the embossed card number over the air, it uses a fixed pseudonym.

See figure 3 for the sample card C output.

Analysis of RFID-enabled credit card protocols

In the following sections, we analyze the susceptibility of the card types to replay, relay, cross-contamination, and privacy/tracking attacks. Our analysis considers only the protection mechanisms of the cards and readers; we do not analyze the security of the charge-processing network (for example, the fraud detection algorithms).

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. The following describe the different types of replay attacks.

- 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.
- 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 and replays that transaction to the network before the legitimate user has a chance to use her card, then the charge-processing network should accept the adversary's transactions and actually decline the legitimate ones. Although the attacker is faced with a counter synchronization problem, such challenges are far easier to defeat than the

FIGURE 1

Card A

Bxxxxxx6531xxxxxx^DOE/JANE^0906101000000000000000000000000000858000000
xxxxxx6531xxxxxx=09061010000085800000

Notes: This is the serial output from a commercial reader after a radio frequency transaction with a card of type A. See the text and table 1 for further details.

FIGURE 2

Card B

Bxxxxxx1079xxxxxx^DOE/JANE^0901101100000000000100000000000
xxxxxx1079xxxxxx=090110110000***016***00221
Bxxxxxx1079xxxxxx^DOE/JANE^0901101100000000000100000000000
xxxxxx1079xxxxxx=090110110000***074***00231

Notes: This is the sample of the reader serial output after a radio frequency transaction with a card of type B. In this sample, there are a three-digit code (in bold and italics) and a four-digit counter (underlined). See the text and table 1 for further details.

FIGURE 3

Card C

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

Notes: This is the sample output from a card of type C. Transaction codes are in bold and italics, while the transaction counter is underlined. See the text and table 1 for further details.

cryptographic problems (we prefer to base our security on cryptography whenever possible).

- Counter rollover: If a transaction counter is the only changing input to a code, then the number of possible codes is limited by the maximum possible transaction counter value. There are then two cases. In one case, 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 has 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, a denial-of-service attack 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 with a hypothetical card that combines a challenge-response protocol with a transaction counter (a case not examined here), the relay attack may still succeed (Hancke, 2005). In an example of a relay attack, the adversary consists of a *mole* and a *proxy* that perform a purchase at an innocent user’s expense. The mole possesses a clandestine *credit card reader emulator* with a (non-RFID) radio link to the proxy's clandestine *credit card emulator*. The mole sits down or stands next to the user, and the mole's device rapidly discovers the user's credit card. The proxy receiving this relayed signal approaches the POS terminal and initiates a purchase. The proxy presents his credit card emulator to the POS terminal. The emulator receives commands from the POS terminal and relays them to the mole's device, which transmits the commands to the user's credit card. The responses from the user's card are likewise relayed through the mole's device and are broadcast from the proxy's emulator to the POS terminal. The purchase should succeed, and the cost will be charged to the user. 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's name transmitted through the envelope (for postal mail, the attacker already knows the cardholder's 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 merchants that do not require a CVC.

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-enabled credit card is easily demonstrated in the lab, and should be feasible in the field. This vulnerability is exacerbated by an adversary who could use the full identity disclosure of the RFID-enabled credit card to build up a database of associated pseudonyms based on other RFID tags with a longer read range that a user may commonly carry.

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. Those heavily using their cards might be targeted for specific advertising, for instance.

Countermeasures

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

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 slipcases to shield their RFID-enabled cards against unwanted scanning (DIFRwear LCC, 2006). Note that this countermeasure offers no protection when the card is in use, since a card must be removed from a shielded wallet before an RF purchase can be made. However, credit card companies ought to 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. Blocker tags (Juels, Rivest, and Szydlo, 2003) and the RFID Guardian (Rieback et al., 2006) are two examples of devices that can selectively disrupt RFID communications to offer tag owners improved access control.

Signaling cardholder's intent

As an alternative approach to protections such as the Faraday cage, the credit cards themselves could be modified to activate only after indication of user intent. A simple push button would serve this purpose (Selker, 2003), 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. Ultimately, credit card functionality will see incorporation into higher-powered consumer devices, such as near-field-communication-ready (NFC-ready) mobile phones, and will benefit from the security protections of these host devices, such as biometric sensors and increased computational capacity (Carey, 2006).

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 (EuroPay, MasterCard, Visa) standards, detailed in the next section. If personally identifiable data can only be decrypted by authorized readers, then the danger of many of the privacy invasion attacks discussed here are obviated. Anecdotal accounts suggest payment associations are moving to improve the on-chip cryptographic features of these cards, including challenge-response protocols, to further frustrate replay attacks.

Discussion

As time goes on and technology costs decrease, we can expect issuers to provide more effective cryptographic protocols. Well-established methods to thwart these attacks already exist, and issuers may in fact already be implementing these defenses. But even today, in most cases an attacker has easier avenues to exploit than RF-based attacks to perpetrate financial fraud. For instance, simple cloning of cards is often not sufficient to commit fraud. There are many back-end fraud detection measures in place to help thwart fraudulent use of card information. Nevertheless, privacy vulnerabilities should be addressed wherever they are found; privacy invasion may lead to financial fraud, but preventing financial fraud is not the only reason to protect privacy.

Comparison with other types of fraud

It is hard to directly compare the security of traditional magnetic stripe 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 magnetic stripe generally means handing one's card to a clerk who may have nefarious intent. By contrast, an RF 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 magnetic stripe. This mechanism protects against some kinds of attacks, but creates opportunities for new types of attacks that cannot be easily addressed by traditional fraud control (such as cardholder tracking attacks).

Perhaps the most important difference between RFID-enabled cards and traditional cards is the difference in the cardholder's control. Whereas a traditional magnetic stripe 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 without the knowledge or consent of the cardholder.

Comparison with other electronic cards

The relationship between the cards we examined and the EMV series of standards is unclear (EMVCo LLC, 2004). Certainly in Europe, EMV techniques such as the UK's "Chip and PIN" (personal identification number) are seeing wide deployment and analysis.[5] But based on our observations, the protocols used by the U.S. contactless cards do not appear in the EMV standards.

It is not clear to us why the U.S. payment associations have chosen to develop new protocols, with significant vulnerabilities, rather than use the more secure protocols that have already been deployed in Europe. We can surmise that this choice was motivated by the prevalence of online readers in the U.S. (some of the expense of supporting the EMV standards has to do with support for off-line operation) and a focus on contactless operation (whereas most of Europe's cards are contact-based).

Policy and regulation

Several state legislatures have recently considered bills on RFID. For instance, California Governor Arnold Schwarzenegger recently vetoed his state's bill 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 (Ferguson, 2006; and Molnar, 2006). The information made available by the cards, including the cardholder's name and card number are called personally identifiable information (PII) in the parlance of that bill (Molnar, 2006). 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. While credit cards are not state ID cards, as time goes on we can expect more RFID-related legislation like California's SB 768 to be introduced. Indeed, U.S. Senator Charles Schumer (D–NY) recently announced his intent to increase federal regulation of RFID-enabled credit cards (Chan, 2006).

Beyond regulation, it is an important open question as to how best to offer incentives for all custodians of personal data to take adequate precautions. Risk management is critical to the financial industry. However, as researchers and providers of risk management, we have yet to find a satisfying definition of privacy. How do we quantify user privacy when different users place a different value on privacy? In hard figures, how does this value affect the bottom line of businesses that are custodians of personal data?

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 capable of mounting several advanced replay attacks under laboratory conditions. While absolute security and privacy in a contactless card form factor may be impossible to achieve, we hope that the next generation of RFID-enabled payment systems will protect against the vulnerabilities that our study identifies.

NOTES

[1] This article was originally published as Heydt-Benjamin, Bailey, et al. (2008). The full version of this paper appears as a University of Massachusetts Amherst technical report (Heydt-Benjamin, Bailey, et al., 2006). See www.rfid-cusp.org for the latest version.

[2] See Associated Press (2003), Greenemeier (2006), Harper (2005), HowStuffWorks Inc. (2006), O'Connor (2005), and Schuman (2005).

[3] See International Organization for Standardization and International Electrotechnical Commission (2006).

[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.

[5] See Adida et al. (2006); Anderson, Bond, and Murdoch (2006); and UK Chip and PIN Program (2006).

REFERENCES

Adida, B., M. Bond, J. Clulow, A. Lin, S. Murdoch, R. Anderson, and R. Rivest, 2006, "Phish and chips (traditional and new recipes for attacking EMV)," University of Cambridge, Computer Laboratory, technical report, available at www.cl.cam.ac.uk/~mkb23/research/Phish-and-Chips.pdf.

Anderson, R., M. Bond, and S. Murdoch, 2006, *Chip and SPIN!*, available at www.chipandspin.co.uk/problems.html.

Associated Press, 2003, "Wave the card for instant credit," *Wired.com*, December 14, available at http://tinyurl.com/yc45ll.

Averkamp, J., 2005, "ITS Michigan: Wireless technology and telecommunications," presentation to Intelligent Transportation Society of Michigan, May 24, available at www.itsmichigan.org/ppt/AM2005/Joe.ppt.

Bono, S., M. Green, A. Stubblefield, A, Juels, A. Rubin, and M. Szydlo, 2005, "Security analysis of a cryptographically enabled RFID device," paper at 14th USENIX Security Symposium, Baltimore, MD, July 31–August 5.

Bray, H., 2006, "Credit cards with radio tags speed purchases but track customers, too," *Boston Globe*, August 14, available at http://tinyurl.com/lmjt4.

Carey, D., 2006, "NFC turns phone into a wallet," *EE Times*, September 18.

Chan, S., 2006, "Manhattan: Warning about credit risks," *New York Times*, December 4, available at www.nytimes.com/2006/12/04/nyregion/04mbrfs-credit.html.

DIFRwear LLC, 2006, "DIFRwear: Faraday-caged apparel," available at www.difrwear.com.

Dougherty, G., 2000, "Real-time fraud detection," Massachusetts Institute of Technology (MIT), Lab for Computer Science (LCS), Applied Security Reading Group, report, February 28, available at http://pdos.csail.mit.edu/asrg/02-28-2000.html and http://pdos.csail.mit.edu/asrg/02-28-2000.doc.

EMVCo LLC, 2004, *EMV Integrated Circuit Card Specifications for Payment Systems*, Version 4.1, May, available at http://tinyurl.com/oo663.

EPIC (Electronic Privacy Information Center), 2005, "E-passport mock point of entry test, November 29 thru December 2, 2004: Operational impact on the inspection process," report, Washington, DC, August 24, p. 48, available at www.epic.org/privacy/us-visit/foia/mockpoe_res.pdf.

Ferguson, R. B., 2006, "Schwarzenegger quashes RFID bill," *eWeek.com*, October 4, available at http://tinyurl.com/y29z6s.

Greenemeier, L., 2006, "Visa expands contactless card efforts," *InformationWeek*, March 27, available at http://tinyurl.com/ykzo4t.

Hancke, G. P., 2006, "Practical attacks on proximity identification systems (short paper)," in *Proceedings of the 2006 IEEE Symposium on Security and Privacy*, Los Alamitos, CA: IEEE Computer Society, pp. 328–333.

__________, 2005, "A practical relay attack on ISO 14443 proximity cards," University of Cambridge, Computer Laboratory, technical report, February.

Harper, J., 2005, "RFID wiggles its way into credit cards?," Politech, email to Declan McCullagh on mailing list, May 20, available at http://lists.jammed.com/politech/2005/05/0038.html.

Heydt-Benjamin, T. S., D. V. Bailey, K. Fu, A. Juels, and T. O'Hare, 2008, "Vulnerabilities in first-generation RFID-enabled credit cards," in *Financial Cryptography and Data Security: 11th International Conference, FC 2007, and 1st International Workshop on Usable Security, USEC 2007, Scarborough, Trinidad and Tobago, February 12–16, 2007, Revised Selected Papers*, Sven Dietrich and Rachna Dhamija (eds.), Berlin; Heidelberg, Germany; and New York: Springer, pp. 2–14.

__________, 2006, "Vulnerabilities in first-generation RFID-enabled credit cards," University of Massachusetts Amherst, technical report, October 22, No. CS TR-2006-055.

Heydt-Benjamin, T. S., H. J. Chae, B. Defend, and K. Fu, 2006, "Privacy for public transportation," in *Privacy Enhancing Technologies: 6th International Workshop, PET 2006, Cambridge, UK, June 28–30, 2006, Revised Selected Papers*, G. Danezis and P. Golle (eds.), Berlin; Heidelberg, Germany; and New York: Springer, pp. 1–19.

HowStuffWorks Inc., 2006, "How blink technology works," *HowStuffWorks*, available at http://money.howstuffworks.com/blink1.htm.

International Organization for Standardization and International Electrotechnical Commission, 2006, "ISO/IEC 14443, proximity cards (PICCs)," technical report, available at http://wg8.de/sd1.html.

Juels, A., 2006, "RFID security and privacy: A research survey," *IEEE Journal on Selected Areas in Communication*, Vol. 24, No. 2, February, pp. 381–394.

Juels, A., R. L. Rivest, and M. Szydlo, 2003, "The blocker tag: Selective blocking of RFID tags for consumer privacy," in *Proceedings of the 10th ACM Conference on Computer and Communications Security*, S. Jajodia, V. Atluri, and T. Jaeger (chairs), New York: Association for Computer Machinery, pp. 103–111.

Kfir, Z., and A. Wool, 2005, "Picking virtual pockets using relay attacks on contactless smartcard systems," *Proceedings of IEEE/Create-Net SecureComm 2005, 5–9 September 2005, Athens, Greece*, Los Alamitos, CA: IEEE Computer Society.

Koper, S., 2006, "Contactless acceptance made easy for business payment systems," presentation at BPS 2006 Summer Conference, Las Vegas, NV, available at http://tinyurl.com/sjte6.

Metropolitan Transit Authority, 2006, "Fares and MetroCard," New York City, available at http://tinyurl.com/y5egfd.

Molnar, D., 2006, personal communication.

O'Connor, M. C., 2006, "At McDonald's, ExpressPay fits the bill," *RFID Journal*, January 23, available at http://tinyurl.com/yc58sa.

__________, 2005, "Chase offers contactless cards in a blink," *RFID Journal*, May 24, available at http://tinyurl.com/yzy9u5.

Rieback, M., G. Gaydadjiev, B. Crispo, R. Hofman, and A. Tanenbaum, 2006, "A platform for RFID security and privacy administration," in *Proceedings of the 20th Conference on Large Installation System Administration*, New York: Association for Computer Machinery, pp. 89–102.

Schuman, E., 2005, "How safe are the new contactless payment systems?," *CIO Insight*, June 20, available at http://tinyurl.com/y9a525.

Selker, E., 2003, "Manually operated switch for enabling and disabling an RFID card," Massachusetts Institute of Technology, technical report, and United States Patent, No. 20030132301.

SourceMedia Inc., 2006, "PayPass subway trial starts in New York," *Card Technology*, July 12, available at http://tinyurl.com/uya3k.

UK Chip and PIN Program, 2006, *Chip and PIN* website, available at www.chipandpin.co.uk.

Westhues, J., 2005, "Hacking the prox card," in *RFID: Applications, Security, and Privacy*, S. Garfinkel and B. Rosenberg (eds.), Reading, MA: Addison-Wesley Professional, pp. 291–300.

Yoshida, J., 2004, "Tests reveal e-passport security flaw," *EE Times*, August 30, available at http://tinyurl.com/surgr.