RAPID7

HACKING NEXT-GEN ATMS

FROM CAPTURE TO CASHOUT



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.


SAFETY
FIRST



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



	Bin	Card	Debit/Credit	Mark	Expires	Track 1	Code	Country	Bank	Base	Price	Cart
☐	372733	AMEX	CREDIT	PLATINUM	06/16		101	United States, MT, MISSOULA , 0	AMERICAN EXPRESS COMPANY	Lepid (valid rate %35)	13.5$	+
☐	483316	VISA	0		09/15		101	United States, MT, MISSOULA , 0	U.S. BANK N.A.	Lepid (valid rate %35)	3.31$	+
☐	3	09/16	Yes		101		United States, ND, BISMARCK, 58504		WELLS FARGO BANK N.A.	Beaver Cage 1 (valid rate 35%)	12.6$	+
☐	4											+
☐	4	05/16	Yes		101		United States, ND, BISMARCK, 58504		WELLS FARGO BANK N.A.	Beaver Cage 1 (valid rate 35%)	12.6$	+
☐	5	10/15	Yes		101		United States, ND, BISMARCK, 58504		WELLS FARGO BANK N.A.	Beaver Cage 1 (valid rate 35%)	12.6$	+
☐	4											+
☐	4	07/16	Yes		101		United States, ND, BISMARCK, 58504		WELLS FARGO BANK N.A.	Beaver Cage 1 (valid rate 35%)	12.6$	+
☐	481582	VISA	0		10/16		101	United States, MT, MISSOULA , 0	BANK OF HAWAII	Lepid (valid rate %35)	4.73$	+
☐	425409	VISA	DEBIT	CLASSIC	03/16		101	United States, MT, MISSOULA , 0	FIRST INTERSTATE BANK	Lepid (valid rate %35)	6.75$	+

Buy Stolen Credit Card Data

Chain Fed Creditcard/EMV Data









Show More

Buy EMV/Chip Card Data

+ VIEW MORE

Buy RFID Data

+ VIEW MORE

Buy Classic Track 1,2,3 Data W/Wout PIN

+ VIEW MORE

Buy Devices Skimmers/Shimmers Cashout Devices

+ VIEW MORE

Buy Credit Card Data for all your scamming needs. Hotprice Carder Site has the

Buy Small Batch Skims

HOT PRICE

Buy Stolen Credit Card Data

Chain Fed Creditcard/EMV Data

HOME | PAPERS | COLLECTIONS | ABOUT | CONTACT | BLOG | 0

The Carder Site of the Future !!!



EMV/Chip 500$ ATM $1100 POS

SKU: 0001

Quality Of Source: One

$45.99

F-Region USA: Select

Automated ?: Select

Time Zone: Select

Set up for Fraud SMS?: Select

Stage one Password: Password: Password

Stage Two Password: Password: Password

You Private Key For Cashout: Enter up to 500 chars 500

Chat Method ? ICQ, Twitter, Bang5Chat, PureFDataApp: Enter up to 500 chars 500

Quantity: 1

# of Transactions?: Select

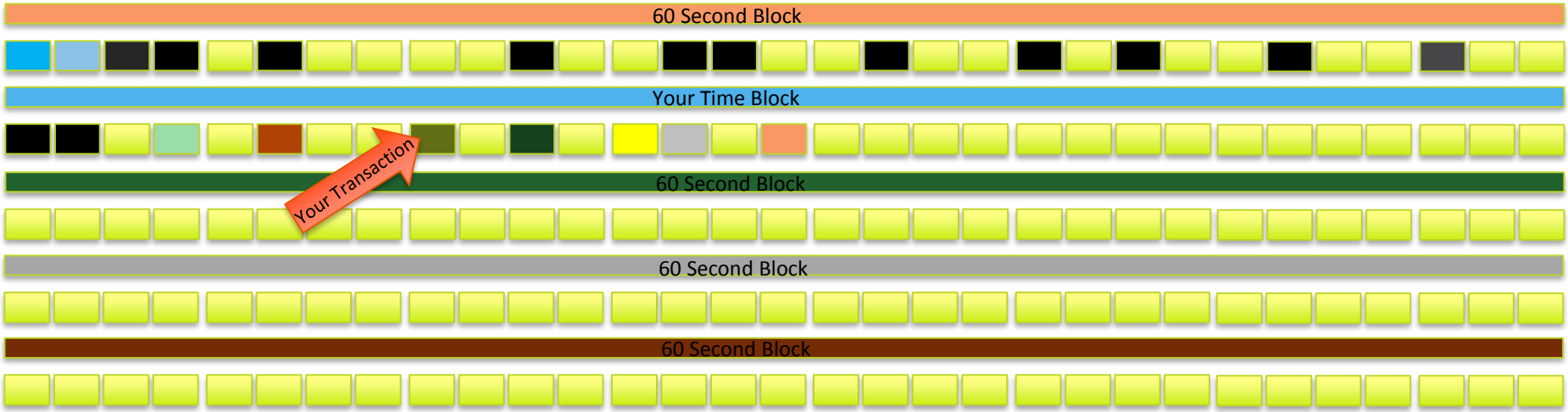
Time for Cashout ? EX 3:15: Enter up to 500 chars 500

ADD TO CART

PRODUCT INFO

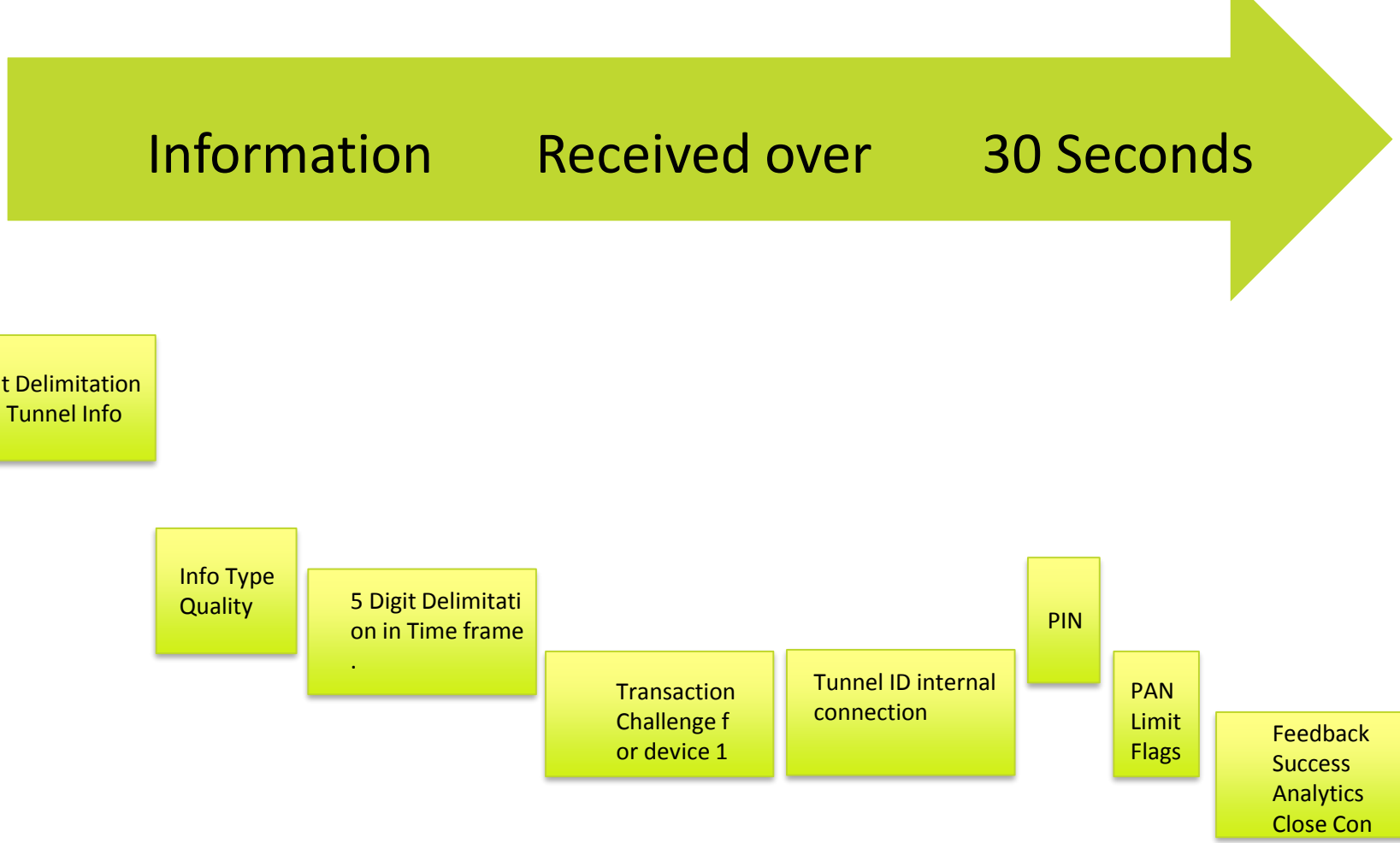
Live Chip Transaction Select Limit Bellow.

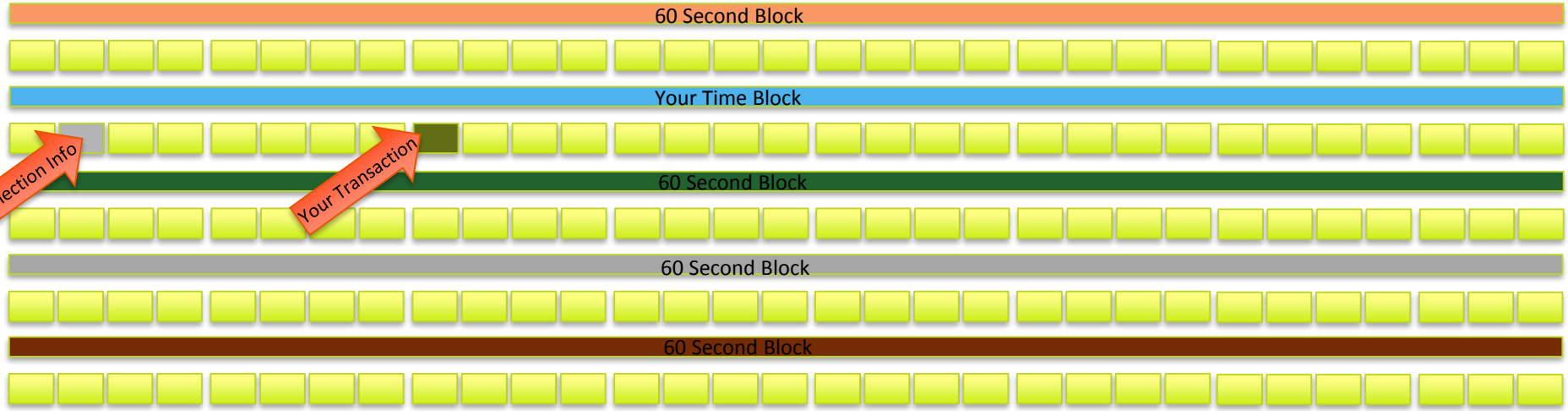
Complete With Spelling Errors !!



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


Information Received over 30 Seconds
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



Acceptable time Frame 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

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)

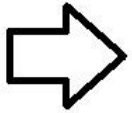
--SOME 13.56 RFID NFC (NON TOKEN BASED)

REJECTS CARDS WITH FLAGS NOT SET FOR ATM

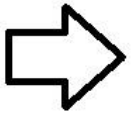
ASIDE FROM CARD PASS OFF BAD GUYS WILL ALSO GET PIN NUMBER AND ASSUMED ATM LIMIT

Shimmed ATM's





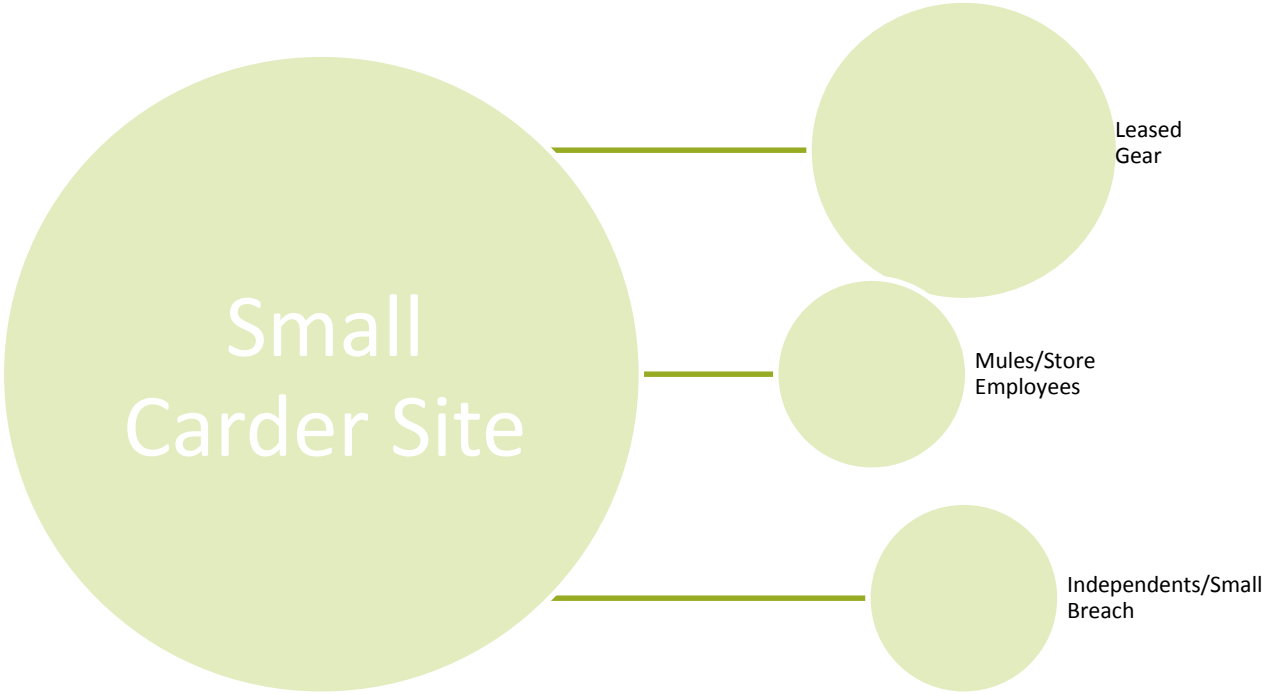


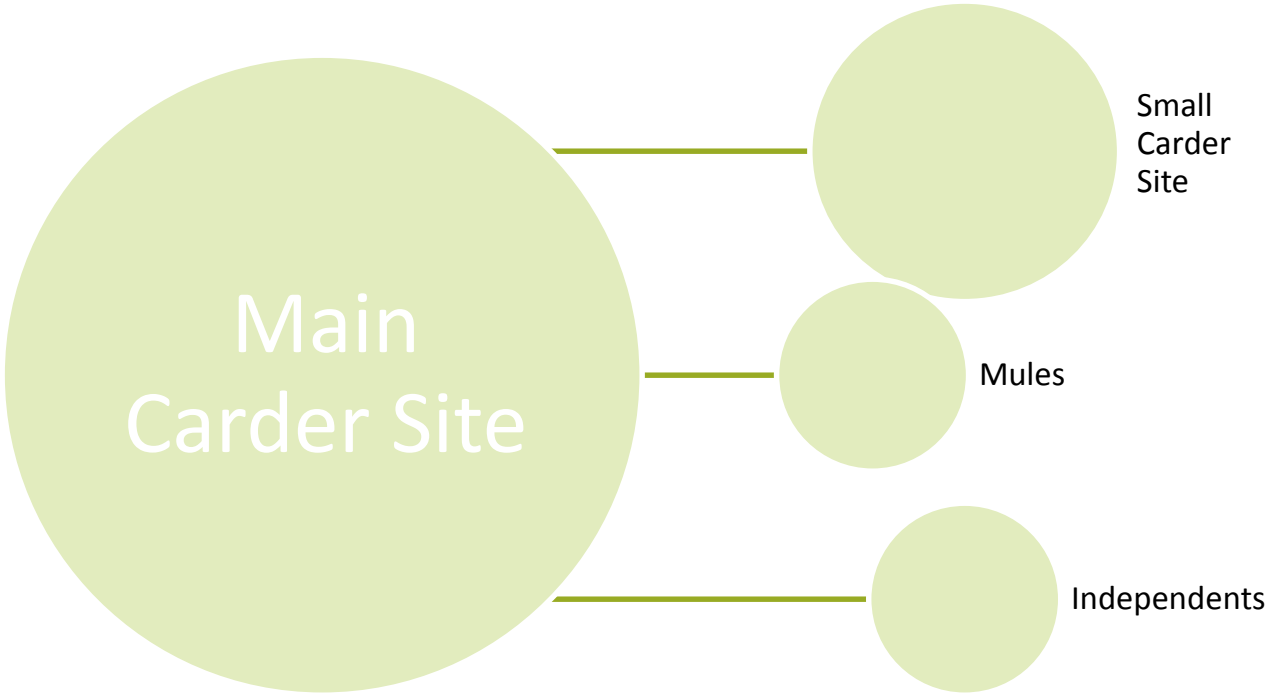


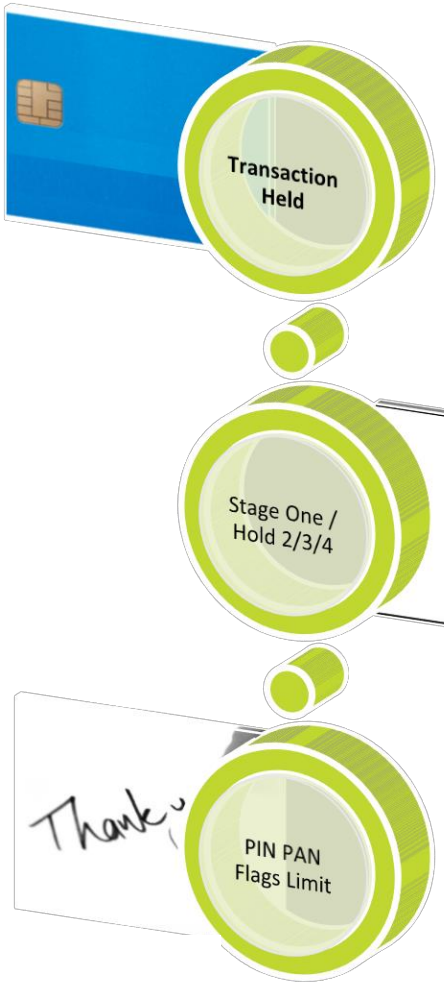
Cashout ATM



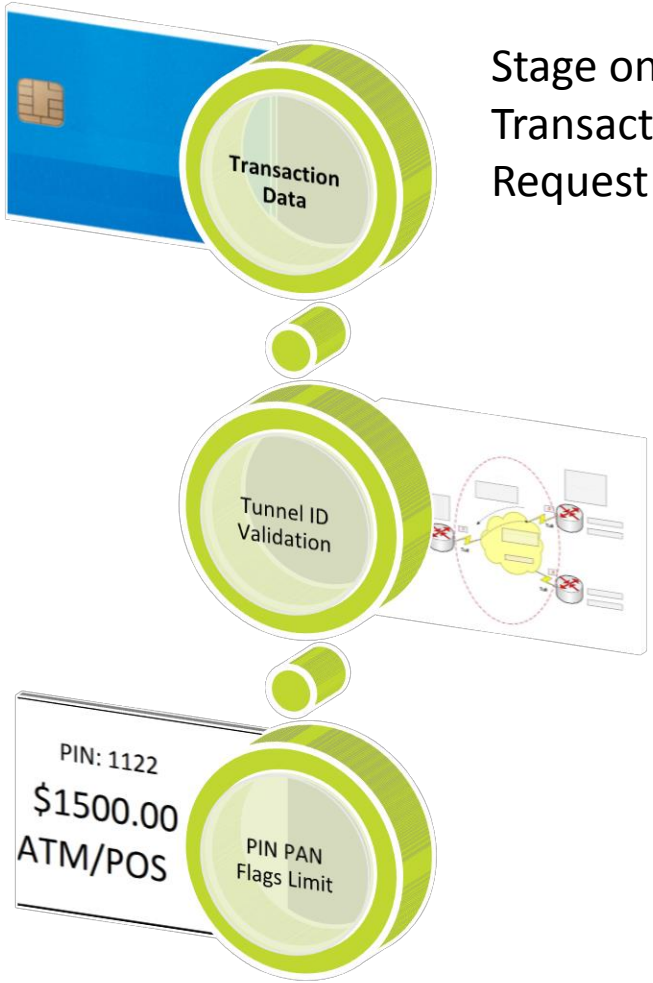
Here is the most likely method that sites get data that is sold.




Main
Carder Site
Small
Carder
Site
Mules
Independents



Hold for Round Two



Stage one Initial Transaction Request

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?

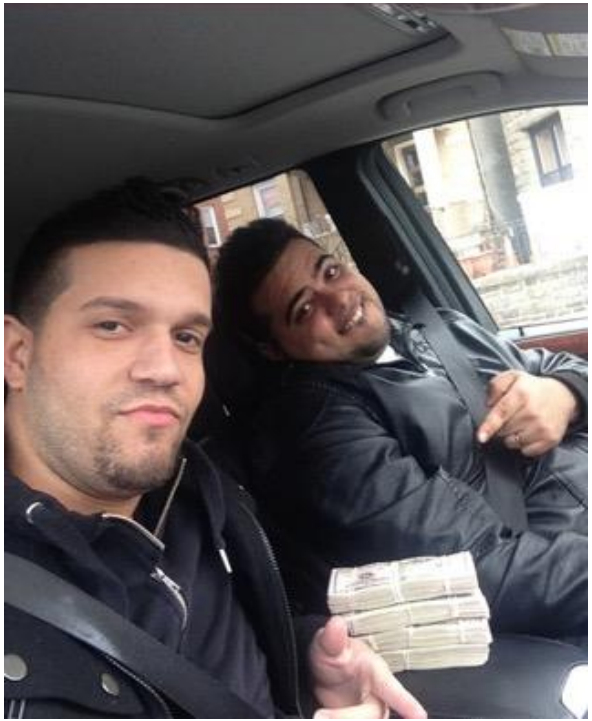


IC CARD
EXTENSION

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



@LaCaraATM

ATMs don’t have a twitter account ….



Making of La-Cara

That guy smiling like a child in the reflection is me



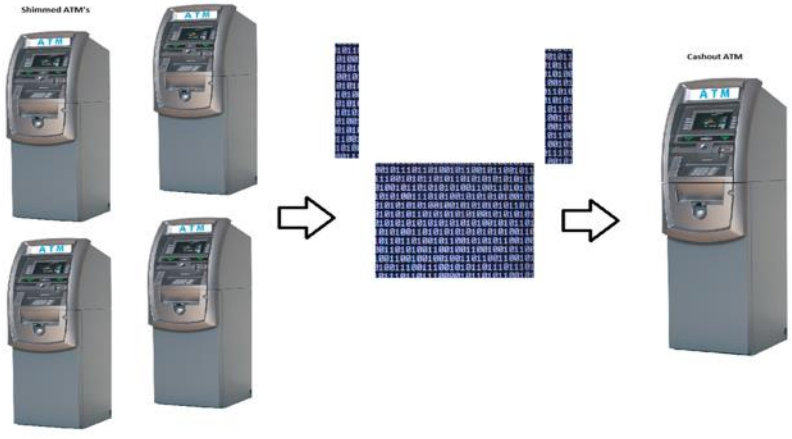

CANCEL
CLEAR
ENTER


CANCEL

Making of La-Cara

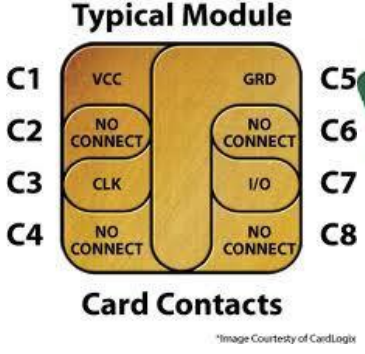


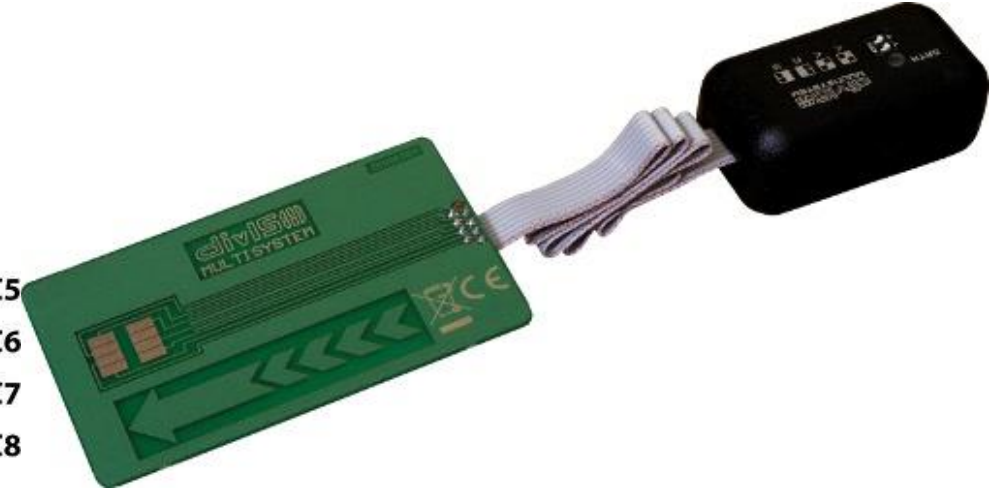
La-Cara Swiss army knife











Building your Own Banking Backend

Off branch ATM DES keys account signing

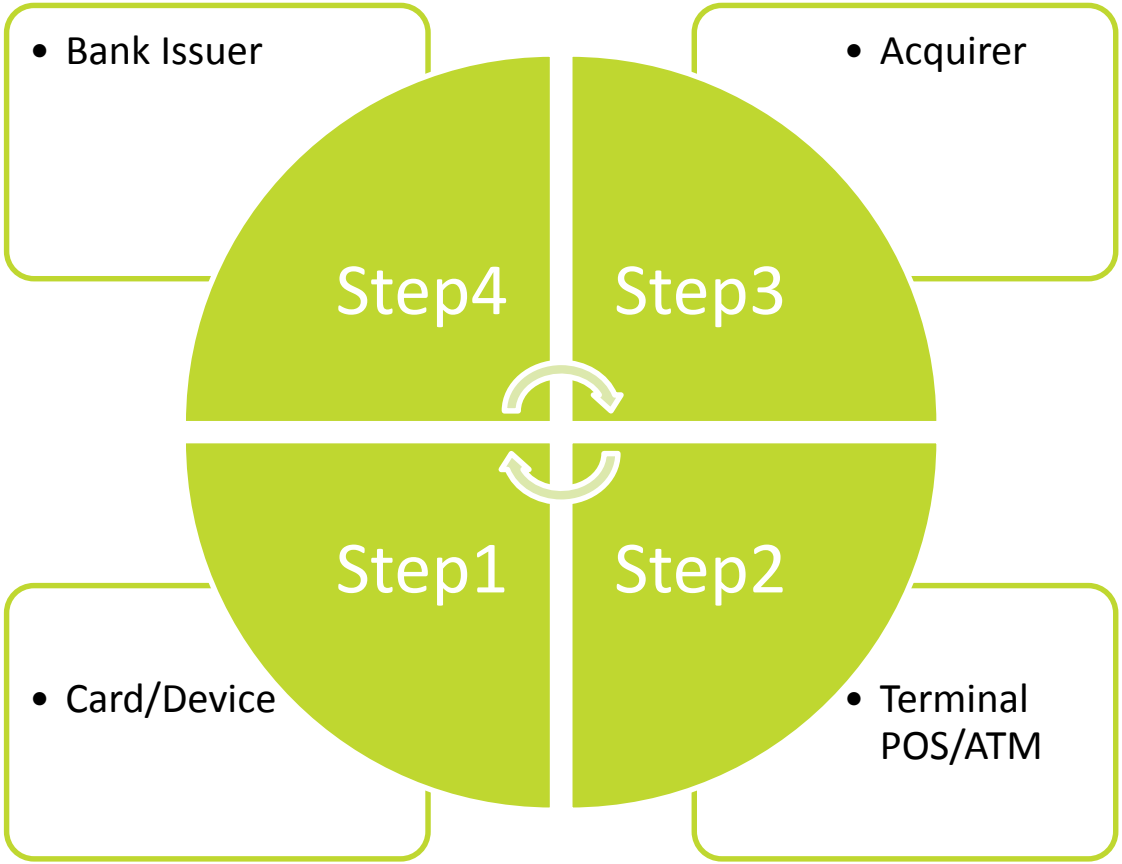
Each one of the accounts are signed with banking Keys

Each Card Transaction in Demo is Signed

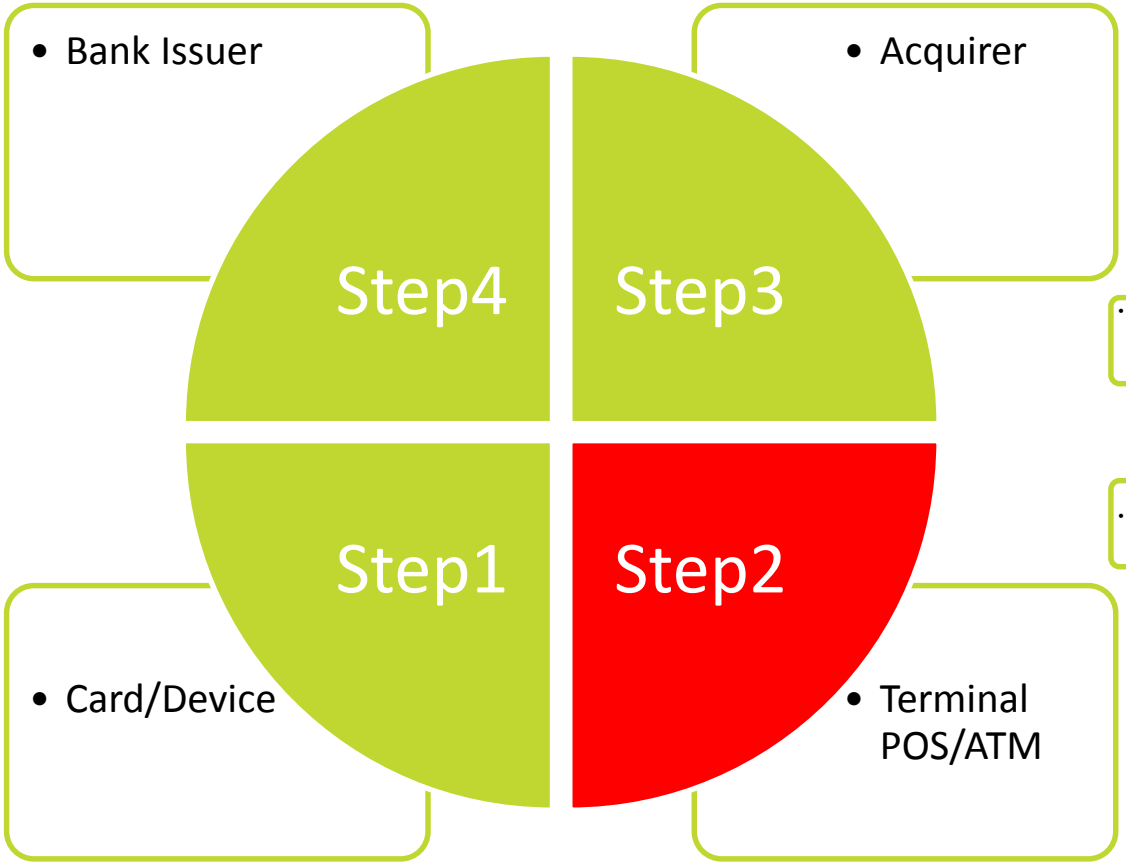
Skimmer Generation is signed with

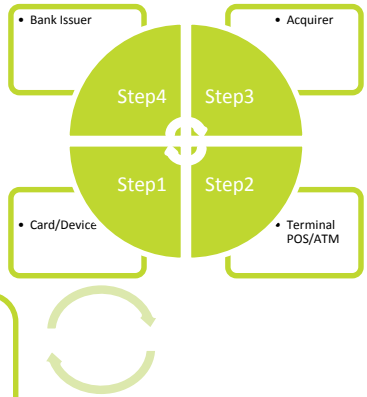
Field 55 training

EMV transaction



EMV transaction





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





Demo of Automation

- ✓$50,000 Prop money
- ✓So $500-$900 Per Transaction
- ✓So at most 60 transactions
- ✓Transaction 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