Differential Attacks on PIN Processing APIs

Graham Steel

LSV

Overview

Photo: redspotted/Flickr

Verizon Breach Report 2008

Released April 2009

Verizon Breach Report 2008

Released April 2009

“While statistically not a large percentage of our overall caseload in 2008, attacks against PIN information represent individual data-theft cases having the largest aggregate exposure in terms of unique records,”

“In other words, PIN-based attacks and many of the very large compromises from the past year go hand in hand.”

Verizon Breach Report 2008

Released April 2009

“While statistically not a large percentage of our overall caseload in 2008, attacks against PIN information represent individual data-theft cases having the largest aggregate exposure in terms of unique records,”

“In other words, PIN-based attacks and many of the very large compromises from the past year go hand in hand.”

“We’re seeing entirely new attacks that a year ago were thought to be only academically possible,”

Verizon Breach Report 2008

Released April 2009

“While statistically not a large percentage of our overall caseload in 2008, attacks against PIN information represent individual data-theft cases having the largest aggregate exposure in terms of unique records,”

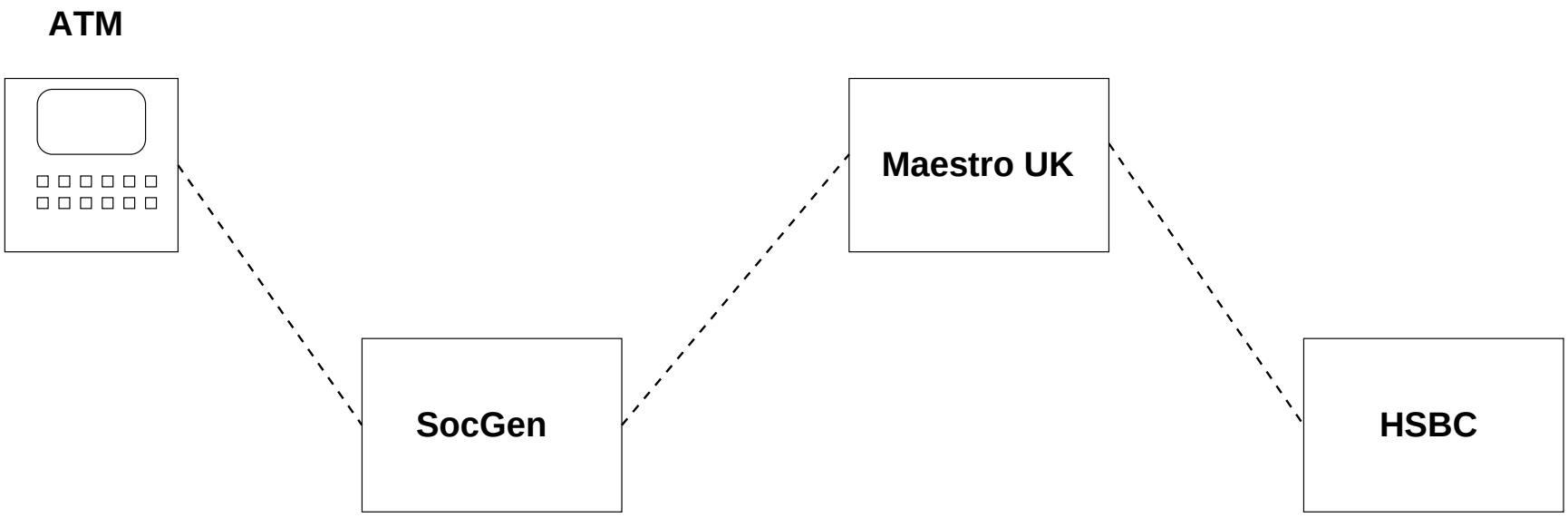
“In other words, PIN-based attacks and many of the very large compromises from the past year go hand in hand.”

“We’re seeing entirely new attacks that a year ago were thought to be only academically possible,”

“What we see now is people going right to the source [..] and stealing the encrypted PIN blocks and using complex ways to un-encrypt the PIN blocks.”

(Quotes from Wired Magazine interview with report author, Bryan Sartin)

Cash Machine Network



HSMs

- Manufacturers include IBM, VISA, nCipher, Thales, Utimaco, HP
- Cost around $10 000

Deriving a PIN: IBM 3624 Method

IPIN derived by:

Encode account number (PAN) as 0000AAAAAAAAAAAA

Deriving a PIN: IBM 3624 Method

IPIN derived by:

Encode account number (PAN) as 0000AAAAAAAAAAAA

3DES encrypt under a PDK (PIN Derivation Key)

Deriving a PIN: IBM 3624 Method

IPIN derived by:

Encode account number (PAN) as 0000AAAAAAAAAAAA

3DES encrypt under a PDK (PIN Derivation Key)

Take 4 leftmost hexadecimal digits of result

Deriving a PIN: IBM 3624 Method

IPIN derived by:

Encode account number (PAN) as 0000AAAAAAAAAAAA

3DES encrypt under a PDK (PIN Derivation Key)

Take 4 leftmost hexadecimal digits of result

Decimalise using a mapping table (’dectab’)

```
0123456789ABCDEF
0123456789012345
```

Deriving a PIN: IBM 3624 Method

IPIN derived by:

Encode account number (PAN) as 0000AAAAAAAAAAAA

3DES encrypt under a PDK (PIN Derivation Key)

Take 4 leftmost hexadecimal digits of result

Decimalise using a mapping table (’dectab’)

```
0123456789ABCDEF
0123456789012345
```

PIN = IPIN + Offset (modulo 10 each digit)

PIN Processing API

Verify PIN:

$\{\mathsf{PIN}\}_K, \mathsf{PAN}, \mathsf{Dectab} \quad \rightarrow$

Offset

yes/no $\quad \leftarrow$

K, PDK

PIN Processing API

Verify PIN:

$\{\mathsf{PIN}\}_K, \mathsf{PAN}, \mathsf{Dectab} \quad \rightarrow$

Offset

yes/no $\quad \leftarrow$

K, PDK

If host machine is attacked, PIN should remain secure (ANSI X7.8, ISO 9564 requirement)

Decimalisaton Table Attack (Clulow '02, Bond & Zeilinski '03)

Suppose in a hacked switch, an attacker has a set

$\{\mathsf{PIN}\}_K, \mathsf{PAN}, \mathsf{Dectab}, \mathsf{Offset}$ that verifies PIN is correct

Decimalisaton Table Attack (Clulow '02, Bond & Zeilinski '03)

Suppose in a hacked switch, an attacker has a set

$\{\mathsf{PIN}\}_K, \mathsf{PAN}, \mathsf{Dectab}, \mathsf{Offset}$ that verifies PIN is correct

Original Dectab

0123456789ABCDEF

0123456789012345

Dectab'

0123456789ABCDEF

1123456789112345

Decimalisaton Table Attack (Clulow '02, Bond & Zeilinski '03)

Suppose in a hacked switch, an attacker has a set

$\{\mathsf{PIN}\}_K, \mathsf{PAN}, \mathtt{Dectab}, \mathsf{Offset}$ that verifies PIN is correct

Original Dectab

```
0123456789ABCDEF
0123456789012345
```

Dectab'

```
0123456789ABCDEF
1123456789112345
```

Repeat verification command with Dectab'

Successfull verification indicates no 0s in PIN

More dectab attack

To find the 0s, try changing the offset

Attacker set offset	Result from HSM	Knowledge of PIN
0001	Incorrect PIN	????
0010	Incorrect PIN	????
0100	Incorrect PIN	????
1000	Incorrect PIN	????
0011	Incorrect PIN	????
0101	Correct PIN	?0?0

More PIN Cracking Attacks

- Dectab attacks
- Reformatting attacks
- Check value attack
- Calculate offset attack
- Competing verification algorithms attack

All require attacker to make ‘tweaked’ queries to HSM

Preventing Tweaked Queries

We use a Message Authentication Code (MAC)

Existing MAC on card: CVV/CVC - Card Verification Value(/Code)

5 decimal digits

Designed to make construction of fake cards more difficult

Preventing Tweaked Queries

We use a Message Authentication Code (MAC)

Existing MAC on card: CVV/CVC - Card Verification Value(/Code)

5 decimal digits

Designed to make construction of fake cards more difficult

PAN	Exp date	Service code	0 pad
16 digits max	4 digits	3 digits	9 digits max
Block B1	Block B2		

Preventing Tweaked Queries

We use a Message Authentication Code (MAC)

Existing MAC on card: CVV/CVC - Card Verification Value(/Code)

5 decimal digits

Designed to make construction of fake cards more difficult

PAN	Exp date	Service code	0 pad
16 digits max	4 digits	3 digits	9 digits max
Block B1	Block B2		

2-part DES key K1, K2.

$$CVV_{hex} \quad := \quad enc(K1, dec(K2, enc(K1, (enc(K1, B1) \oplus B2))))$$

CVV’

We add the data required for a verification query to the MAC

Dectab	Offset/PVV	original CVV	0 pad
16 digits	4 digits	5 digits	7 digits
Block B1’	Block B2’		

Operation of Scheme

CVV’ is written onto card at issue time

CVV’ is sent along with trial PIN from each ATM transaction

Intermediate switches simply pass along the CVV’

At the verification facility, the supplied CVV’ is checked against the true derived value instead of full MAC

If the CVV’ matches, the query is processed

Otherwise, the query is refused

Evaluation - Advantages

- CVV’ can be calculated in advance

  - can be written to magstripe track 2, just like CVV

- Existing infrastructure already passes track 2 through network

  - no need for costly changes to infrastructure

- Institutions can choose to upgrade individually

  - no need to await standardization

Evaluation - Disadvantages

- Low entropy of MAC allows brute force attack

  - though overhead for PIN cracking attacks considerably increased

- Does not address translation command attacks

  - that would require point to point MACs, bigger overhead

- Change needed to HSM software

  - maybe not a big deal

Evaluation - Disadvantages

- Low entropy of MAC allows brute force attack

  - though overhead for PIN cracking attacks considerably increased

- Does not address translation command attacks

  - that would require point to point MACs, bigger overhead

- Change needed to HSM software

  - maybe not a big deal

Circulated in ANSI X.7

Further Reading

Wired Magazine, *PIN Crackers Nab Holy Grail of Bank Card Security* http://www.wired.com/threatlevel/2009/04/pins/

G. Steel. *Formal analysis of PIN block attacks*. Theoretical Computer Science 367(1-2), 2006.

R. Focardi, F. L. Luccio and G. Steel. *Blunting Differential Attacks on PIN Processing APIs*. In NordSec'09, LNCS 5838.

M. Centenaro, R. Focardi, F. L. Luccio and G. Steel. *Type-based Analysis of PIN Processing APIs*. In ESORICS'09, LNCS 5789

Mohammad Mannan, P.C. van Oorschot. *Reducing threats from flawed security APIs: The banking PIN case*, Computers & Security 28 (6), 2009.