RFID Payment Card Vulnerabilities Technical Report

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

1: University of Massachusetts at Amherst {tshb, kevinfu}@cs.umass.edu
2: RSA Security {dbailey, ajuels}@rsa.com
3: Innealta, Inc tom@innealta.com

Abstract

Recently, payment card issuers in the United States have begun mass deployment of radio-frequency-enabled payment cards. We examine a few examples of this new class of payment card and observe that while the card issuers have implemented some new security features, all of them admit practical attacks to a greater or lesser degree. This report serves as the first of two installments describing the threats and vulnerabilities of RFID-based credit cards as demonstrated by our laboratory experiments.

1. About RFID Credit Cards

An increasing number of credit cards now contain a tiny wireless computer known as an RFID chip (Radio Frequency Identifier) or a contactless smart card chip. There are reportedly over 20 million RFID credit cards[1] already deployed in the U.S., and this number is increasing rapidly. According to Visa ``This has been the fastest acceptance of new payment technology in the history of the industry'[1].

RFID credit cards are growing in popularity because they permit contactless payment transactions which are fast, easy, can be more reliable than magstripe transactions, and require only physical proximity (rather than physical contact) between the credit card and the reader. These same features, however, are also the basis for our concern about security and privacy vulnerabilities. Traditional credit cards require that an entity have visual access or direct physical contact in order to obtain information from the card 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. In the remainder of this technical report we will examine what data are conveyed, what kind of equipment is required to receive such a transmission, and whether such transmissions can be initiated by adversarial (not authorized by credit card companies) readers.

2. Summary of Findings

We examined representative RFID enabled credit cards from the major payment associations. We engaged each of the cards in various transactions with several different kinds of RFID readers, including specialized point-of-sale equipment deployed by major retailers. We determined that cheap off-the-shelf hardware and software are sufficient for an adversary with only modest technical skills to obtain critically sensitive data from the RF interface of the cards. While it is possible that some existing RFID credit cards have mechanisms for protection of sensitive information, cards from most issuers reveal all of the following information totally unprotected by any cryptographic security mechanism:

- **Cardholder Name**
- **Complete credit card number**
- **Credit card expiration date**
- **Credit card type**
- **Information about software version and supported communications protocols**

Cards from one issuer revealed this same information with the exception that the credit card number used by the RF interface is a different number from that encoded onto the magnetic stripe.

Off-the-shelf hardware requires reasonably close proximity (on the order of 10cm) in order to read these data from an RFID credit card. This is sufficient to read a credit card through clothing or a wallet, but the reader must still be close to the targeted card. The maximum potential range available seems to be hotly debated in press accounts of the situation. Experiments conducted by Royal Dutch Shell of Canada and reported in [4] indicate a read range of 26 inches, while retailer 7-Eleven insists that the range is only 2 inches. This longer range is supported by the academic literature: detailed instructions on how to build and operate such a specialized reader are already available to the public on the World Wide Web [2]. Additionally the range at which it is possible to detect the presence of a tag or eavesdrop on a transaction may be much longer than the range required for an active skimming attack [3]. This fact is apparently behind the report from the National Institute of Standards and Technology that the protocol used with these kinds of RFID chips can be read from up to 30 feet away using specialized reading hardware [4].

3. Summary of Basic Attacks

In this section we give a very brief description of some of the attacks which which we experimented. Some technical details of these attacks are available at the end of this document, and considerably more details will be available in the next installment of our report.

3.1 Skimming Attack

Point-of-sale readers - like the $200 Vivotech Vivopay 3000 HP we used - energize and interrogate a card and report the transaction data over a serial port to a PC. Moreover, the data is formatted into Track 1 and Track 2 data like a traditional mag-stripe credit card. This data includes:

- **Cardholder Name**
- **Complete credit card number**
- **Credit card expiration date**
- **Credit card type**

No cryptography or passwords were required to obtain this data. For some of the cards we examined, this data is static - the same every time. This fact means an attacker merely has to interrogate a target card once with a rogue reader to thereafter simulate as many transactions as desired.

Other cards emit slightly different strings each time. The differences are confined to a transaction counter and an random-looking code. The width of the counter and code again vary by issuer as does an important fact: in some of the cards, we were able to "roll over" the counter. By performing an hour's worth of transactions, we recorded every possible transaction counter and code. After this point, the card continued to emit the same counter-and-code pairs in order.

By spending an hour with a transaction-counter card, an attacker can simulate as many transactions as desired. The attacker faces a counter-synchronization problem with the legitimate card, but this type of problem does not present a level of difficulty approaching that of a cryptographic protection.

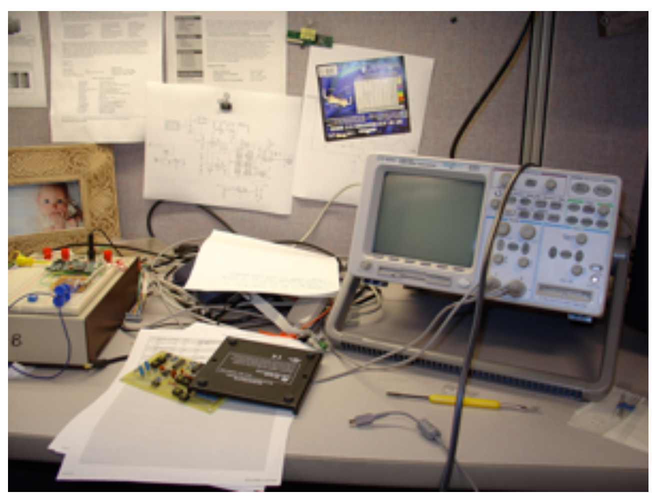
3.2 Eavesdropping Attack

In the eavesdropping attack an adversary captures a copy of the transmission between a legitimate credit card reader and an RFID credit card. We performed an eavesdropping attack in our laboratory by placing an antenna next to an off-the-shelf commercial RFID credit card reader. The antenna was connected to an oscilloscope which was used to capture the radio signal picked up by the antenna. We wrote some simple software to translate this captured radio signal into a human readable form.

Using the above mentioned set-up we found that an eavesdropper placed near a normal RFID credit card transaction can intercept the following pieces of data:

- **Cardholder Name**
- **Complete credit card number**
- **Credit card expiration date**
- **Credit card type**
- **Information about software version and supported communications protocols**

As previously mentioned, we successfully intercepted all of these data from all of the cards that we examined with the exception that the one of the cards broadcasts a different credit card number over the air than is recorded on the magnetic stripe.



We eavesdrop on communication between RFID credit cards and readers using an oscilloscope connected to a conventional computer to decode the signals.

The eavesdropping attack should be possible at longer range with much cheaper and more compact hardware than we used for our proof-of-concept demonstration. This is because our laboratory setup is designed for maximum flexibility of experimentation in that it can be used for any RF protocol over a very wide frequency range. It should be relatively easy to build a small clandestine reader based on more specialized circuitry given the instructions available at [2] since only one frequency and a very simple radio protocol need to be supported in order to read an RFID credit card. This simple protocol (known as BPSK) was chosen for RFID credit cards precisely because it is possible to implement in small, low-cost hardware.

3.3 Replay Attack

This prototype cloning device is shown with its antenna detached and a pencil for scale.

We built a prototype of a credit card cloner which uses easily available hardware to replay a transaction between an RFID credit card and an RFID credit card reader. We have determined that our cloned credit card broadcasts the same data as the real credit card on which it is based. Our experiments indicate that our two commercial credit card readers could not distinguish a cloned credit card from a real one. The transactions weren't submitted to the charge-processing networks, but we have every indication they would be approved.

4. Practical Significance

We believe that the typical RFID payment card holder did not previously understand that their payment card could be used to track their movements even while in their clothing, wallet, or purse. We further believe that the privacy implications of revealing name, credit card number, and other information to unauthorized readers needs to be the subject of discourse between credit card users, customer advocates, and credit card companies.

To take an illustrative example: We imagine that most consumers would choose not to wear a T-shirt printed with their full name, credit card number, and credit card expiration date. If a credit card makes these same pieces of information available at a distance to any entity, regardless of authorization, then every consumer should be aware of this threat so that they can make informed decisions about their personal data.

5. Videos

To appear.

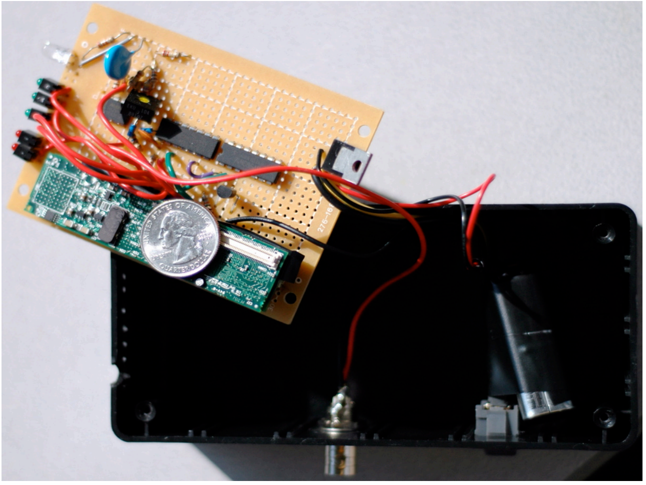
6. Brief Technical Details

6.1 Eavesdropping Attack

In order to determine what data are broadcast in cleartext (i.e. broadcast without the use of any cryptography) we used a standard commercial credit card reader, a standard commercial RFID antenna, and an oscilloscope. We performed transactions between the commercial credit card reader and each of the cards under study. We placed the RFID antenna underneath the credit card reader, and set the oscilloscope to capture all radio frequency data broadcast by the credit card reader. The captured data was then processed by analysis software that we wrote. The analysis software performed no decryption of any kind. The software simply followed the same process that a normal RFID reader would use to understand a transmission. All the information that we needed to write our software is supplied in the publicly available ISO 14443 documentation. Our software will be available for public scrutiny when the full version of our paper is submitted.

6.2 Replay Attack

Our credit card cloner is constructed from a single board linux computer, a small custom circuit constructed from cheap (less than $10) ubiquitous components, and a device driver of our own authorship. A diagram and parts list will be made available at the same time as the submission of the full version of our paper. A version of our device driver will also be made available, although certain details will be redacted in order to prevent illegal use by the unethical.



References - reminder: this section needs reformatting

1. Boston Globe, "Credit cards with radio tags speed purchases but track customers, too", August 14, 2006

2. Kirschenbaum, et. al. "How to Build a Low-Cost, Extended-Range RFID Skimmer", e-print archive 2006:054

3. Juels, et. al. "Security and Privacy Issues in E-passports", SECURECOMM'05 p74-88
4. Schuman, Evan, "How safe are the new contactless payment systems?," in *eWeek*, June 20, 2005. Observed 2006 at http://www.cioinsight.com/print_article2/0,2533,a=154404,00.asp.
5. Yoshida, Junko, "Tests reveal e-passport security flaw", EE Times 08/30/2004