HACKING NEXT-GEN ATMS: FROM CAPTURE TO CASH-OUT

Weston Hecker, Senior Security Consultant with Rapid7
@westonhecker

Abstract

To build better protection methods and safeguard ATM networks, I spent the past year analyzing and testing new methods that ATM manufacturers implemented to produce "next-generation" secure ATM systems. This presentation explains that a motivated attacker could bypass anti-skimming/anti-shimming methods introduced to the latest generation ATMs, and perform EMV/NFC long-range attacks that allow real-time card communication from over 400 miles away.

I will demonstrate how a $2,000 investment can perform unattended "cash-outs," also touching on past failures with EMV implementations and how credit card data of the future will most likely be sold with the new EMV data, with a short life span. I will introduce "La-Cara," an automated cash-out machine that works on current EMV and NFC ATMs. La-Cara is an entire fascia placed on the machine to hide the auto PIN keyboard and flash-able EMV card system that silently withdraws money from harvested card data. This demonstration of the system can cash-out around $20,000-$50,000 in 15 minutes. Our hope is that revealing these methods will drive mitigation of these types of attacks.

Introduction

Criminals of the credit card theft underworld will face a challenge as the world switches entirely to Europay, MasterCard and Visa (EMV), or chip and pin transactions. Magnetic card data will be limited to 40 USD in the coming year, which is pushing a large amount of fraud onto online Card Not Present (CNP) theft, such as online transactions.

This research idea came to me while I was exploring carder sites used by criminals. I was writing web-based software to track and monitor online databases of Bank/Issuer Identification Numbers, or BINs/IINs. BINS/IINs consist of only the first 6 digits of the card and indicate the issuer of the card. For example, 000000 is the Weston Bank of Manhattan.

While searching for this information, I noticed that BIN/IIN box lists were being discussed on several of the harder-to-visit forums. BIN/IIN box lists are Assumed POS (Point of Sale) limits of cards and ATM limits based on the issuer. This information was being harvested from cash-out crews and reported back to the people on top. This led me to think about what the bad guys' next step(s) will be. So I started researching EMV protocols and standards, looking at how they have changed over the years and been modified to compensate for fraud.

EMV is a very in-depth and progressive method of conducting credit card transactions. Originally conceived in the mid '80s and integrated in Europe several years ago, it is also used in several other countries, except the United States, which is expected to adopt the change in several phases, the first of which occurred in 2015. Several other liability shifts will happen over the next few years, and a reference to a list of relevant dates is provided at the end of this paper. These "milestones" are explained in more detail, but the gist is that stores and other entities will become increasingly liable for damages that occur from theft and fraud from a variety of sources.

With this paper and lecture, I hope to improve the overall knowledge of financial institutions and ATM manufacturers regarding the lengths that carders will go to in order to use stolen credit card data. My goal is to encourage proper maintenance and communication with fraud backend systems, in order to reduce the negative impact of attacks against these systems.

Active Research Phase

While there is no lack of published EMV protocol exploits and relay attacks online (and there are links to several at the end of this report), I had never seen a situation where carders had successfully used EMV attacks on ATM machines. Looking at other research, it is clear why: the volatility and time constraints associated with these transactions. There is a very small window of time available for the attack to actually occur.

The first step of this research required constructing a real-time delivery system, as most of the cards issued in the United States at the time of this paper do not use static cards. For detailed explanations of the different EMV chips—including SDA (Static Data Authentication), DDA (Dynamic Data Authentication), or CDA (Combined Data Authentication)—several online resources are listed at the end of this report. These methods have evolved because of their effectiveness at fighting fraud due to counterfeiting.

The second step of my research included reading the standards related to the EMV protocol. After gaining an understanding of how everything worked, I explored previous research by the University of Cambridge Security Group[1], among others, that demonstrated relay attacks on point of sale (POS) systems in the past. I looked at what was still working from the attacks and, with that information and an understanding of some of the changes to the standards that had occurred during my own research, I could understand the current attack surface and what would be needed to apply some of the same methods to ATM machines.

The third step was acquiring an ATM that would work for the purposes of my testing. I chose an ATM that was affordable but still in wide production. After the ATM was purchased, I converted and upgraded it with an "EMV-ready kit," which included hardware and software updates to the system. The ATM that is used in the demo is unmodified, aside from the hardware being switched from a (DIP) Magnetic Card Reader to a (DIP) EMV card reader.

For some of the other testing, I also fitted the device with a third-party Foreign Object Detection (FOD) system, which is a device for detecting skimmers installed on the ATM; it puts the device into service mode if something is detected on the machine. This ATM, as stated, is unmodified aside from the upgrade I performed. The only thing necessary to put this ATM into a full production environment would be DES keys to associate with the Gateway Provider, which is the first step in communication with banks and the accounts associated with the banks.

The fourth step in the research included looking at open source software used to read some of the smartcards and EMV cards that are on the market. After I felt like I had a grasp of the EMV transaction limitations, I bought some hardware to start relaying the transactions over short distances. The first device I purchased was one used for relaying a card and the information associated with the smart card to other rooms in the house.

This concept may seem simple, but some of what this device evolved into once it was switched to longer range and modulated for transfer over Ethernet becomes a bit more difficult to understand. I will be doing presentations on the hardware associated with this in additional research papers and talks in the future.

Along with some of the previous methods used to pass off EMV transactions, I focused on the "skimmer" portion. When performed on EMV cards, it is a process called "shimming[2]," as the device is set in-between the contacts of device A and relayed to contacts on device B on the cash-out side.

I built a simple "Pong" approach to test how the device handled data passed from one pin in one machine to another. The pong tool I build can test the effect of data when latency and other factors are introduced also view some of the limitations that come with devices, including distance errors and percentage rates associated with the nature of electromagnetic data. This should have provided enough information to move on to the next phase of the attack: the distribution of stolen card data.

1 https://www.cl.cam.ac.uk/research/security/banking/relay/

2 http://krebsonsecurity.com/2015/08/chip-card-atm-shimmer-found-in-mexico/

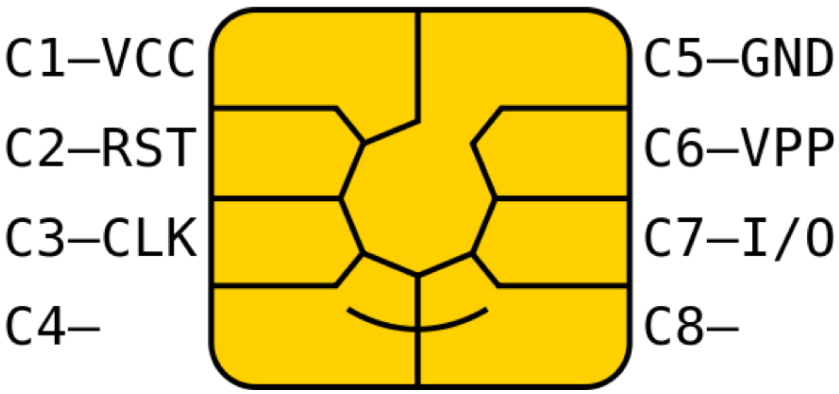

Figure 1: Image showing contacts where information is relayed

System That Allows Transactions to Be Delivered in Real-Time

For these transactions to be monetized by malicious parties, the way credit card fraud is performed needed a complete redesign. The current method involves skimmed batches of credit card data, which is used to create cloned credit cards. The magnetic strips originally found usage on modern day credit cards in the '60s and '70s. The high amount of fraud and ease of duplication is what led to the standard for EMV.

Figure 1 shows what is required to monetize transactions that have a one-minute life span. It includes what information is sent, along with the actual card and transaction data. This includes instructions for PIN entry into an Arduino-based motor system like on La-Cara, the automated method demonstrated on stage at Black Hat.

Today, the system for Live Transaction sales – made up of carder purchase pages and the delivery platform – do not work as they did for carder sites of the past. Previously, you simply purchased static data; however, the nature of EMV transactions means this no longer works as they have data that is not static – it evolves through each transaction and requires communication with the cashout ATM.

So as carders would buy specific bank and ATM limits they now buy transaction timeframes or blocks of time when their transactions, along with the previous field cart information, will be passed to their required cashout device.

Before this card data can be passed off in real time, secure communications need to be established to ensure that there are no lags or windows of time that are missed. It takes about seven seconds to construct the tunnel needed for the transaction to be passed through the secure fraud network.

Before the cashout ATM even reads the initial conversation with the remote shimmed card, the transaction is passed off to a protected network. The device is on a protected DMVPN (Dynamic Multipoint Virtual Private Network) network for several seconds before the transaction takes place.

There is encoded information provided in the payment blockchain; details of other transactions are sent through to initialize the tunnel. This is the point when the initial challenge conversation from the cash out ATM is passed to the shimmer for the hijacking of the transaction. It is the initial secure connection that allows secure real time communication to take place.

This leads to the second requirement when the carder is checking out, which is two passwords: one to establish a VPN tunnel to the device and another to sign the keys to the device to register it as the device of that transaction. So in addition to the VPN tunnel information generated off the passwords, there are also device keys generated to add the device to the fraud network. This is so devices on the fraud network can form trust to their assigned skimmer and not other devices on the network.

Figure 2 shows an example of the functionality that will most likely be added to the carder sites once the ability to sell shimmed EMV transactions is more wildly explored. There are already indicators of the carders heading down this path, as they seem to be researching the settings and flags for each of the financial institutions as they probe the devices. When thinking of the concept behind the page, I thought of what the current systems offer and what will be needed to deliver live data of this nature, as well as some of the shortcomings they would come across and how the third generation of the sale and the transmission of stolen data would progress in the never-ending cat-and-mouse game between the good guys and the bad guys.

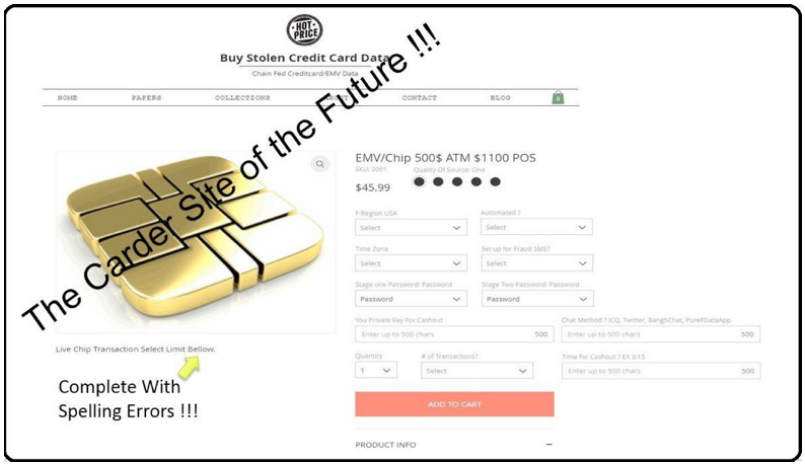

Figure 2: Example of carder site once EMV transactions become a method of cash-out.

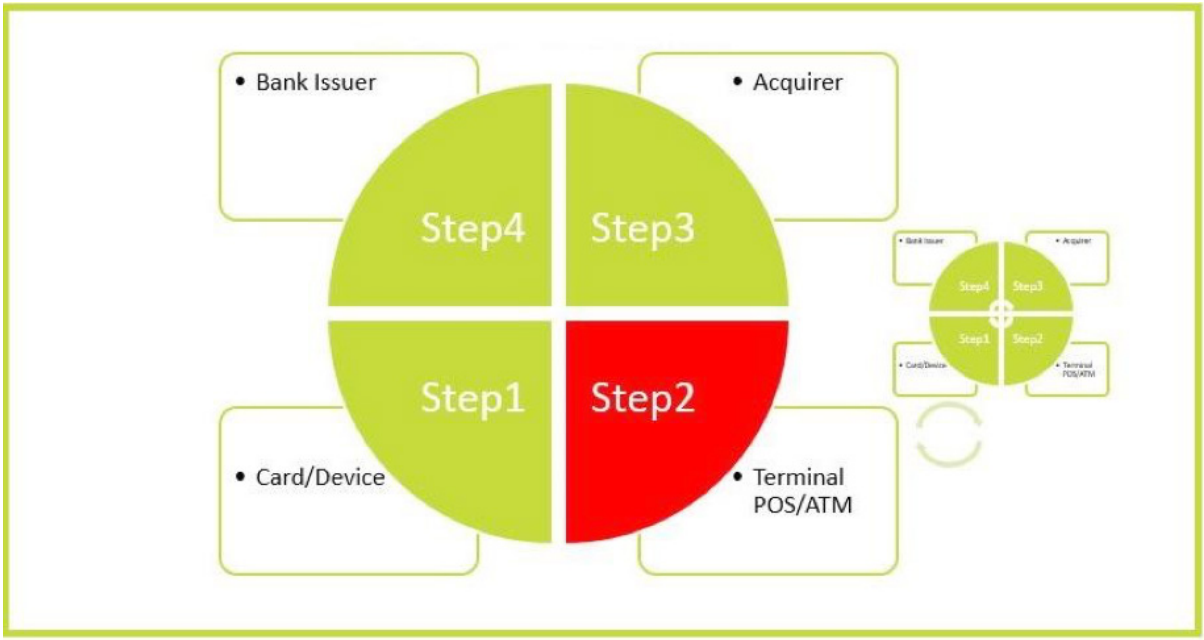

Figure 3: Communication in EMV transaction and transaction being passed off in stage 2.

Figure 3 shows a graphical representation of how the second phase of the transaction is passed off to another device. This includes the initial conversation between the two devices. Without the relay of this information, the transaction would be worthless. Since it was authorized on the skimmed device and not the cash-out device, the entire first conversation the two devices have would lead to different transaction information, which would be flagged and canceled.

As you can see in Figure 4, once a carder has purchased a transaction, they receive all of the transactions happening on the network. This is when the passwords and keys given at purchase come into play. The "cash-out network" uses the same method at the ATM network; it requires a key to speak to the shimmed device and to be allowed on the cash-out network.

The other passwords allow delimiting characters to be set for the cash-out device. These characters trigger information to be sent on when the unique portion of cards starts coming through the chain.

So, a carder receives all the transactions but does not have the keys and passwords to receive their data, and it is impossible to reverse the other transactions in the timeframe in which they're happening.

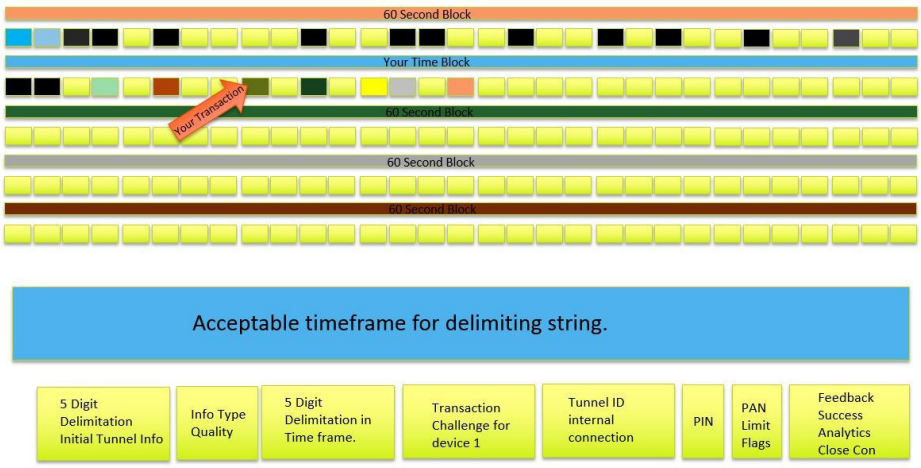

Figure 4: Stages and time used to distribute transactions. This is an example of delivery system at work.

Look at the Cash-Out End

Figure 5 shows the entire setup needed in order to relay the three most common methods of credit card transactions: classic magstripe, EMV, and near-field communications (NFC) (13.56Mhz).

The black card in the picture is a contact card that is used to pass the information to and from the contacts inside the cash-out ATM. These types of devices are similar to those that have been used in relay attacks in the past. This setup was made to encompass all the modern transactions according to the standards that will be in use until late 2017.

Ongoing Work

I will continue to work on some of the attack surface as the implementation becomes solidified. I will also continue work on the fraud detection training software that has come from this research.

Figure 5: Setup needed to relay the three most common transaction types: EMV, NFC, and magstripe.

Recommended Further Reading

http://www.emv-connection.com/emv-migration-driven-by-payment-brand-milestones/

http://krebsonsecurity.com/2015/04/revolution-crimeware-emv-replay-attacks/

https://www.emvco.com/specifications.aspx

https://www.cl.cam.ac.uk/research/security/banking/relay/

http://krebsonsecurity.com/2016/02/the-great-emv-fake-out-no-chip-for-you/comment-page-1/

http://sec.cs.ucl.ac.uk/users/smurdoch/papers/oakland14chipandskim.pdf

http://www.securityweek.com/fraudsters-stole-680000-mitm-attack-emv-cards