Hack in, Cash out
Hacking and Securing Payment Technologies

Tim Yunusov
Transaction stream fraud
Main question of the payment pentest

WHERE'S THE MONEY
Good pentest

Bad pentest
Get money from the bank 
From our own accounts
Decisions, decisions...

4 accounts in 2018
4 accounts in 2019

Prepared by: Arif Sidiqui
Card payment processing

Card → Endpoint → Acquirer → Card brands → Issuer’s Authorisation host
## Endpoints

<table>
<thead>
<tr>
<th>Endpoints</th>
<th>ATM</th>
<th>POS</th>
<th>Online</th>
</tr>
</thead>
<tbody>
<tr>
<td>Money</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Card's data</td>
<td>+</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Card's testing</td>
<td>Limited</td>
<td>+</td>
<td>+</td>
</tr>
<tr>
<td>Card's attacks</td>
<td>Limited</td>
<td>+</td>
<td>Limited</td>
</tr>
</tbody>
</table>
Most ATMs can be hacked in under 20 minutes

Experts tested ATMs from NCR, Diebold Nixdorf, and GRGBanking.

By Catalin Cimpanu for Zero Day | November 16, 2018 -- 05:30 GMT (05:30 GMT) | Topic: Security
@A1ex_S
@groke1105
@ivachyou
@L_AGalloway
POS+RCE – is the instrument

• EMV/NFC core real implementation
  • May contain a lot of bugs
• Real payment process workflow
  • Payment packet
  • Configurations (limits, etc)
  • Offline authentication and risk management
Example of the payment packet

BER encoding
• TLV – Tag Length Value
Example
• AA0105 [hex]
• Tag – AA
• Length – 1 byte
• Value - 05
Example of the payment packet

- PAN/Track2/Expiry date
- Transaction date and time
- Amount and currency
- Type of the operation (payment, cashback, refund, other)
- Type of the cryptogram, cardholder verification method

https://tvr-decoder.appspot.com
Attacks

- Refund/reverse attacks
- Chip & PIN attacks
- Card testing
Reverse attacks

Criminals Steal $4 Million In Cash With Novel 'Reverse ATM' Attack

Thomas Brewster Forbes Staff

Security

I cover crime, privacy and security in digital and physical forms.
Refund attacks

Money movements
Free infinite credit line

Purchase

Credit card

Refund

Debit card
Chip & PIN is still broken

• 2005 University of Cambridge, [https://murdoch.is/papers/cl05chipandspin.pdf](https://murdoch.is/papers/cl05chipandspin.pdf)

• 2010 Inverse Path (F-Secure) / Aperture Labs
  • Intercept PIN (ICC plaintext PIN verification)
  • Make transactions without PIN knowledge (“PIN OK” attack)
  • Downgrade to chip&signature
Chip & PIN is still broken

- CVM list – cardholder verification method list
  - CVM list is defined on the card
  - CVM List provides the terminal with four pieces of information on how an issuer wishes the cardholder to be verified:
    - CVM method (in priority)
    - Conditions of use
    - What if the CVM method is failed
    - Encrypted PIN if supports, then Unencrypted PIN if supports, the signature, than cancel
  - https://tvr-decoder.appspot.com
- Offline data authentication – when POS checks that card and it’s data were genuine: SDA, DDA, CDA
When hackers come

  - 40 cards
  - PIN-OK additional chip
  - 7000 transactions
  - 680,000 USD
Chip & PIN is still broken

- 2019, Europe
  - PIN interception, “PIN OK” attack, chip&signature downgrading

- Why?
  - “Nowadays CVM is signed” (c) Inverse Path - CDA
  - Weak CVM Lists: PIN Online if unattended, PIN Offline elsewhere
  - Visa cards do not provide Offline Data Authentication
  - Card supports (DDA,CDA), terminal supports (DDA,CDA):
    - Terminal choose DDA
    - Terminal goes online if the offline authentication is failed
Card testing

- Balance testing for stolen cards
When hackers come first

- Nov, 2016, 40,000 accounts, 9,000 successfully

Tesco Bank says attack cost it £2.5m and hit 9,000 people

Was it hacked?

Tesco did not use the "H" word in its statement and in interviews
Card testing

• 1 Dec 2016, Newcastle University
• https://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf

• Consecutive enumeration:
  • BIN (public DB)
  • PAN (online banking registration)
  • Expiry Date (refund, recipient of funds)
  • CVV (regular payment)
  • Postcode for AVS (different error)
Card testing

- 1 Dec 2016, Newcastle University
- https://eprint.ncl.ac.uk/file_store/production/230123/19180242-D02E-47AC-BDB3-73C22D6E1FDB.pdf

Consecutive enumeration:
- PAN (mobile banking registration)
- Expiry Date (refund, recipient of funds)
- CVV (regular payment)
- Postcode for AVS (different error)

FCA fines Tesco Bank £16.4m for failures in 2016 cyber attack

Press Releases | Published: 01/10/2018 | Last updated: 01/10/2018
Card testing

- July 2018, Monzo

Transaction attacks

On the Monday morning I visited Monzo’s offices, just 12 hours earlier there had been a “pan enumeration” attack on its computer systems. This is where fraudsters, often based overseas, bombard a bank’s computers, trying to guess passwords and logins, or attempting to do transactions by generating card expiry dates and three-digit CVVs (card verification codes) in the hope that some might break through.
Rounding

Practical exploitation of rounding vulnerabilities in internet banking applications

Adrian Furtună, PhD, OSCP, CEH
adif2k8@gmail.com

Round error issue – produce money for free on itBit bitcoin exchange (hackerone.com)
70 points by waffle_ss on Mar 3, 2017
Rounding

- 1 GBP = 1,30 USD
- 0.02 USD => float(0.0153; 2) == 0.02 GBP
- 0.02 GBP => float(0.026; 2) == to 0.03 USD
- Profit = 0.01 USD
Rounding

- 1 GBP = 1,30 USD
- 0.02 USD => float(0.015)
- 0.02 GBP => float(0.03)
- Profit = 0.01 USD
Rounding

• 1 GBP = 1,30 USD
• 0.02 USD => float(0.0153; 2) == 0.02 GBP
• 0.02 GBP => float(0.026; 2) == to 0.03 USD
• Profit = 0.01 USD

x10,000
• OTP bypass
• Antifraud bypass
• Don’t need to do everything manually
Stat

- Maximum amount per project – $463,843 in 3 days (in live)
- In 2019 – 8/8 banks in Europe were *potentially* vulnerable to rounding,
  
  one bank has confirmed the vulnerability
How to lose money during payment research

• Startup, which “allows you to spend money from any of your accounts using just one * Card” - *1234
• Connect any of your cards in the mobile app
• When you pay from the card *1234, money will be withdrawn from the card you’ve chosen and connected (*5678)
• What if we will use Card2Card and send From *1234 To *5678
• Just a regular transaction for *5678
• We will get a cashback!
How to lose money during payment research

- Send £100
- Money were withdrawn twice!
- Waited 5+ days
- Used 3 different card2card services
- Used 3 different cards, connected in the app
How to lose money during payment research
How to lose money during payment research

https://medium.com/@Tim_Y/how-to-lose-money-during-payment-research-or-in-searching-for-financial-ombudsman-5047bff89bc2
Who will pay?

- Not all vendors/banks are the same
- Risk-based model doesn’t care “where’s the money”, but “how much money”

<table>
<thead>
<tr>
<th>Bugbounty company from Google</th>
<th>Bank “A”</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Found vulnerability</td>
<td>1. Found vulnerabilityity</td>
</tr>
<tr>
<td>2. Reported with lowest CVSS/out of scope</td>
<td>2. Reported medium CVSS</td>
</tr>
<tr>
<td>3. Thanks, $$$</td>
<td>3. It’s not been used in the wild</td>
</tr>
<tr>
<td>4. Now vulnerabilities won’t be used in the wild</td>
<td>4. Vulnerabilities still can be used in the wild</td>
</tr>
</tbody>
</table>