INVERSE PATH

Aperture Labs

Chip & PIN is definitely broken

Credit Card skimming and PIN harvesting in an EMV world

Andrea Barisani
<andrea@inversepath.com>

Daniele Bianco
<daniele@inversepath.com>

Adam Laurie
<adam@aperturelabs.com>

Zac Franken
<zac@aperturelabs.com>

What is EMV?

EMV stands for Europay, MasterCard and VISA, the global standard for inter-operation of integrated circuit cards (IC cards or "chip cards") and IC card capable point of sale (POS) terminals and automated teller machines (ATMs), for authenticating credit and debit card transactions.

IC card systems based on EMV are being phased in across the world, under names such as "IC Credit" and "Chip and PIN".

Source: Wikipedia

Why EMV?

- ICC / smartcard
- improved security over existing magnetic stripe technology
- “offline” card verification and transaction approval
- multiple applications on one card

Liability shift

- liability shifts away from the merchant to the bank in most cases (though if merchant does not roll EMV then liability explicitly shifts to it)
- however the cardholders are assumed to be liable unless they can unquestionably prove they were not present for the transaction, did not authorize the transaction, and did not inadvertently assist the transaction through PIN disclosure
- PIN verification, with the help of EMV, increasingly becomes "proof" of cardholder presence

Liability shift

- VISA Zero Liability fine print (US):

  Does not apply to ATM transactions, PIN transactions not processed by Visa, or certain commercial card transactions. Individual provisional credit amounts are provided on a provisional basis and may be withheld, delayed, limited, or rescinded by your issuer based on factors such as gross negligence or fraud, delay in reporting unauthorized use, investigation and verification of claim and account standing and history. You must notify your financial institution immediately of any unauthorized use. Transaction at issue must be posted to your account before provisional credit may be issued. For specific restrictions, limitations and other details, please consult your issuer.

INVERSE PATH

Aperture Labs

Liability shift

Canadian Imperial Bank of Commerce (CIBC) spokesman Rob McLeod said in relation to a $81,276 fraud case: “our records show that this was a chip-and-PIN transaction. This means [the customer] personal card and personal PIN number were used in carrying out this transaction. As a result, [the customer] is liable for the transaction.”

The Globe and Mail, 14 Jun 2011

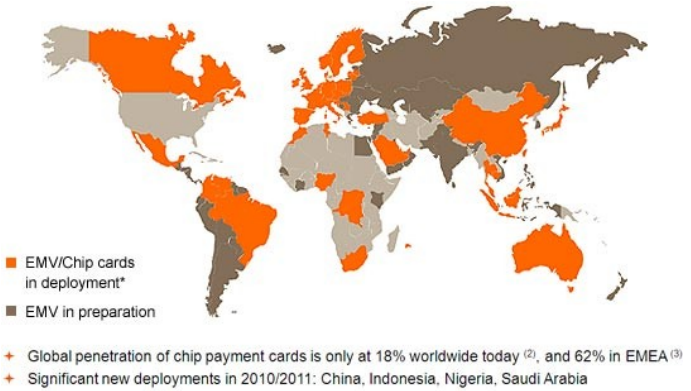
EMV adoption

Worldwide EMV Deployment and Adoption*

Region	EMV Cards	Adoption Rate	EMV Terminals	Adoption Rate
Canada, Latin America, and the Carribbean	182,185,043	26.4%	2,000,000	55.6%
Asia Pacific	305,126,927	26.6%	3,200,000	41.6%
Africa & the Middle East	16,841,874	13.7%	348,000	62.5%
Europe Zone 1	555,688,434	65.4%	9,400,000	84.7%
Europe Zone 2	22,817,271	11.5%	457,800	61.2%
United States†				
TOTALS	1,082,659,549	36.0%	15,405,800	65.0%

* Figures reported in September 2010 and represent the latest statistics from American Express, JCB, MasterCard and Visa, as reported by their member financial institutions globally.

† Figures do not include data from the United States.



- 03/2006 EPC Card Fraud Prevention Task Force presentation: "Ban of magstripe fallback foreseen (date to be decided)"
- as of 03/2011 magstripe fallback is still accepted pretty much everywhere

EMV is broken

- S. J. Murdoch, S. Drimer, R. Anderson, M. Bond, "Chip and PIN is Broken" - University of Cambridge
- the excellent group of researchers from Cambridge proved that stolen cards can be successfully used without knowing the PIN
- the industry claims difficult practicality of the attacks, at least one bank rolled out detection/blocking procedures

INVERSE PATH

Aperture Labs

Skimming, Cloning and PIN harvesting

- skimmer: hidden electronic device that intercepts card <> terminal communication and collects available data
- we analyze the practicality of credit card information skimming, cloning and PIN harvesting on POS terminals
- we intentionally ignore magstripe skimming (which is still effective and widely used) and focus on the chip interface

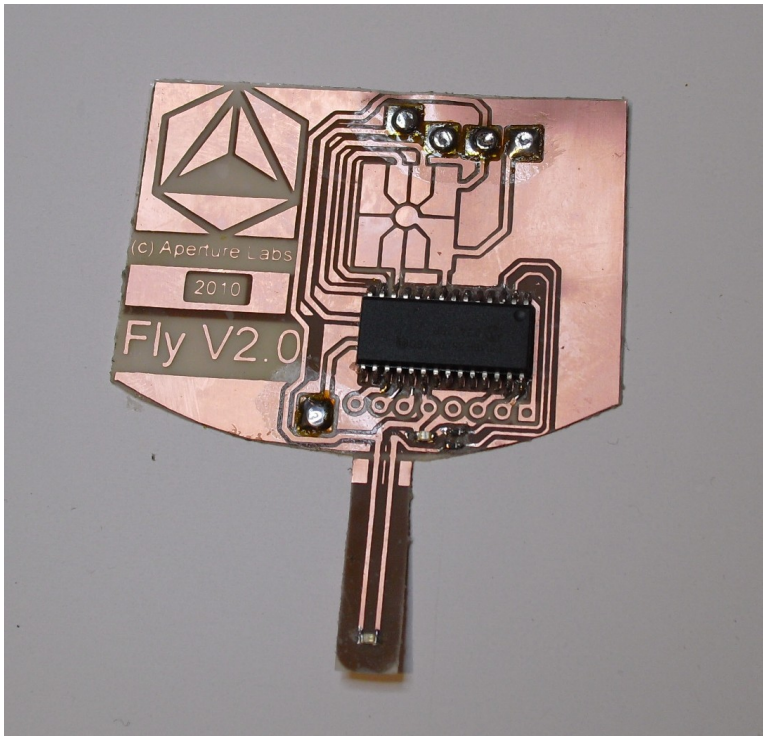
INVERSE PATH

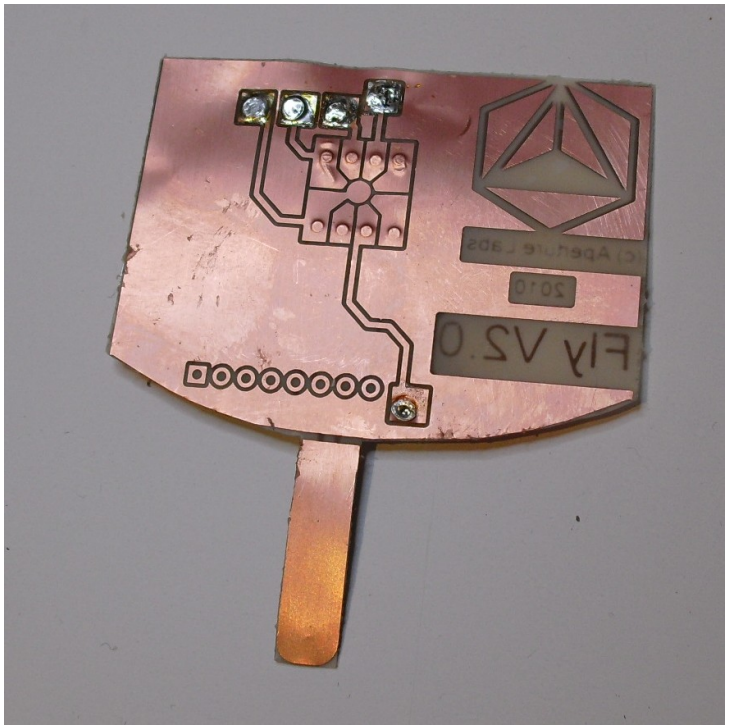
Aperture Labs

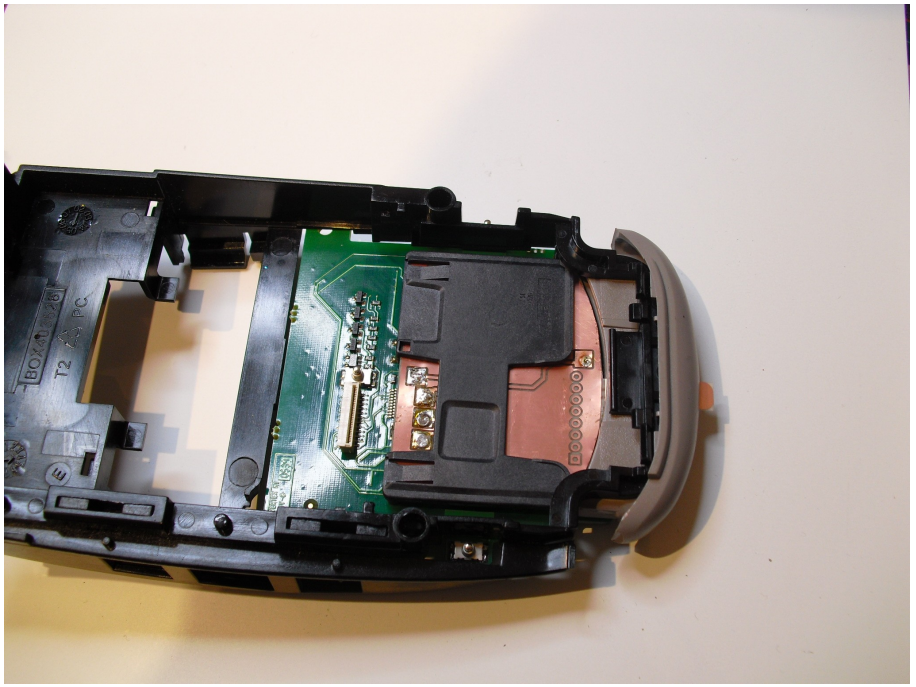
ATM skimmers

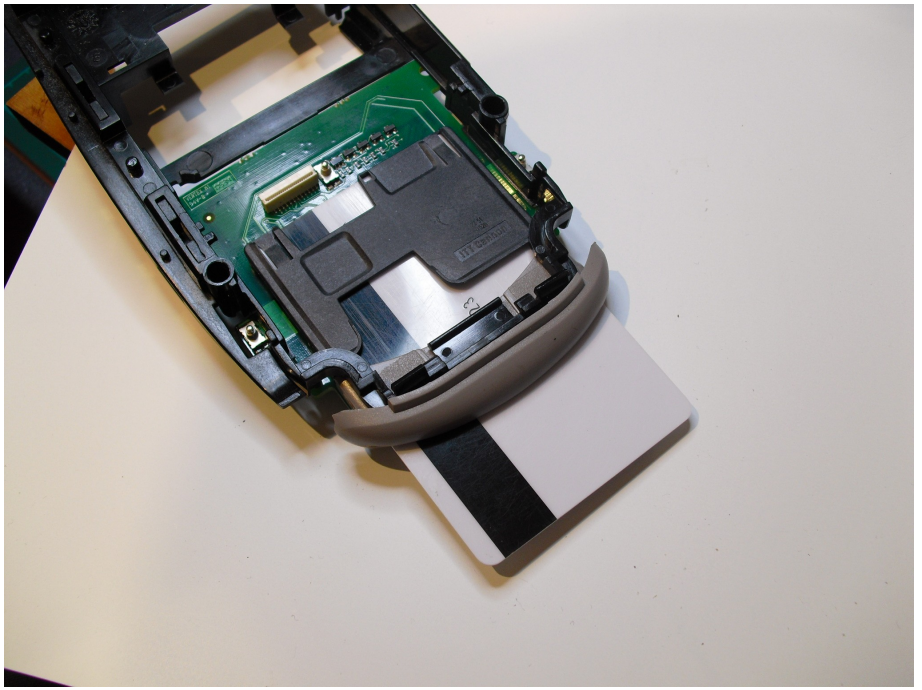
EMV skimmers

- we predict that skimming the chip will become an extremely appealing target to fraudsters
- the chip interface is inherently accessible
- it becomes impossible for the user to verify if the terminal has been tampered as the chip interface is not visible (unlike most magstripe one for POS terminals)
- an EMV skimmer could go undetected for a very long time and requires little installation effort









EMV skimmer

- trivial installation by “hooking” with a special card
- powered by the POS itself
- data can be downloaded with a special card recognized by the skimmer
- little development effort + cheap

EMV smartcards

- information is stored on a filesystem organized in applications, files and records

- the terminal talks to the card via APDU messages for reading records and issuing commands

```
Examples:

00A404000E315041592E5359532E4444463031 <- Select '1PAY.SYS.DDF01'
0020008008246666FFFFFFFFFF             <- Verify PIN ('6666')
```

- the EMV skimmer can intercept, read, man-in-the middle every part of the terminal <> ICC exchange

Terminal <> ICC exchange

1 | initiate application processing

2 | read application data

3 | offline data authentication (if indicated in the AIP)

4 | cardholder verification (if indicated in the AIP)

5 | issuer script processing

Read application data

- stored with BER-TLV templates and read by the terminal, some examples:

```
 tag name
----|-------------------------------------
  4f Application Identifier (VISA)
5f2d Language Preference (itenfrde)
9f1f Track 1 Discretionary Data
  57 Track 2 Equivalent Data
5f25 Application Effective Date
5f24 Application Expiration Date
  5a Application PAN (credit card number)
  8e Cardholder Verification Method (CVM) List
5f20 Cardholder Name
9f36 Application Transaction Counter (ATC)
9f17 PIN Try Counter
```

EMV application data - magstripe clone

```
      Format Code: 'B' (fixed value for financial cards)

      Service Code: 229 (use chip, online transaction)

   5a Application Primary Account Number: 4030330000000001

 5f20 Cardholder Name: DARTH VADER

 5f24 Application Expiration Date YYMM: 141231

 9f1f Track 1 Discretionary Data: 5482300000000000228000000

   57 Track 2 Equivalent Data: 4030330000000001=141229954823228

Track 1 clone:
B4030330000000001^DARTH VADER                ^1412229548230000000000228000000

Track 2 clone:
4030330000000001=141222954823228
```

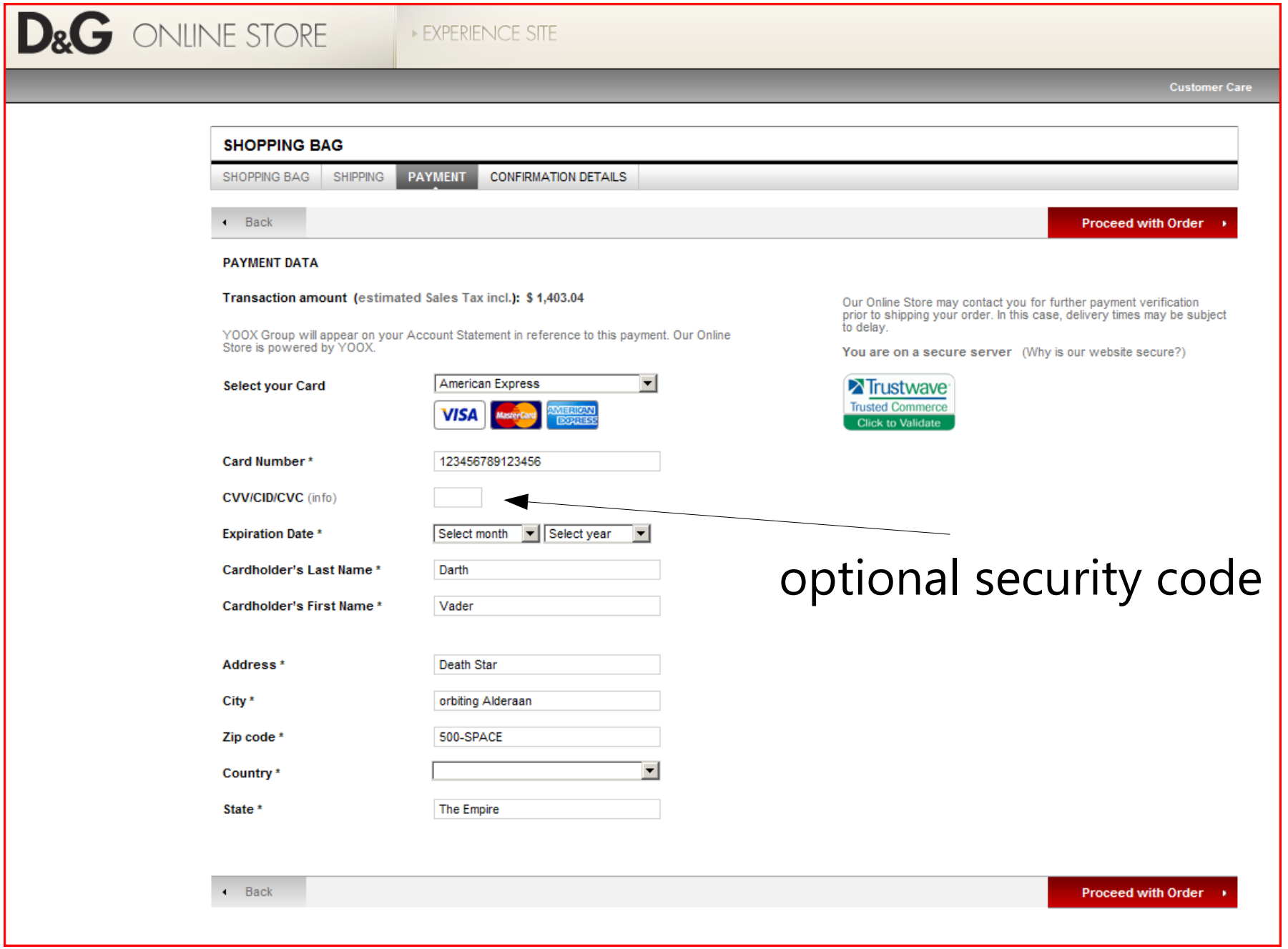
The CVV (228) matches the magstripe one only for cards that do not use iCVV (a different stored value to protect against this attack, introduced in January 2008 but not present on all cards)

EMV application data - magstripe clone

- while the service code on the magstripe might indicate that the chip must be used, inserting a card without a readable chip will trigger magstripe fallback on all tested terminals
- EMV skimmers cannot clone successfully to magstripe if iCVV is used
- however it is fair to say that the possibility of massive harvesting + being protected by a 3 digits code is not a comforting scenario

EMV application data - online usage

- application data can be used to perform Card Not Present transactions (online, phone, ...) with parties that do not check Card Security Code (CVV, CVV2, ...) and do not employ 3-D secure (Verified by Visa, MasterCard SecureCode also known as phishing heaven)
- if you think that the amount of websites that do not check the security code is negligible...think again
- ironically one of the authors has been defrauded on such sites while this presentation was being written...



Offline data authentication

- depending on the chip technology three methods are available: Static Data Authentication (SDA), Dynamic Data Authentication (DDA), Combined Data Authentication (CDA)
- used by the terminal to validate the authenticity of the card
- enables offline transactions where supported
- never used by ATM (always online)
- Visa and MasterCard mandate all cards issued after 2011 to use DDA

INVERSE PATH

Aperture Labs

Static Data Authentication (SDA) cards

- cheapest and most widely used technology
- selected records (advertised by the card and customized by the issuer) are signed with a static signature
- symmetric key is used for online transactions
- offline PIN verification is always cleartext

```
  8f: Certificate Authority Public Key Index (PKI)
  90: Issuer PK Certificate
9f32: Issuer PK Exponent
  92: Issuer PK Remainder
  93: Signed Static Application Data
```

INVERSE PATH

Aperture Labs

Dynamic Data Authentication (DDA) cards

- chip is more expensive, rare usage as of 2011
- static data validation (against hash within certificate)
- dynamic data validation, terminal asks the card to sign data + random number with ICC PK
- ICC PK embeds PAN (limiting private key usage to this card)
- offline PIN verification can be cleartext or enciphered

```
  8f: Certificate Authority Public Key Index (PKI)

  90: Issuer PK Certificate       9f46: ICC PK Certificate
9f32: Issuer PK Exponent          9f47: ICC PK Exponent
  92: Issuer PK Remainder         9f48: ICC PK Remainder

9f49: Dynamic Data Authentication Data Object List (DDOL)
```

Chip cloning

- SDA cards can be cloned and used without PIN for offline transactions only (“Yes” card)
- DDA cards clone ineffective for offline and online transactions, however a valid DDA card can be used to pass offline authentication and perform fake offline transaction (not tied to the authentication)
- offline transactions are rare in EU

Threats

- data stealing: we discussed EMV skimming usage for magstripe cloning and online usage
- card stealing: Cambridge research shows that stolen cards can be used without PIN, hopefully this attack will be fixed
- does state of the art EMV usage really protect against PIN harvesting and therefore the use of stolen cards?

INVERSE PATH

Aperture Labs

Cardholder verification

- the card advertises to the terminal the cardholder verification method preference via the CVM List (tag 8E)

Cardholder Verification Method (CVM) Condition Codes

Bits	Meaning	Value
8 7 6 5 4 3 2 1		
0	RFU	N/A
0	Fail cardholder verification if this CVM is unsuccessful	N/A
1	Apply succeeding CV rule if this CVM is unsuccessful	N/A
0 0 0 0 0 0	Fail CVM processing	00 or 40
0 0 0 0 0 1	Plaintext PIN verification performed by ICC	01 or 41
0 0 0 0 1 0	Enciphered PIN verified online	02 or 42
0 0 0 0 1 1	Plaintext PIN verification by ICC and signature (paper)	03 or 43
0 0 0 1 0 0	Enciphered PIN verification by ICC	04 or 44
0 0 0 1 0 1	Enciphered PIN verification by ICC and signature (paper)	05 or 45
0 0 0 1 0 1	Enciphered PIN verification by ICC and signature (paper)	05 or 45
0 x x x x x	Values in range 000110 – 011101 reserved for future use	06-1D/16-5D
0 1 1 1 1 0	Signature (paper)	1E or 5E
0 1 1 1 1 1	No CVM required	1F or 5F
1 0 x x x x	Values in range 100000 – 101111 reserved for future use	20-2F/60-6F
1 1 x x x x	Values in range 110000 – 111110 reserved for future use	30-3E/70-7E
1 1 1 1 1 1	Not available	3F or 7F

CVM List

- the CVM List is nowadays signed on all cards, therefore it is believed to be tamper proof
- if the preferred authentication method is `Signature (paper)`, `Enciphered PIN verified online` or `Enciphered PIN verification by ICC` then the PIN is not sent by the terminal to the card
- it is believed that only when `Plaintext PIN verification performed by ICC` is present and selected from the CVM List the PIN can be harvested by the EMV skimmer

Action Codes

- assuming a scenario with DDA only cards and a “secure” CVM List can we still harvest the PIN ?
- Issuer Action Codes (card) and Terminal Action Codes (terminal) specify policies for accepting or rejecting transactions (using TVR specifications)
- Issuer Action Codes and Terminal Action Codes are OR'ed
- three kinds: Denial, Online, Default; the Online Action Codes specify which failure conditions trigger online transactions

INVERSE PATH

Aperture Labs

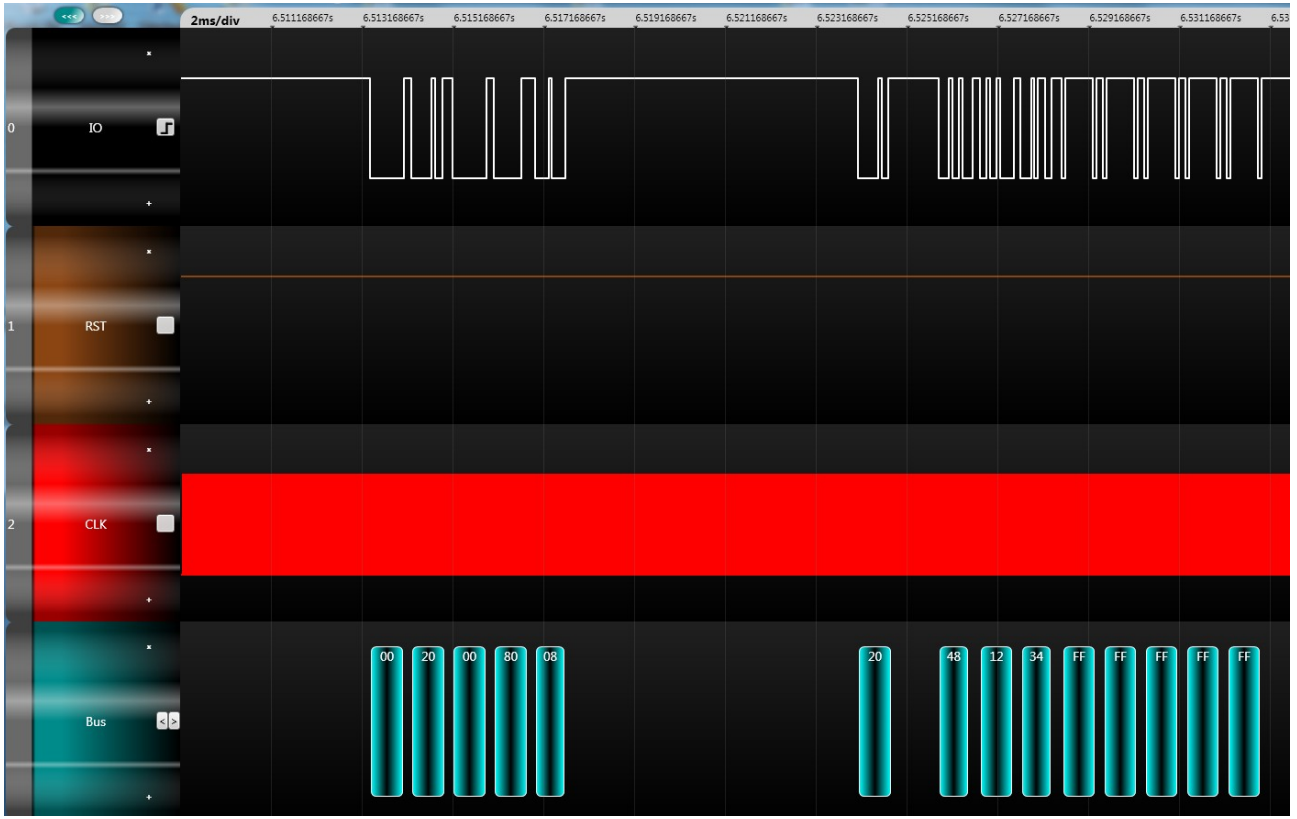
Action Codes Example

```
9f0e Issuer Action Code - Denial  (5 bytes): 00 00 00 00 00
9f0f Issuer Action Code - Online  (5 bytes): f0 78 fc f8 00
9f0d Issuer Action Code - Default (5 bytes): f0 78 fc a0 00
```

- translation: “do not deny a transaction without attempting to go online, if offline SDA fails transmit the transaction online”
- in all tested terminals / cards we were able to manipulate the action codes (when necessary) so that tampering with the CVM List would not result in offline rejection

CVM List downgrade

- the modified CVM List is honoured by the terminal which means that `Plaintext PIN verification performed by ICC` can be presented enabling PIN harvesting for SDA/DDA cards



INVERSE PATH

Aperture Labs

transaction log: card with online PIN verification

```
00a4040007a0000000031010 Select AID (VISA)
00c0000027               Get additional data
80a80000028300           Get processing options
00c0000010               Get additional data
00b2010c00               Read data files...
00b2010c40
00b2011400
00b20114c3
00b2021400
00b20214b2
00b2011c00
00b2011c52
00b2021c00
00b2021c45
80ae80001d...            Generate AC (online transaction)
...
```

INVERSE PATH

Aperture Labs

transaction log: same card with tampered CVM

```
00a4040007a0000000031010 Select AID (VISA)
00c0000027               Get additional data
80a80000028300           Get processing options
00c0000010               Get additional data
00b2010c00               Read data files...
00b2010c40
00b2011400
00b20114c3
00b2021400
00b20214b2
00b2011c00
00b2011c52
00b2021c00
00b2021c45
80ca9f1700                 Get PIN try counter (unknown length)
80ca9f1704                 Get PIN try counter (corrected length)
0020008008241234ffffffffff Verify PIN (1234)
80ae80001d...              Generate AC (online transaction)
...
```

INVERSE PATH

Aperture Labs

Backend detection - Terminal Data

```
8 7 6 5 4 3 2 1 Bits
--------------------------------------------------------------------
```

Terminal Verification Results (byte 1 of 5)

```
1 x x x x x x x Offline data processing was not performed
x 1 x x x x x x SDA failed
x x 1 x x x x x ICC data missing
x x x 1 x x x x Card number appears on hotlist
x x x x 1 x x x DDA failed
x x x x x 1 x x CDA failed
--------------------------------------------------------------------
```

CVM Results (byte 3 of 3)

```
0 0 0 0 0 0 0 0 unknown
0 0 0 0 0 0 0 1 Failed
0 0 0 0 0 0 1 0 Successful

                CVM Results byte 1: code of CVM Performed
                CVM Results byte 2: code of CVM Condition
```

Backend detection - Card Data

```
8 7 6 5 4 3 2 1 Bits
-------------------------------------------------------------------
```

Cardholder Verification Results (bytes 1,2 of 4)
Common Payment Application Specification format

```
0 0 x x x x x x AAC returned in second GENERATE AC
0 1 x x x x x x TC returned in second GENERATE AC
1 0 x x x x x x Second GENERATE AC not requested
x x 0 0 x x x x AAC returned in first GENERATE AC
x x 0 1 x x x x TC returned in first GENERATE AC
x x 1 0 x x x x ARQC returned in first GENERATE AC
x x x x 1 x x x CDA performed
x x x x x 1 x x Offline DDA performed
x x x x x x 1 x Issuer Authentication not performed
x x x x x x x 1 Issuer Authentication failed

x x x x 1 x x x Offline PIN Verification Performed
x x x x x 1 x x Offline PIN Verification Performed and Failed
x x x x x x 1 x PIN Try Limit Exceeded
x x x x x x x 1 Last Online Transaction Not Completed
```

INVERSE PATH

Aperture Labs

Backend detection

- the attack execution might be detected by the backend (via the TVR, CVM Results and CVR advertising failed data authentication and cleartext CVM) but blocking a card solely on this information does not feel like a realistic solution

- a downgraded CVM List with offline PIN + fallback to online PIN might be used to “hide” cleartext CVM Results and CVR by answering incorrect PIN offline verification to the terminal (without passing the command to the card), customer would be prompted twice for the PIN

INVERSE PATH

Aperture Labs

Backend detection

- (untested) it would be also possible for the skimmer to advertise relevant offline authentication records from a stored valid SDA card with a convenient CVM List for the authentication phase, and use the real card for the transaction, this would result in “clean” TVR, CVM Results and CVR
- Terminal Capabilities (9f33), when requested by the card via CDOL1/CDOL2 and sent by the terminal via GENERATE AC, can be intercepted and rewritten to advertise only SDA capability in case of DDA card skimming
- CDA is designed to protect against this but it should still be possible for the skimmer to force usage as an SDA card

Summary

- an EMV skimmer poses a serious threat due to ease of installation and difficult detection
- EMV data allows fraudulent usage on websites that perform insufficient validation (as well as magstripe clone for cards that do not use iCVV)
- the PIN can be always intercepted despite card type (SDA or DDA) and CVM / Issuer Action Codes configuration
- stealing an EMV chip & pin card that was previously skimmed enables full usage and raises serious liability considerations

Vendor Response

- EMVCo announced that the hole will not be fixed saying that "when the full payment process is taken into account, suitable countermeasures are available"
- MasterCard spokesman Jan Lundequist (head of chip product management) said in an interview that the EMV system is simply too complex for an easy fix
- In the Netherlands the hole has been reportedly closed by updating POS firmware with a version which apparently disables plaintext PIN verification for domestic cards (believed to be 100% DDA)

Recommendations

- despite industry claims about reduced fraud levels in our opinion EMV is inadequate and overly complex, it should be replaced with a simpler and cleaner solution
- correctly implemented crypto should be performed between card <> backend (online) or card <> terminal (offline) for double authentication and preventing interception/man-in-the-middle attacks for every single step of the transaction
- terminals cannot be trusted, PIN input and verification should be confined on the card itself (e-ink scrambled touchpad)

Recommendations

- "patching" EMV is possible by disabling plaintext PIN verification on POS and ATM firmwares preventing the downgrade attack
- despite some vendor response claiming otherwise this would play nicely with every card type as on-line PIN verification can be used for SDA
- actually on-line PIN verification could be used all the time, both North America and European banks have reportedly little use for the whole off-line verification mess pushed by EMV and could do everything on-line...

INVERSE PATH

Aperture Labs

chip skimmer installations dated 2008 have been reported in the wild by law enforcement authorities after this presentation was made available

INVERSE PATH

Aperture Labs

http://www.inversepath.com

http://www.aperturelabs.com

sponsored by:

http://www.integra-group.it