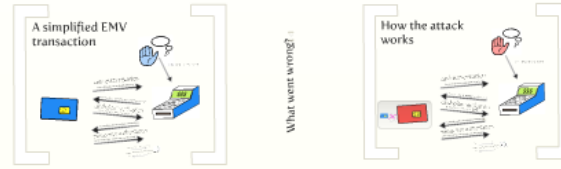


The EMV protocol and its flaws



Chip and PIN is Broken

steven J. murdoch, saar drimer, ross anderson, mike bond

ard company receives a claim about a fraudulent
n from a customer, they will always rely on
vidence to review the facts of the case and would
a paper receipt (which in fact they could only see
omer provided the copy) for evidence as

"Neither the banking industry nor the police have any
vidence of criminals having the capability to deploy such
 sophisticated attacks. Our research suggests that criminal
interest in chip-based attacks is minimal at this time as
there are no real-world reports to make a realistic assessment of
money from any of the plausible attack scenarios."

Responses

stry is confident that the
signature of such an attack
detectable within the data
at the time of the
on."

In addition to the TVR, the card produces a
CVR (card verification results) and the
terminal may optionally produce a CVMR
(cardholder verification method result)

security

- Alters PIN-based authentication, PIN
- enables offline transactions
- Allows card cloning hardware
- enables banking
- enables in person
- enables
- enables

Total fraud in the UK

dip in 2005-2006, but up 35% to €704.3m

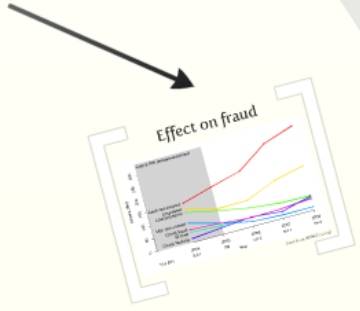
Effect on fraud

EMV

Europay MasterCard Visa

security

- Allows PIN-based authentication, even for offline transactions
- Makes card cloning harder
- does not affect
 - online banking
 - card-not-present
 - checks
 - False applications



EMV

EuroPay MasterCard Visa

EMV is deployed or in planning in most countries except the US, but not even using best practices.

Point-of-sale and ATM Credit and Debit

Smart card based payments

Used on 750m cards, billions of pounds, euros, dollars

Many customers claim that their card has been stolen and used

Banks claim EMV is infallible, so victims do not get their money back



EMV

EuroPay

MasterCard

Visa

EMV is deployed or in planning in most countries
except the US, but vendors are working hard to change this

Point-of-sale and ATM

Credit and Debit

Smart card based payments

Used on 750m cards, billions
of pounds, euros, dollars

Many customers claim that their
card has been stolen and used

Banks claim EMV is infallible, so
victims do not get their money back

44% according to latest figures

Security

*Allows]
even for*

Makes

do not affect

SECURITY

Allows PIN-based authentication,
even for offline transactions



Makes card cloning harder



does not affect

online banking



card-not present



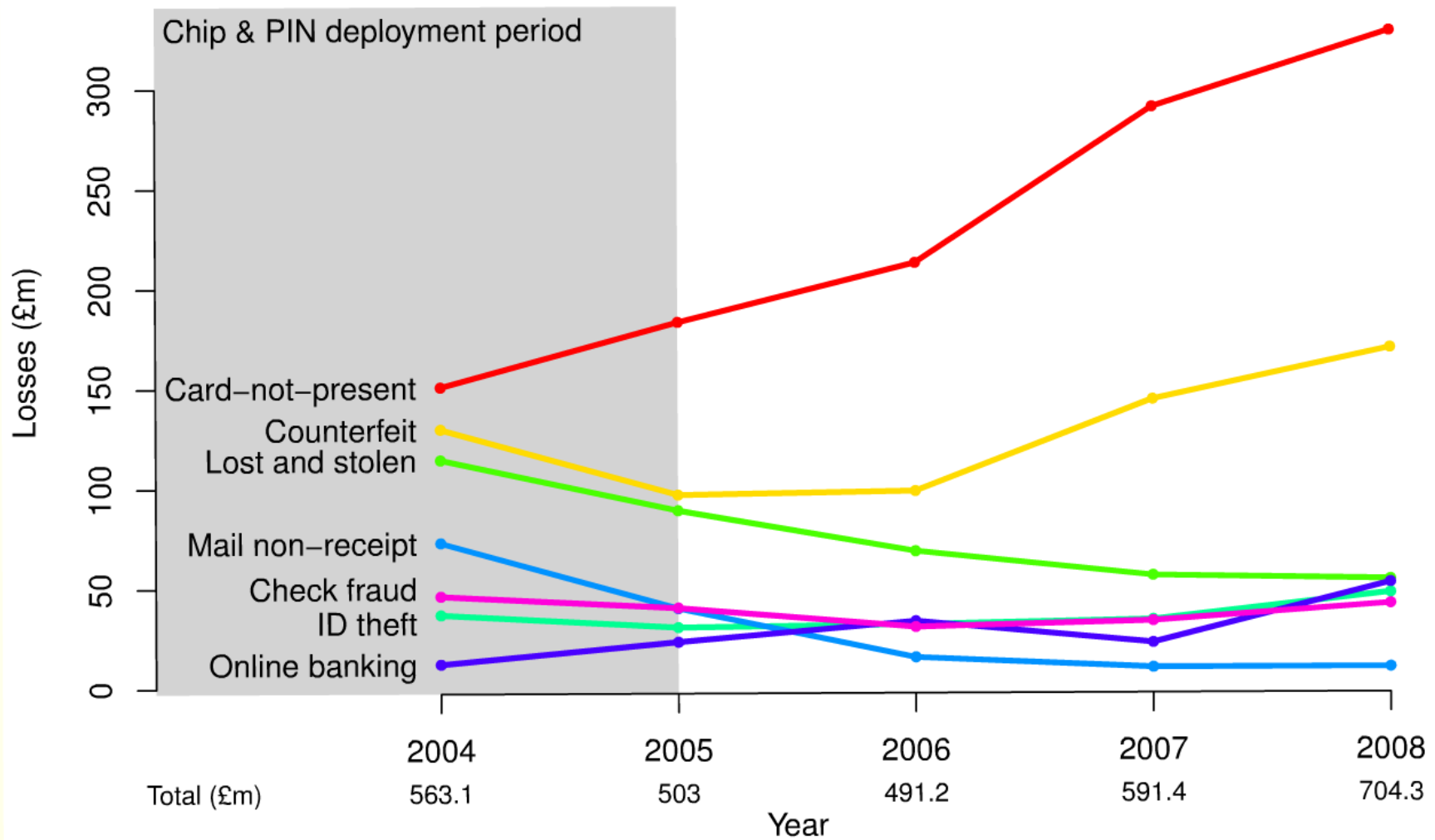
checks



False applications



Effect on fraud



Data from APACS (2009)

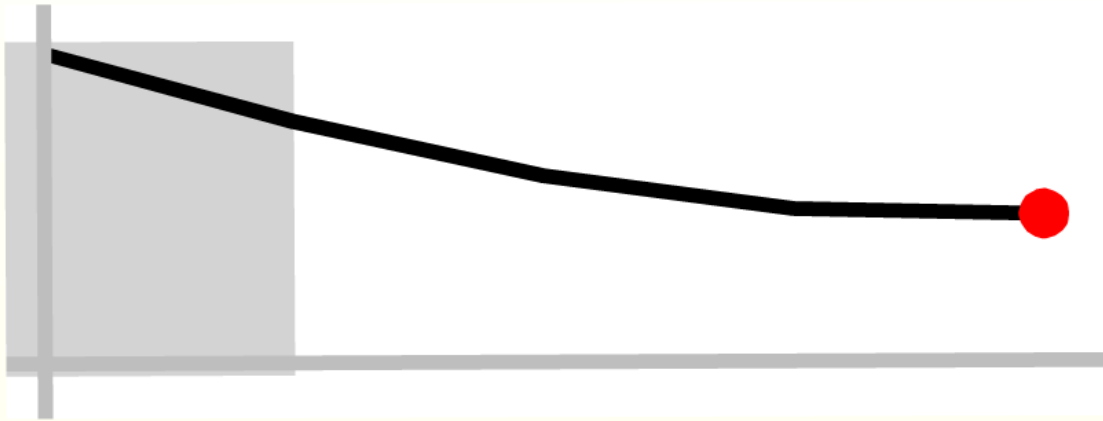
Allows PIN-based authentication,
even for offline transactions



Makes card cloning harder

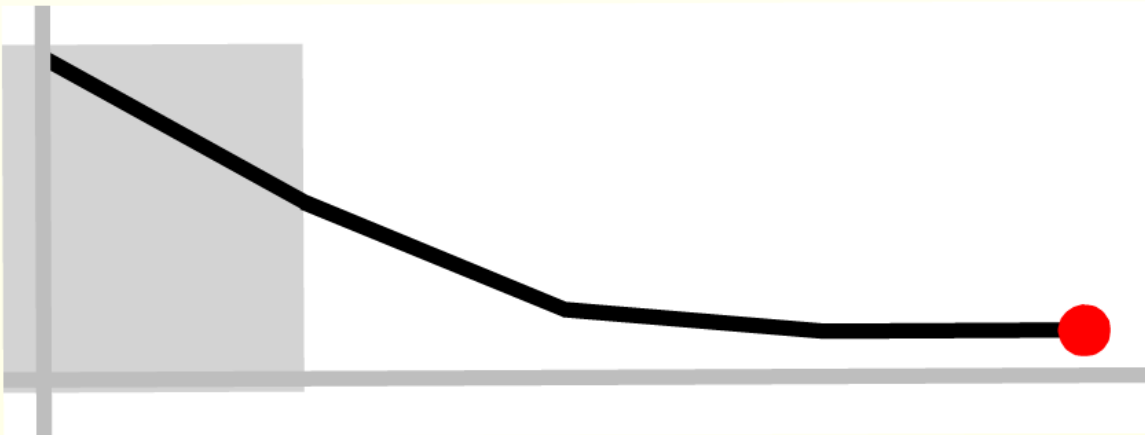


counterfeit
up 31% to £169



Lost and stolen

down 53% to £54.1m



mail non receipt

down 86% to £10.2m

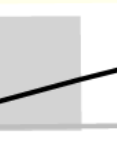
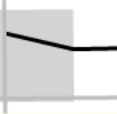
Allows PIN-based authentication
even for offline transactions

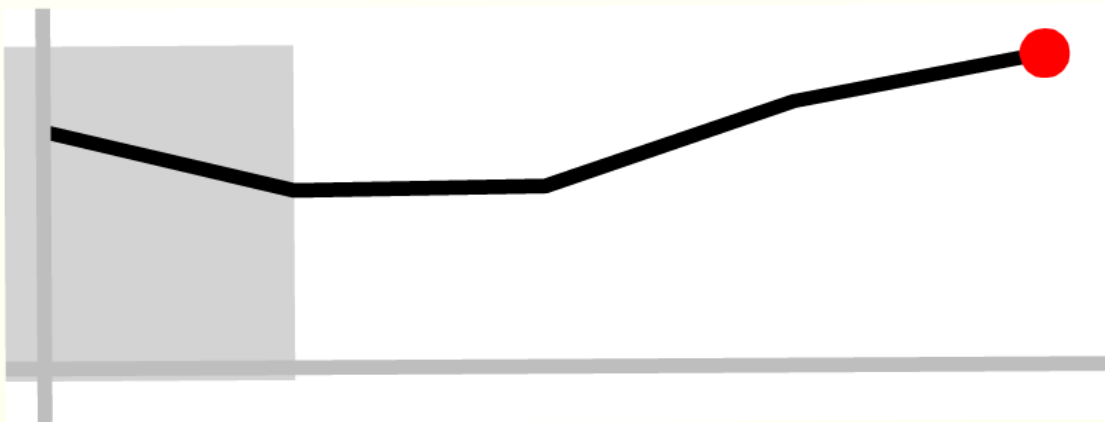
Makes card cloning harder

not affect

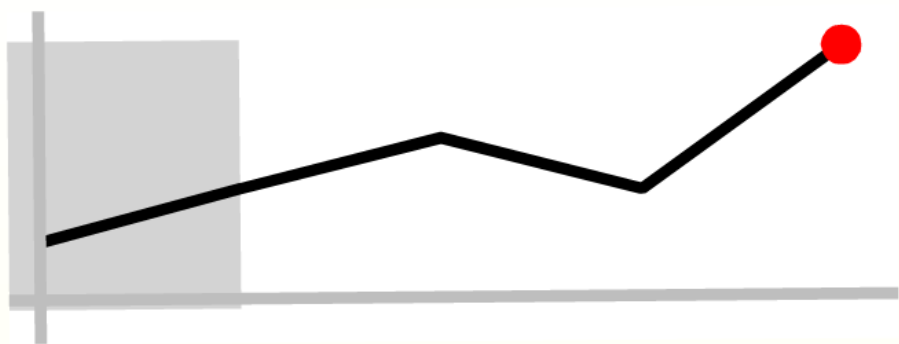
online banking

card-not present

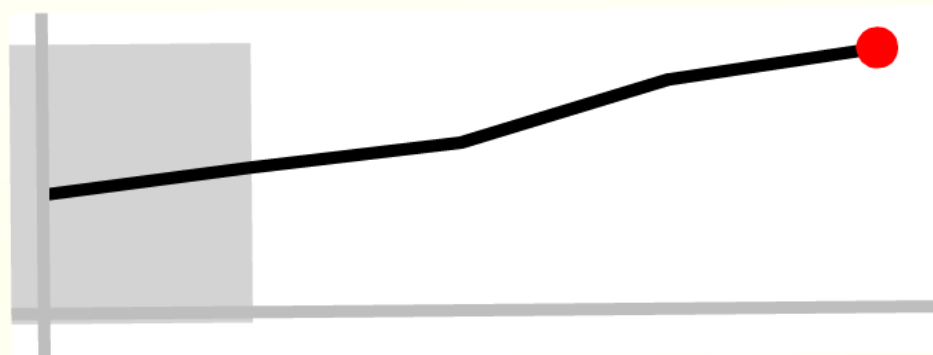




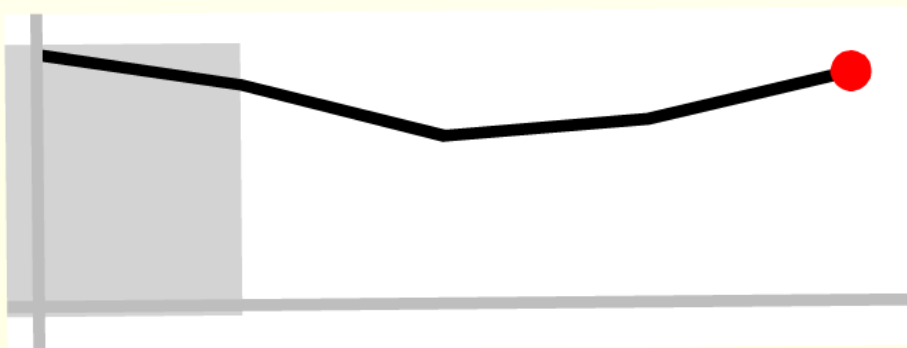
counterfeit
up 31% to £169m



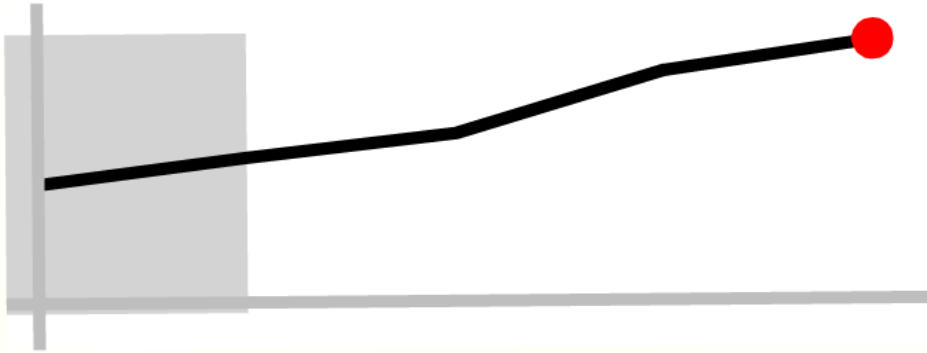
online banking
up 330% to £52.5m



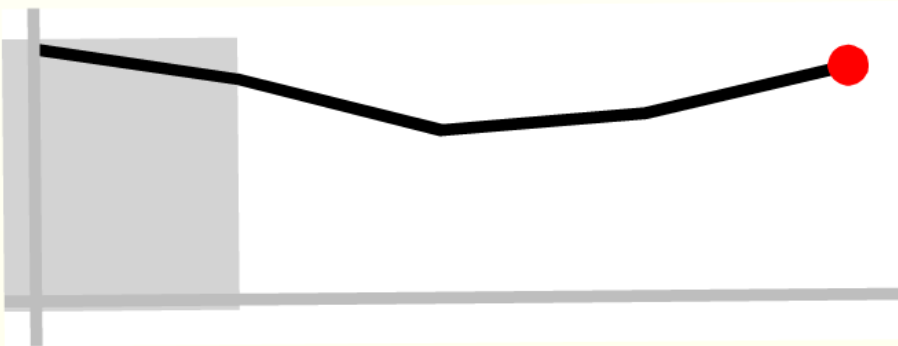
card not present
up 118% to £328.4m



checks
down 9% to £41.9m



card not present
up 118% to £328.4m



checks
down 9% to £41.9m



False applications
up 28% to £47.4m

Total fraud in the UK

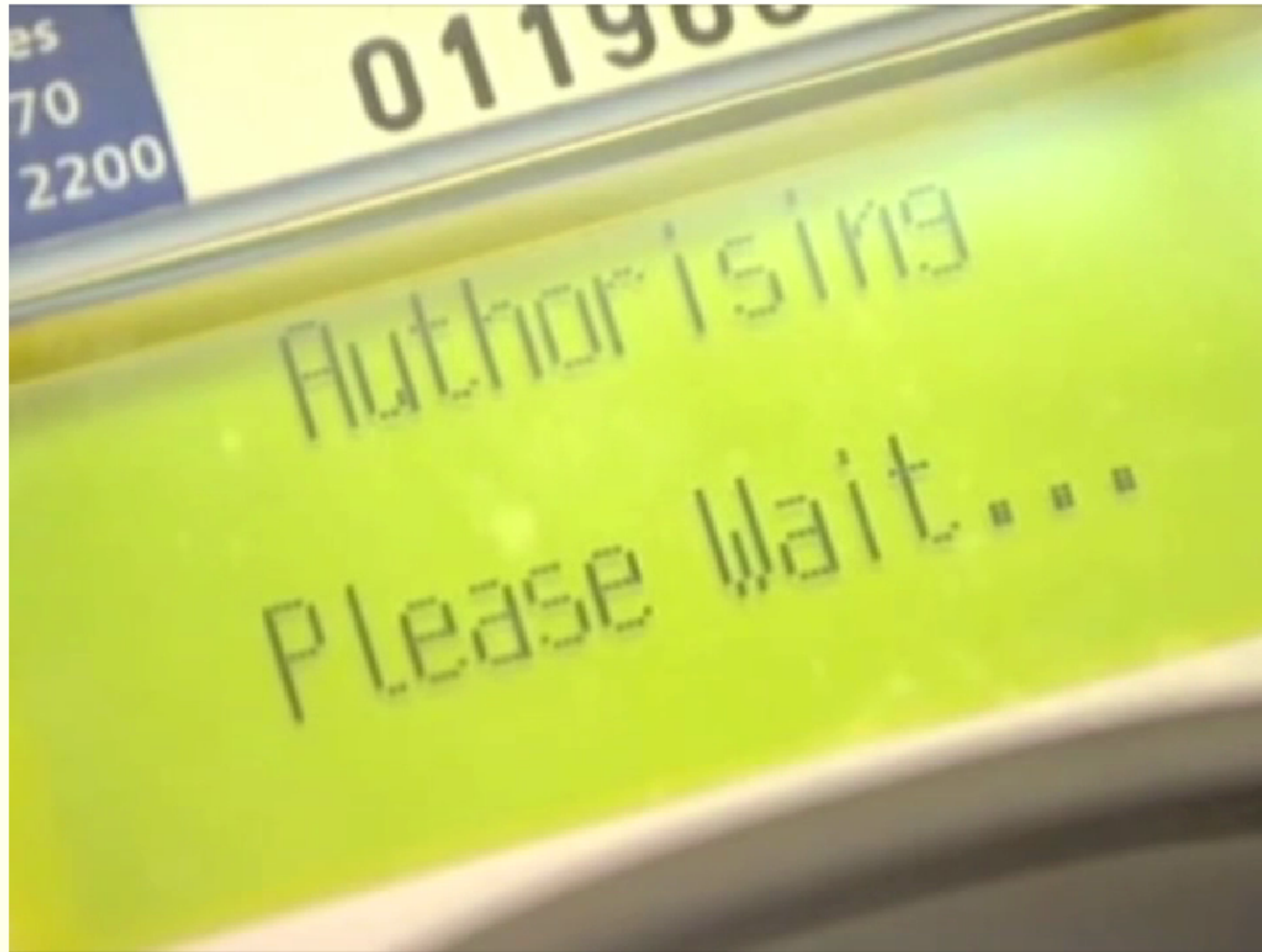


dip in 2005—2006,
but up 25% to £704.3m

Many o
card ha

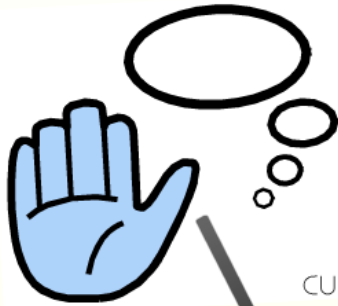
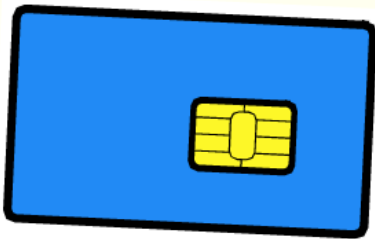
Banks claim EMV is infallible, so
victims do not get their money back
44% according to latest figures

They were wrong



BBC Newsnight, February 2010

A simplified EMV transaction



customer enters PIN



card authentication
Card to Terminal: card details, digital signature

Terminal to Card: PIN as entered by customer

cardholder verification
Card to Terminal: PIN correct (yes/no)

Terminal to Card: description of transaction

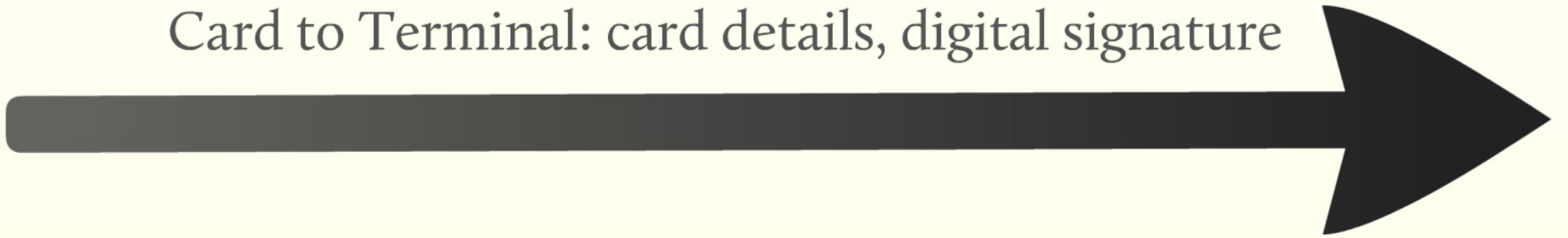
transaction authorization
Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification
online transaction authorization
Bank to Terminal: transaction authorized (yes/no)



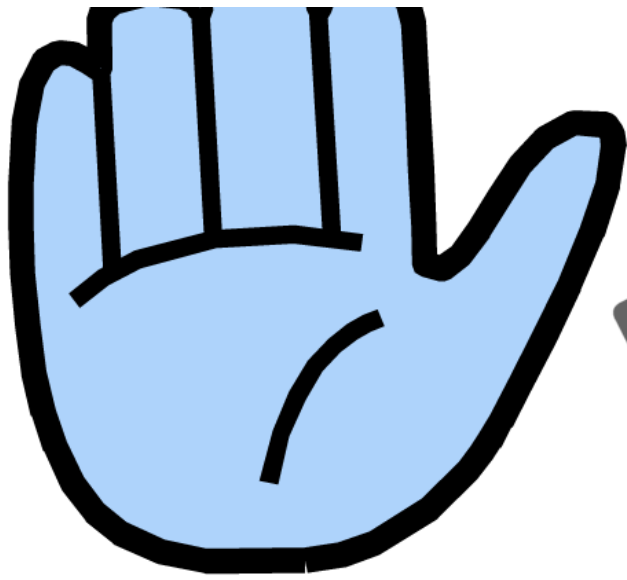
card authentication

Card to Terminal: card details, digital signature

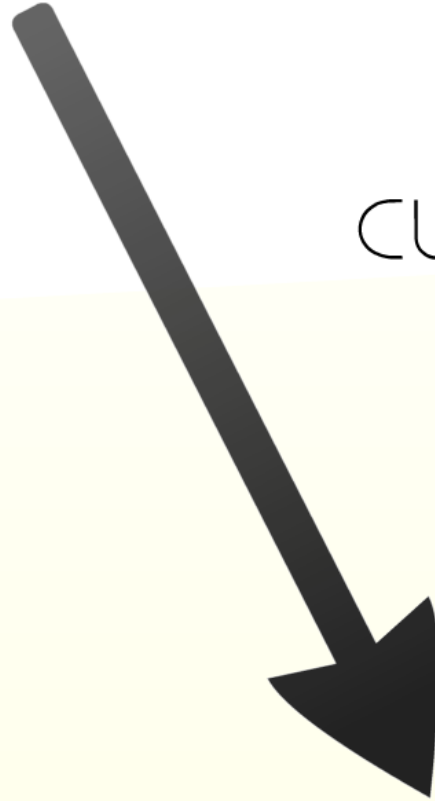


Terminal to Card: PIN as entered by customer

Cardholder



customer enters PIN



Card to Terminal: card details

Terminal to Card: PIN as entered by customer

cardholder verification

Card to Terminal: PIN correct (yes/no)

Terminal to Card: description of transaction
amount, currency, date, nonce, TVR, etc
• did PIN verification fail?
• was PIN required and not entered?
• ...



Terminal to Card: description of transaction

amount, currency, date, nonce, TVR, etc
• did PIN verification fail?
• was PIN required and not entered?
• ...

transaction authorization

Card to Terminal: MAC over transaction and other details




MAC and transaction sent to bank for verification



online transaction authorization

Bank to Terminal: transaction authorized (yes/no)



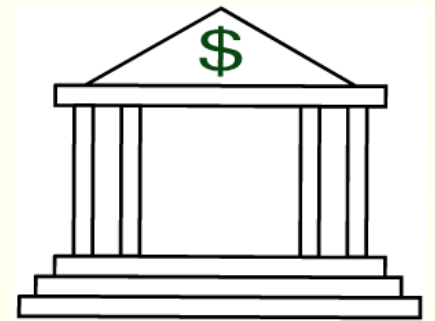
and other details



MAC and transaction sent to bank for verification



online transaction authorization



Bank to Terminal: transaction authorized (yes/no)



What went wrong?

© 2010 Microsoft Corporation. All rights reserved. Microsoft, the Microsoft Dynamics logo, and the Microsoft Dynamics logo are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Microsoft Dynamics is a registered trademark of Microsoft Corporation in the United States and/or other countries.

Microsoft Dynamics is a registered trademark of Microsoft Corporation in the United States and/or other countries.

verification

Card to Terminal: PIN correct (yes/no)

Terminal to Card: description of transaction

amount, currency, date, nonce, TVR, etc
• did PIN verification fail?
• was PIN required and not entered?
• ...

transaction authorization

Card to Terminal: MAC over transaction and other details

MAC and transaction sent to bank for verification

online transaction authorization


Bank to Terminal: transaction authorized (yes/no)





transaction


amount, currency, date, nonce, TVR, etc

- did PIN verification fail?
 - was PIN required and not entered?
 - ...
- 

SACTIONS

date, nonce, TVR, etc

- did PIN verification fail?
- was PIN required and not entered?
- ...



If the PIN is not required by the terminal, the TVR is all zeros
If the PIN is entered correctly, the TVR is still all zeros

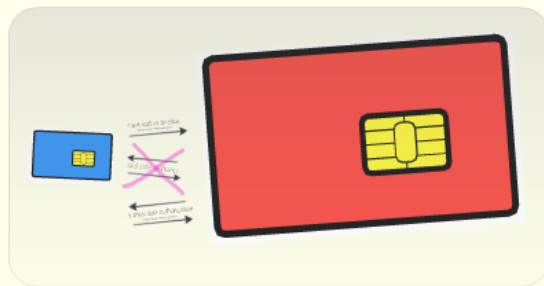
A man-in-the middle tell the card that the PIN was not required
and the terminal that the PIN was correct

Now the criminal can use a stolen card,
give the wrong PIN to the terminal
and still have the transaction succeed

How the attack works



criminal enters 0000



card authentication

Card to Terminal: card details, digital signature

Terminal to MitM: 0000 entered by criminal

cardholder verification

MitM to Terminal: PIN correct **yes!**

Terminal to Card: description of transaction

transaction authorization

Card to Terminal: MAC over transaction and other details

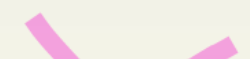
MAC and transaction sent to bank for verification
online transaction authorization

Bank to Terminal: transaction authorized (yes/no)

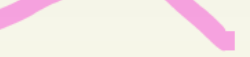




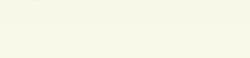
card authentication
Messages relayed without modification



~~cardholder verification~~

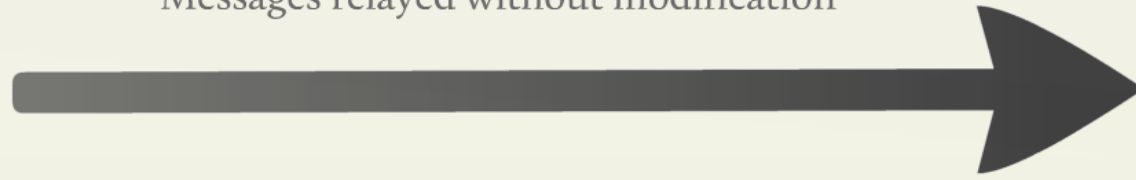


transaction authorization
Messages relayed without modification

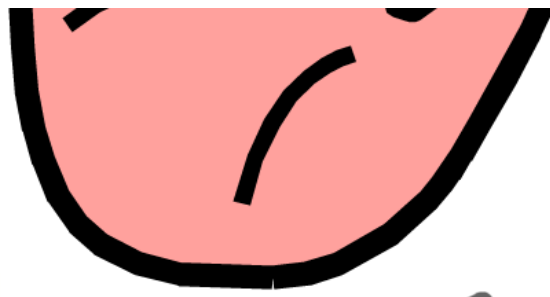


card authentication

Messages relayed without modification



cardholder verifi



criminal enters 0000



Card to Terminal: card details

Terminal to MitM: **0000** entered by criminal

cardholder verification

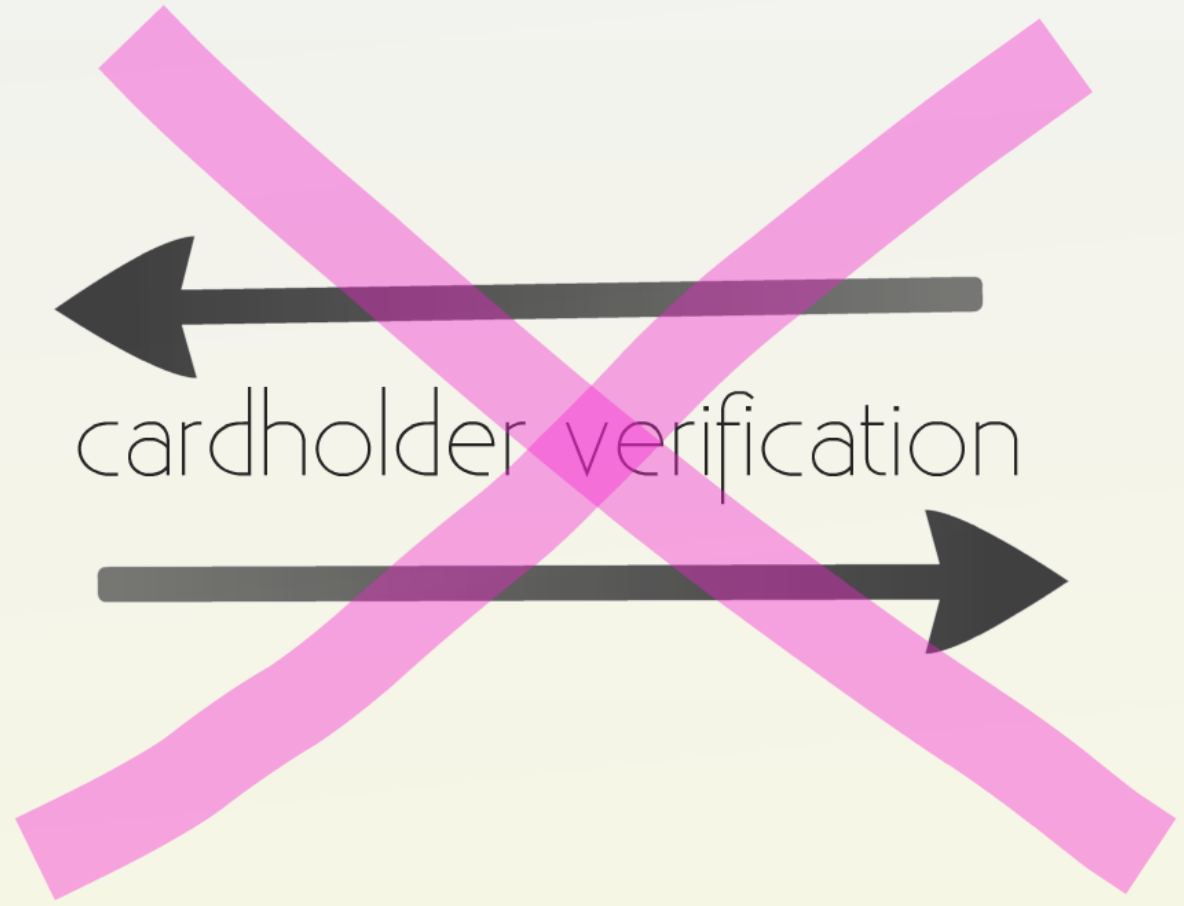
MitM to Terminal: PIN correct **yes!**

Terminal to Card: description of transaction
amount, currency, date, nonce, TVR, etc
did PIN verification fail?
was PIN required and not entered?

Card
Messages relayed without



cardholder verification



transaction authorization

without modification

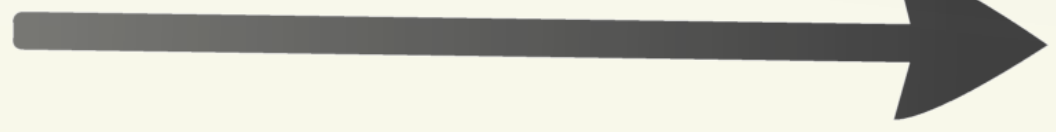


verification



transaction authorization

Messages relayed without modification



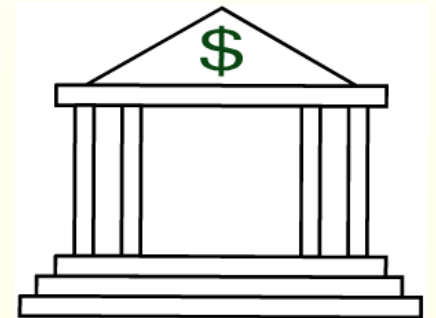
and other details



MAC and transaction sent to bank for verification



online transaction authorization



Bank to Terminal: transaction authorized (yes/no)





Terminal to Card: description of transaction

amount, currency, date, nonce, TVR, etc
• did PIN verification fail?
• was PIN required and not entered?

transaction authorization

Card to Terminal: MAC over transaction and other details




MAC and transaction sent to bank for verification



online transaction authorization

Bank to Terminal: transaction authorized (yes/no)



ACCOUNTS

late, nonce, TVR, etc

- did PIN verification fail?
- was PIN required and not entered?
- ...

Card: No (not attempted)
Terminal: No (verification succeeded)

Card: No
Terminal: No

Card: No (not attempted)

Terminal: No (verification
succeeded)

t entered?

ACCOUNTS

late, nonce, TVR, etc

- did PIN verification fail?
- was PIN required and not entered?
- ...

Card: No (not attempted)
Terminal: No (verification succeeded)

Card: N
Termina

Card: No (not required)

Terminal: No (was entered)

"When a card company receives a claim about a fraudulent transaction from a customer, they will always rely on primary evidence to review the facts of the case and would never use a paper receipt (which in fact they could only see if the customer provided the copy) for evidence as suggested."

"Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks. Our research suggests that criminal interest in chip-based attacks is minimal at this time as they are unable to find ways to make sufficient amounts of money from any of the plausible attack scenarios."

Responses

"The industry is confident that the forensic signature of such an attack is easily detectable within the data available at the time of the transaction."

In addition to the TVR, the card produces a CVR (card verification results) and the terminal may optionally produce a CVMR (cardholder verification method result)

In our attack, the CVR will not match the CVMR

We have shown that the industry's confidence in the forensic signature of such an attack is easily detectable within the data available at the time of the transaction is unfounded. Our research suggests that criminal interest in chip-based attacks is minimal at this time as they are unable to find ways to make sufficient amounts of money from any of the plausible attack scenarios.

"When a card company receives a claim about a fraudulent transaction from a customer, they will always rely on primary evidence to review the facts of the case and would never use a paper receipt (which in fact they could only see if the customer provided the copy) for evidence as suggested."

Response

WRONG



2

We also requested at the time of this claim, supporting documents from [REDACTED] and were provided a copy of the till receipts confirming these charges were verified with the PIN. These receipts also show the products purchase which was for three separate charges of £3000.00, £4000.00 and £2500.00 for currency in Euro's and not for a holiday as thought by [REDACTED] at the time.

Timings and location of these charges are as follows.....

£3000.00 - 20/05/08 - 12.27pm

£4000.00 - 20/05/08 - 12.28pm

£2500.00 - 20/05/08 - 12.30pm

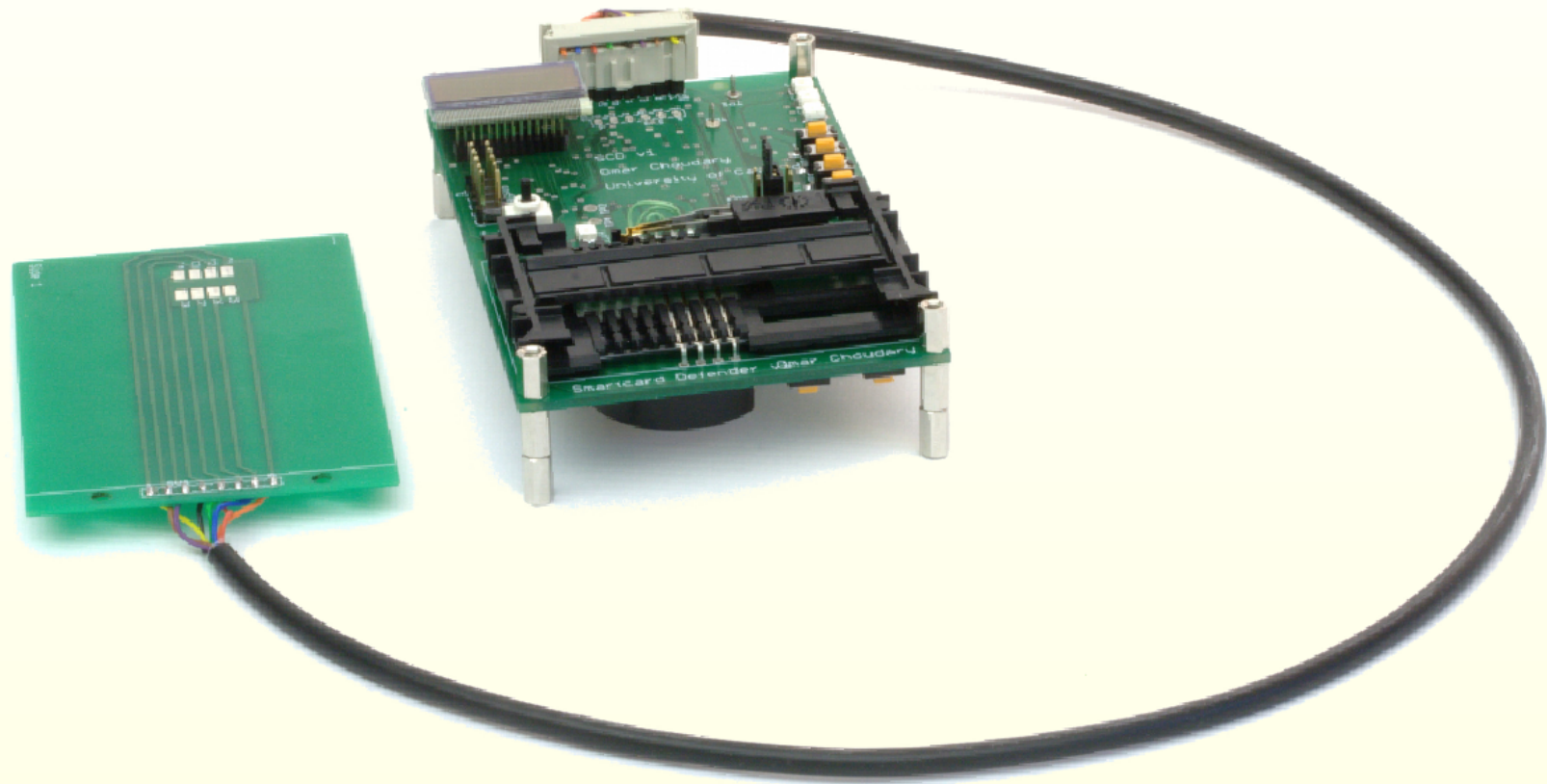
All made at [REDACTED]
[REDACTED]

Unfortunately CCTV was requested for the period of these charges but unfortunately the disk had been recorded over so was/is not available.

"Neither the banking industry nor the police have any evidence of criminals having the capability to deploy such sophisticated attacks. Our research suggests that criminal interest in chip-based attacks is minimal at this time as they are unable to find ways to make sufficient amounts of money from any of the plausible attack scenarios."^[1]



WRONG



"The industry is confident that the forensic signature of such an attack is easily detectable within the data available at the time of the transaction."

WRONG

Below is a list of the dates and times of all transactions performed in [REDACTED] from 23rd July 2009 onwards. I have also included further computerised records for your information:

Date	Amount	Retailer/ATM	Successful/Unsuccessful
24/07	211.66	[REDACTED]	Unsuccessful
24/07	3994.56	[REDACTED]	Successful
24/07	3994.56	[REDACTED]	Successful
24/07	3187.54	[REDACTED]	Unsuccessful
24/07	85.56	[REDACTED]	Unsuccessful

According to our records, all successful transactions were authorised with the genuine card and correct Personal Identification Number (PIN). Therefore, whoever performed these transactions had access to your card and had full knowledge of your PIN. A cloned card was not in operation.

om
our

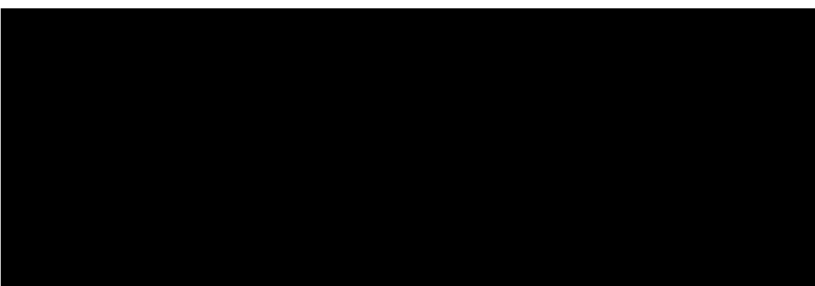


24/07/1980

11:38

KART NO

S.K.T.: 12/10



the
ver
our

EMV : A0000000031010/00A0000000/F800

APP LABEL : VISA DEBIT

000 - ex. entry required, ex. pad present, but ex. was not entered

ORJINAL FISI SAKLAYINIZ.
MUSTERIYE 2. NUSHAYI VERINIZ.

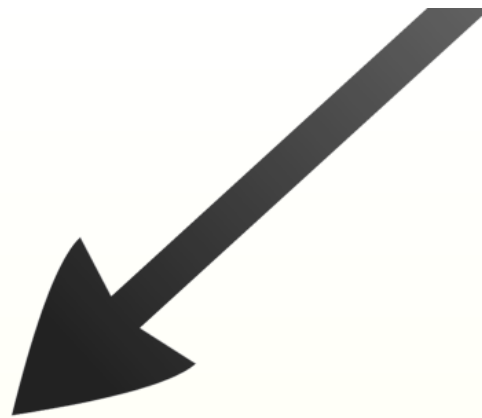
TESEKKURLER

FORTIS 

In addition to the TVR, the card produces a CVR (card verification results) and the terminal may optionally produce a CVMR (cardholder verification method result)



attack, the CVR will not match the CVMR



In our attack, the CVR will not match the CVMR



We hear that the industry are working on a defence based on comparing the CVR and CVMR, but it is not quite that simple:

- Sometimes the CVMR is not produced by the terminal (it is optional)
- Sometimes it is produced but wrong (it has not been considered useful, until now)
- Sometimes it is produced but dropped or corrupted on the way back

Many o
card ha

Banks claim EMV is infallible, so
victims do not get their money back
44% according to latest figures

The EMV protocol and its flaws



Chip and PIN is Broken

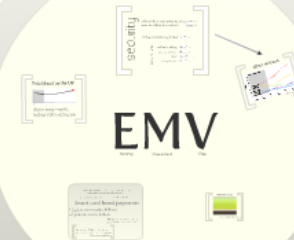
steven J. murdoch, saar drimer, ross anderson, mike bond

Responses

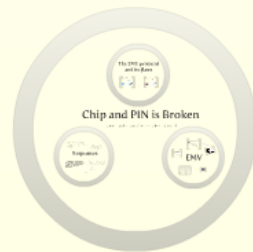
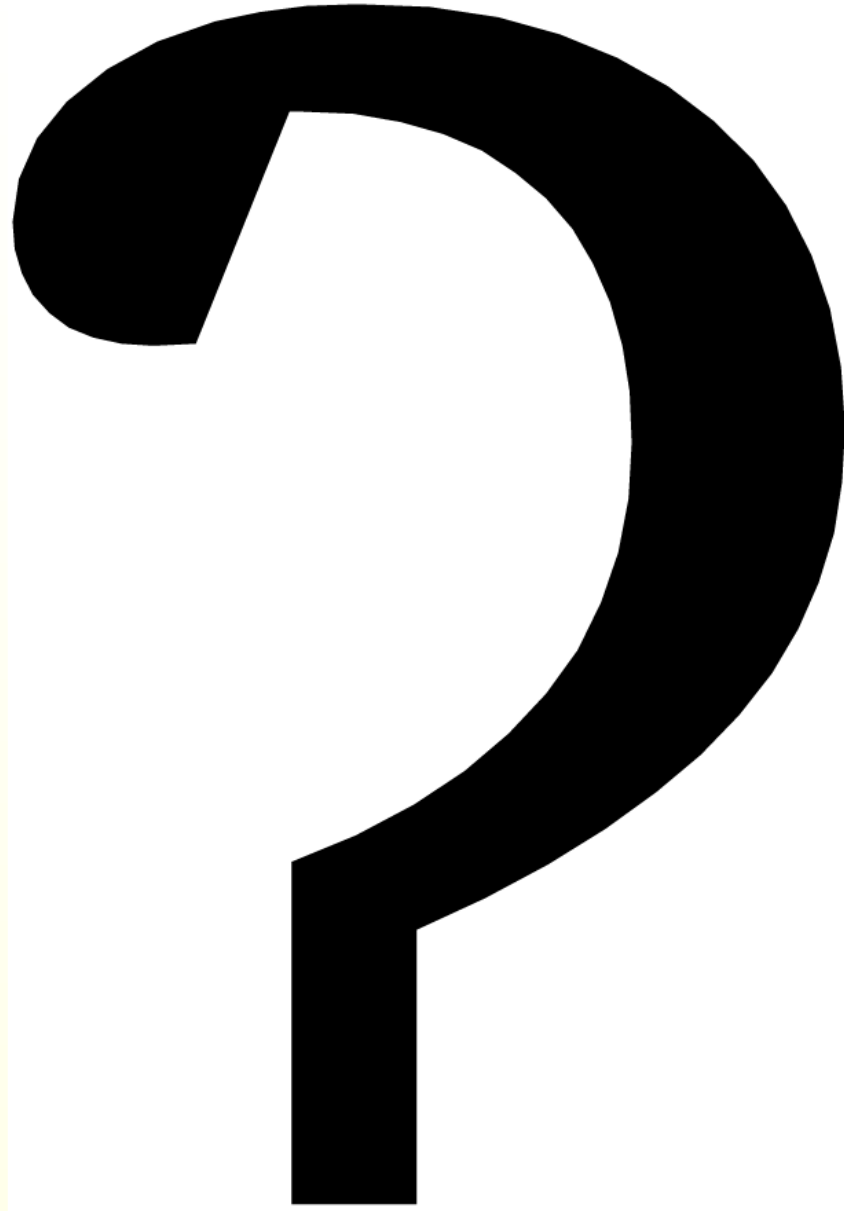
"When a card is given to a merchant, the merchant is responsible for ensuring that the card is not used for any other purpose than the one for which it was issued. This is a responsibility that the merchant should not pass on to the cardholder."

"The industry is confident that the forensic signatures of such an attack is easily detectable within the data available at the time of the transaction."

"In addition to the PIN, the cardholder's CVV2 is also used for authentication. This is a security measure that is not used in other payment systems."



Cloud



How is ATM fraud
happening

