FROM CAPTURE TO CASHOUT

HACKING NEXT-GEN ATMS

Senior Security Consultant/Senior Pentester
TWITTER, LinkedIn @westonhecker
Rapid7 www.rapid7.com
A Little Bit About Myself

✅ Senior Security Engineer / Senior Pentester / Security Researcher with 12 years experience in programming and reverse engineering

✅ Speaker at Defcon 22, 23 and 24 Las Vegas, HOPE 11, TakedownCON 2016, B-sides Boston, Blackhat 2016, Enterprise Connect 2016, ISC2, SC Congress Toronto

✅ Other projects: Attacking 911 centers; malware and ransomware analysis; hacking cars, point of sale systems, hotel key systems, and property management systems.
EMV, Carder Systems, and Automating Cashout

- Attacks on the EMV (Europay, MasterCard, Visa) standard
- Relay attacks on physical cards
- A tour of a new method of distributing stolen credit card data when transactions have 1 minute shelf life
- Attacking next generation ATM security features
- Look at ATM communication backends to financial institutions
- Introducing La-Cara: an automated Ca$hout machine (ACM?)
- Demos representing over 400 hours of research on my own time
What is EMV?

- Developed in France in the 1980s
- Europay, MasterCard, and Visa
- It is a small chip on card
- Standard managed by EMVCo
- Replaces magstripe cards
- Liability shift 2015-2017 in USA
Greetings from he who makes mortals tremble? Stalin of the Russians...

Would you like to trade "The Wheel" for "Credit Card Fraud" and 15 BitCoins.
Your Grampa’s BINS the past

<table>
<thead>
<tr>
<th>Bin</th>
<th>Card</th>
<th>Debit/Credit</th>
<th>Mark</th>
<th>Expres</th>
<th>Track 1</th>
<th>Code</th>
<th>Country</th>
<th>Bank</th>
<th>Base</th>
<th>Price</th>
<th>Cart</th>
</tr>
</thead>
<tbody>
<tr>
<td>372733</td>
<td>AMEX</td>
<td>CREDIT</td>
<td>PLATINUM</td>
<td>09/16</td>
<td>101</td>
<td>United States, MT, MISSOULA</td>
<td>AMERICAN EXPRESS COMPANY</td>
<td>Lepidi (valid rate 35%)</td>
<td>13.55</td>
<td></td>
<td></td>
</tr>
<tr>
<td>453136</td>
<td>VISA</td>
<td>0</td>
<td></td>
<td>08/15</td>
<td>101</td>
<td>United States, MT, MISSOULA</td>
<td>U.S. BANK N.A.</td>
<td>Lepidi (valid rate 35%)</td>
<td>3.15</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td>Yes</td>
<td>101</td>
<td>United States, ND, BISMARCK, 58504</td>
<td>WELLS FARGO BANK N.A.</td>
<td>Beaver Cage 1 (valid rate 35%)</td>
<td>12.6$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Yes</td>
<td>101</td>
<td>United States, ND, BISMARCK, 58504</td>
<td>WELLS FARGO BANK N.A.</td>
<td>Beaver Cage 1 (valid rate 35%)</td>
<td>12.6$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td></td>
<td>Yes</td>
<td>101</td>
<td>United States, ND, BISMARCK, 58504</td>
<td>WELLS FARGO BANK N.A.</td>
<td>Beaver Cage 1 (valid rate 35%)</td>
<td>12.6$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td>Yes</td>
<td>101</td>
<td>United States, ND, BISMARCK, 58504</td>
<td>WELLS FARGO BANK N.A.</td>
<td>Beaver Cage 1 (valid rate 35%)</td>
<td>12.6$</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>10/16</td>
<td>101</td>
<td>United States, MT, MISSOULA</td>
<td>BANK OF HAWAII</td>
<td>Lepidi (valid rate 35%)</td>
<td>4.73</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td></td>
<td></td>
<td></td>
<td>07/16</td>
<td>101</td>
<td>United States, MT, MISSOULA</td>
<td>FIRST INTERSTATE BANK</td>
<td>Lepidi (valid rate 35%)</td>
<td>6.75</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Buy Stolen Credit Card Data
Chain Fed Creditcard/EMV Data

Buy EMV/Chip Card Data
BUY MORE

Buy RFID Data
BUY MORE

Buy Classic Track 1,2,3 Data W/Out PIN
BUY MORE

Buy Devices Skimmers/Shimmers Cashout Devices
BUY MORE

Buy Credit Card Data for all your scamming needs. Hotprice Carder Site has the best Credit Card Data around.
Acceptable timeframe for delimiting string.

- 5 Digit Delimitation Initial Tunnel Info
- Info Type Quality
- 5 Digit Delimitation in Time frame.
- Transaction Challenge for device 1
- Tunnel ID internal connection
- PIN
- PAN Limit Flags
- Feedback Success Analytics Close Con
5 Digit Delimitation
Initial Tunnel Info

Info Type Quality

5 Digit Delimitation in Time frame

Transaction Challenge for device 1

Tunnel ID internal connection

Feedback Success Analytics Close Con

Received over 30 Seconds
Acceptable time Frame for Delimiting String.

<table>
<thead>
<tr>
<th>5 Digit Delimitation on Initial Tunnel Info</th>
<th>Info Type Quality</th>
<th>5 Digit Delimitation in Time frame</th>
<th>Transaction Challenge for device 1</th>
<th>Tunnel ID internal connection</th>
<th>PIN</th>
<th>PAN Limit Flags</th>
<th>Feedback Success Analytics Close Con</th>
</tr>
</thead>
</table>

Your Time Block

60 Second Block

Your Transaction

60 Second Block

60 Second Block

60 Second Block

Connection Info

60 Second Block
What type of credit card data is possible to be sold in real time by the carders?

--STATIC MAG DATA TRACK 1 2 3
--EMV (DDA DYNAMIC AUTHENTICATION)
--EMV (CDA COMBINED DATA AUTHENTICATION)
--SOME 13.56 RFID NFC (NON TOKEN BASED)

REJECTS CARDS WITH FLAGS NOT SET FOR ATM
ASIDE FROM CARD PASS OFF BAD GUYS WILL ALSO GET PIN NUMBER AND ASSUMED ATM LIMIT
How is it used in this attack?
Here is the most likely method that sites get data that is sold.

Small Carder Site

- Leased Gear
- Mules/Store Employees
- Independents/Small Breach
Stage one Initial Transaction Request

Hold for Round Two

Stage One / Hold 2/3/4
PIN: 1122
$38.92
POS ✓

PIN PAN Flags Limit

Transaction Data
Tunnel ID Validation

PIN PAN Flags Limit

PIN: 1122
$1500.00
ATM/POS
This is not cloning the card its relaying it X distance. There are about 1 min windows.

4 stages of EMV transaction are being captured and released into a tunnel to speak to another ATM or POS.

The cash out device regurgitates the exact “send and receive” from a shimmed device to the cash out device.

The shimmed device is told to hold while the tunneled transaction happens.

PIN information is also passed in real time to cash out device.

POS limit shimmed will not count against the ATM daily limit.
Shimmer VS Skimmer? Shimmers Found in Wild!
Cashout Device Standalone?
Introducing La-Cara

Why would criminals automate cashout?

✓ People are un-trustable
✓ Cashout crews brag about it on social media
✓ Busted humans rat out their accomplices
✓ Machines don’t usually have twitter accounts.
✓ Defcon Theme this year is Rise of the machines
ATMs don’t have a twitter account ....
Making of La-Cara

That guy smiling like a child in the reflection is me
Making of La-Cara
La-Cara
Swiss army knife
Building your Own Banking Backend

Off branch ATM DES keys account signing
Each one of the accounts are signed with banking Keys
Each Card Transaction in Demo is Signed
Skimmer Generation is signed with
Field 55 training
EMV transaction

- Bank Issuer
- Acquirer
- Card/Device
- Terminal POS/ATM

Step 1
Step 2
Step 3
Step 4
EMV transaction

- Bank Issuer
- Acquirer
- Card/Device
- Terminal POS/ATM

Step 1
Step 2
Step 3
Step 4
We have the chip, how about the PIN?

Methods of Past Present:

Camera Method

PIN overlay

Unencrypted pin trace
New Automating PIN Capture

OPEN CV

PIN radar
Probing Networks and Card Settings

Estimating POS/ATM limits from a BIN number
What is a BIN?
POS vs ATM limit
Branch ATM vs off-network
Japanese ATMs
Chinese ATMs
Old Favorites Become New Favorites?

Shimming POS Systems

Habits of putting EMV card in early

Takes from POS limit on the in store transaction

ATM cash out is uninterrupted

Shimming bank front desk, Gas Pumps/Electric charge stations 2017+
Special Thanks to

✓ MY WIFE AND KIDS, JESUS,
✓ BARNABY JACK, SAMY KAMKAR,
✓ RUSSEL RYAN, ZACK ANDERSON AND ALESSANDRO CHIESA
✓ PHATPAT, ECONIC, TOTAL DOWNER
✓ RANDOM PEOPLE IN CHATROOMS FORUMS
$50,000 Prop money
So $500-$900 Per Transaction
So at most 60 transactions
Transactional time for online is 18-22 seconds
Card Challenge Auth
Amount Selection Based on PAN/BIN
PIN entered / Downgraded when available
Money comes out !!!!
No receipt selected
QUESTIONS?

Weston Hecker
Senior Security Consultant/Senior Pentester
TWITTER @westonhecker
Rapid7