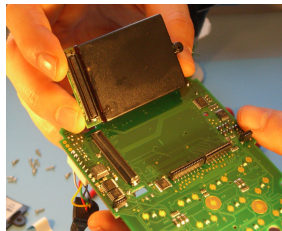
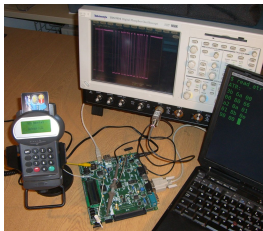


# Chip & PIN 5 years on



Steven J. Murdoch

<http://www.cl.cam.ac.uk/users/sjm217/>

work with Saar Drimer, Ross Anderson, Mike Bond



UNIVERSITY OF  
CAMBRIDGE

Computer Laboratory



[www.torproject.org](http://www.torproject.org)

## Chip & PIN has now been running in the UK for about 5 years

- Chip & PIN, based on the EMV (EuroPay, MasterCard, Visa) standard, is deployed throughout most of Europe
- In process of roll-out elsewhere
- Customer inserts contact-smartcard at point of sale, and enters their PIN
- UK was an early adopter: rollout in 2003–2005; mandatory in 2006
- Chip & PIN changed many things, although not quite what people expected



Chip and PIN

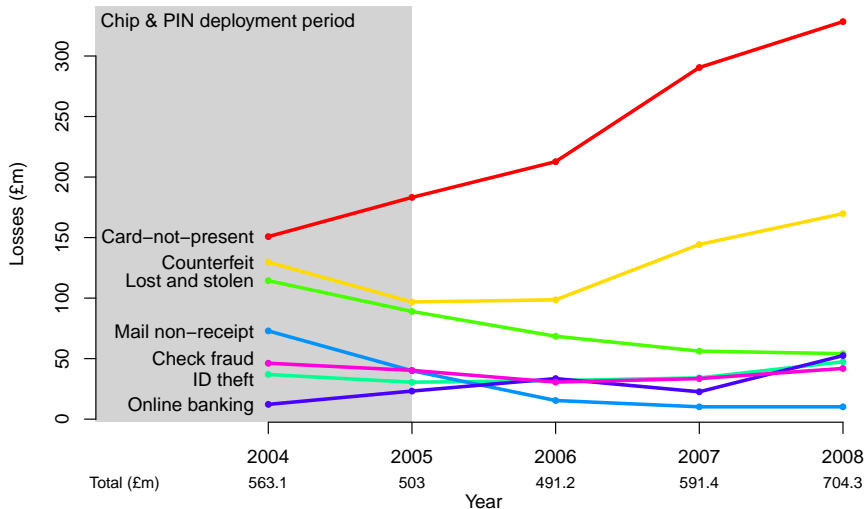


## Card payments in the UK are different from the US (and elsewhere)

	<b>Before Chip &amp; PIN</b>	<b>After Chip &amp; PIN</b>
<b>Cards</b>	magstrip	magstrip and chip
<b>Card verification</b>	magstrip	chip if possible
<b>ATM</b>	PIN used	PIN used
<b>Point-of-sale</b>	signature used	PIN used


- No difference between credit and debit cards
- No ID check at point-of-sale (signature rarely checked either)
- Introducing Chip & PIN really made two changes:
  - Chip used for authenticating card (ATM and PoS)
  - PIN used for authenticating customer (only new for PoS)
- The effects of the two changes are often conflated


# UK fraud figures 2004–2008




## Key trends 2004–2008


- Abuse of authentic cards:

- Lost and stolen: **down** 53%  to £54.1m

- Mail non-receipt: **down** 86%  to £10.2m

- Counterfeit: **up** 31%  to £169.8m

- Non-card security:

- Card-not-present: **up** 118%  to £328.4m

- ID theft: **up** 28%  to £47.4m

- Online: **up** 330%  to £52.5m

- Check: **down** 9%  to £41.9m

- Total:** dip in 2005–2006, but **up** 25%  to £704.3m

## Counterfeit fraud mainly exploited backwards compatibility features

- Upgrading to Chip & PIN was too complex and expensive to complete in one step
- Instead, chip cards continued to have a magstrip
  - Used in terminals without functioning chip readers (e.g. abroad)
  - Act as a backup if the chip failed
- Chip also contained a full copy of the magstrip
  - Simplifies issuer upgrade
  - Chip transactions can be processed by systems designed to process magstrip
- Criminals changed their tactics to exploit these features, and so counterfeit fraud did not fall as hoped
- Fraud against UK cardholders moved outside of the UK

# Criminals could now get cash

Criminals collected:

- card details by a “double-swipe”, or tapping the terminal/phone line
- PIN by setting up a camera, tapping the terminal, or just watching

Cloned magstrip card then used in an ATM (typically abroad)

In some ways, Chip & PIN made the situation worse

- PINs are used much more often (not just ATM)
- PoS terminals are harder to secure than an ATM



Tonight (ITV, 2007-05-04)

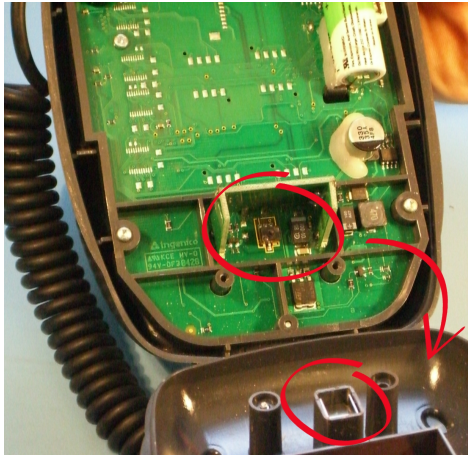
## Terminal tamper proofing is supposed to protect the PIN in transit

- In PoS transaction, PIN is sent from PIN entry device (PED) to card for verification
- Various standard bodies require that PEDs be tamper proofed: Visa, EMV, PCI (Payment Card Industry), APACS (UK bank industry body)
- Evaluations are performed to well-established standards (Common Criteria)
- Visa requirement states that defeating tamper-detection would take more than 10 hours or cost over **USD \$25,000 per PED**



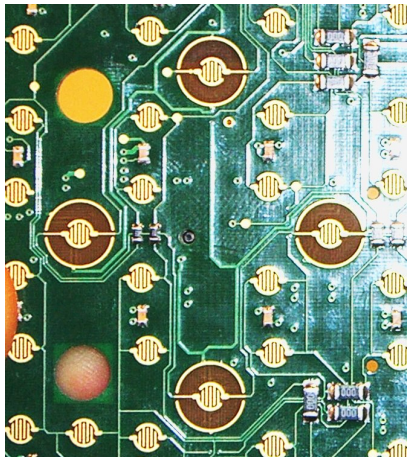
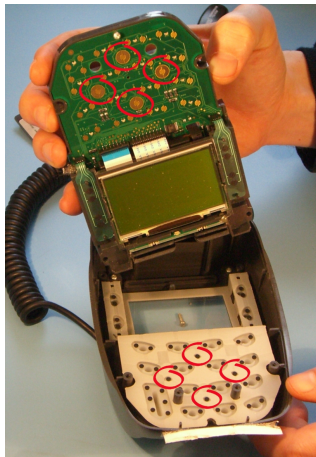


## Protection measures: tamper switches



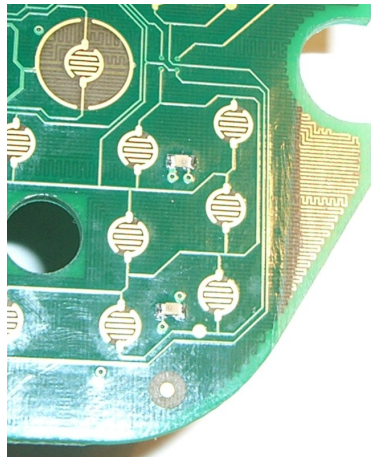
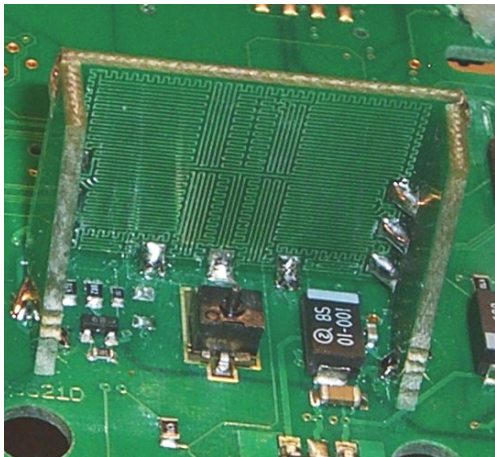
Ingenico i3300

## Protection measures: tamper switches



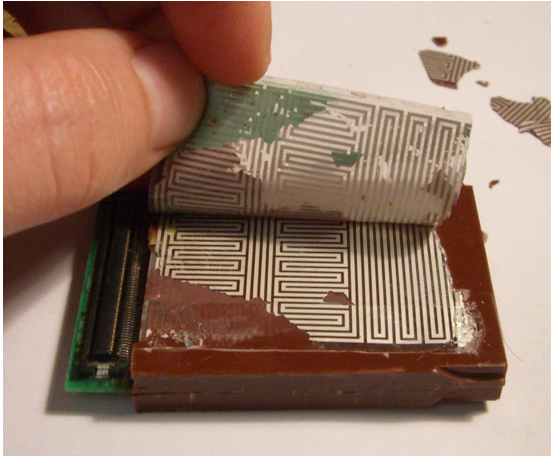
Ingenico i3300

## Protection measures: tamper meshes



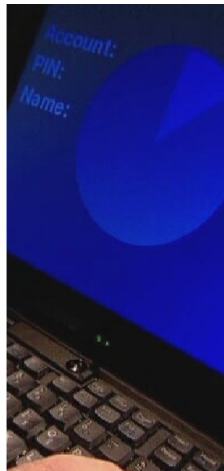
Ingenico i3300

## Protection measures: tamper meshes



Ingenico i3300

## BBC Newsnight filmed our demonstration for national TV



BBC Newsnight, BBC2, 26 February 2008

Holes in the tamper mesh allow the communication line to be tapped



An easily accessible compartment can hide a recording device

## This type of fraud is still a serious problem in the UK

Initially (2005), PEDs were tampered on a small scale and installed by someone impersonating a service engineer

PED was collected later, and card details extracted

Now PEDs are being tampered with at or near their point of manufacture

A cellphone module is inserted so it can send back lists of card numbers and PINs automatically

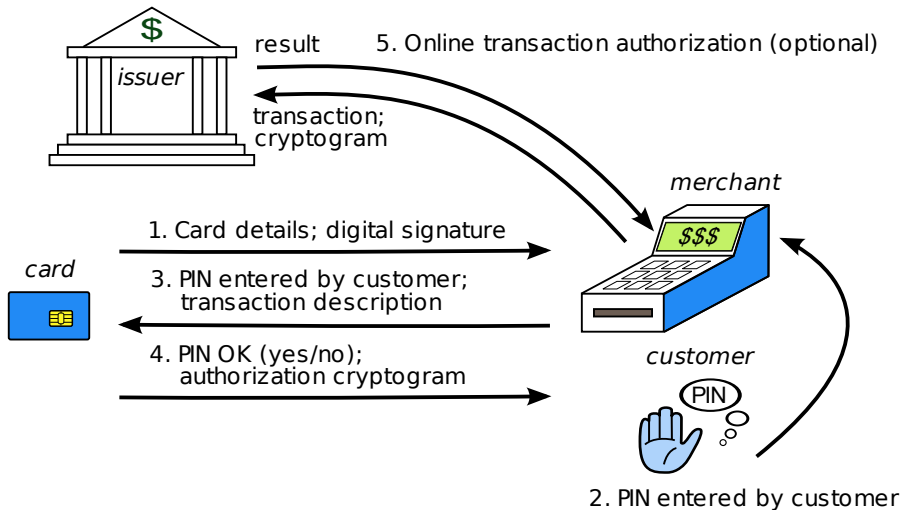


## Chip & PIN vulnerabilities

- Fallback vulnerabilities are not strictly-speaking a Chip & PIN vulnerability
- However, vulnerabilities do exist with Chip & PIN
- To understand these, we need some more background information
- To pay, the customer inserts their smart card into a payment terminal
- The chip and terminal exchange information, fulfilling three goals:
  - **Card authentication:** that the card presented is genuine
  - **Cardholder verification:** that the customer presenting the card is the authorized cardholder
  - **Transaction authorization:** that the issuing bank accepts the transaction

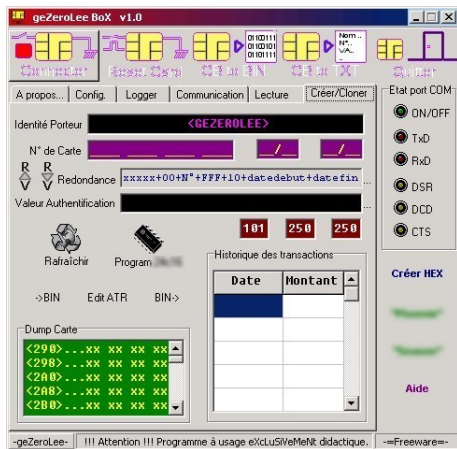


# Simplified Chip & PIN transaction

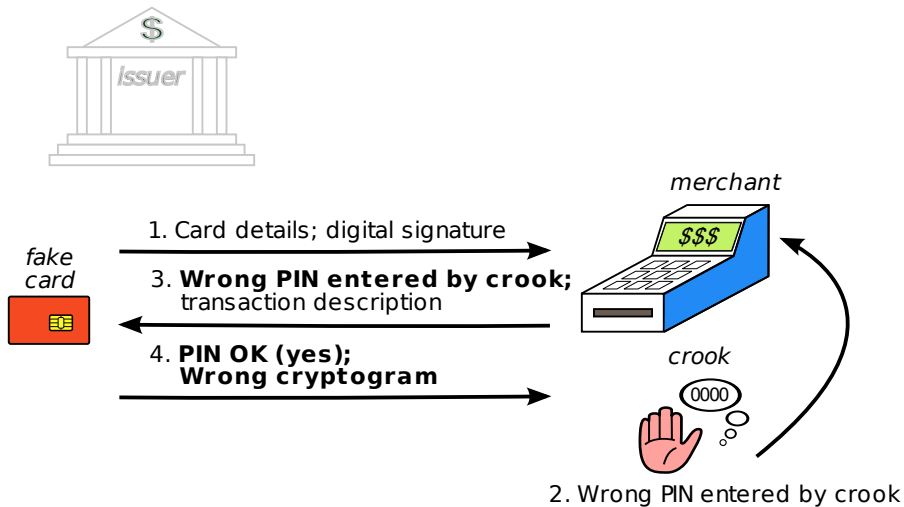


# The YES-card attack

- Criminals can copy EMV chip cards
- This fake card will contain the correct digital signature
- Also, it can be programmed to accept any PIN (hence “YES”)
- However, the fake card can be detected by online transaction authorization



# The YES-card attack

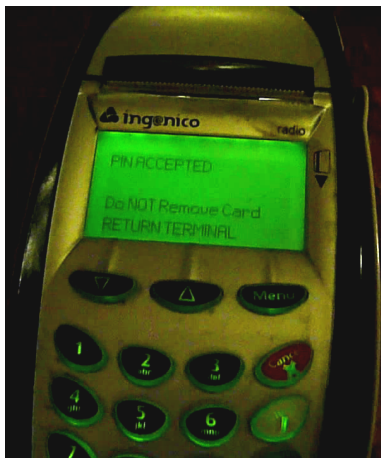


## Defending against the YES-card

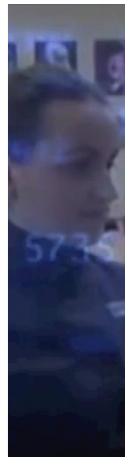
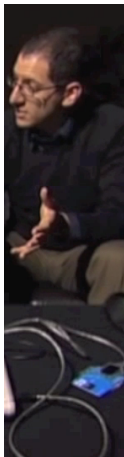
- YES-cards are responsible for a relatively small amount of fraud
- Can be detected by **online** transaction authorization
- Can also be detected by more advanced chip cards which can produce a dynamic digital signature
  - **DDA** (dynamic data authentication), as opposed to **SDA** (static data authentication)
  - Previously DDA cards were prohibitively expensive, but now cost about the same as SDA cards
- PIN verification can be performed online too, rather than allowing the card to do so
  - Need to securely send the PIN back to the issuer
  - UK ATMs use **online** PIN verification
  - UK point-of-sale terminals use **offline** PIN verification

## The no-PIN attack

- The no-PIN attack allows criminals to use a stolen card without knowing its PIN
- It requires inserting a device between the genuine card and payment terminal
- This attack works even for **online** transactions, and **DDA** cards

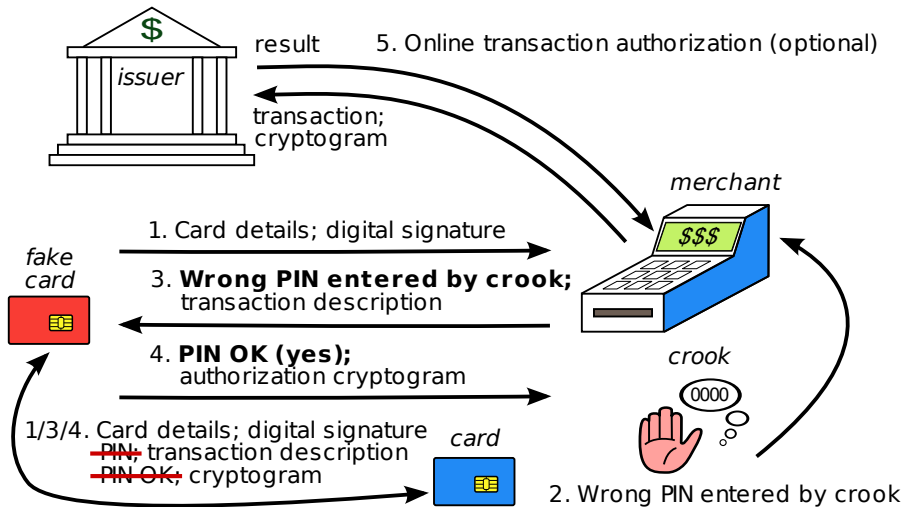


## BBC Newsnight filmed our demonstration for national TV



BBC Newsnight, BBC2, 11 February 2010

# The no-PIN attack



## Current and proposed defences

- Skimming
  - iCVV: Slightly modifying copy of magnetic strip stored on chip
  - Disabling fallback: Preventing magnetic strip cards from being used in EMV-enabled terminals
  - Better control of terminals: Prevent skimmers from being installed
- YES-card
  - Dynamic Data Authentication (DDA): Place a public/private keypair on every card
  - Online authorization: Require that all transactions occur online
- No-PIN attack
  - Defences currently still being worked on
  - Extra consistency checks at issuer may be able to spot the attack
  - Combined DDA/Application Cryptogram Generation (CDA): Move public key authentication stage to the end



## Deployment of Chip and PIN

- Chip and PIN was expensive for both all parties
- Deployment was encouraged through “liability engineering”

Card	Terminal		
	magstrip	chip	chip & PIN
magstrip	Issuer	Issuer	Issuer
chip	Acquirer	Issuer	Issuer
chip & PIN	Acquirer	Acquirer	Issuer

- Liability pushed down the chain: acquirer → merchant; issuer → customer
- Led to rapid deployment, but this caused some problems
- Still took 10 years

## System glitches

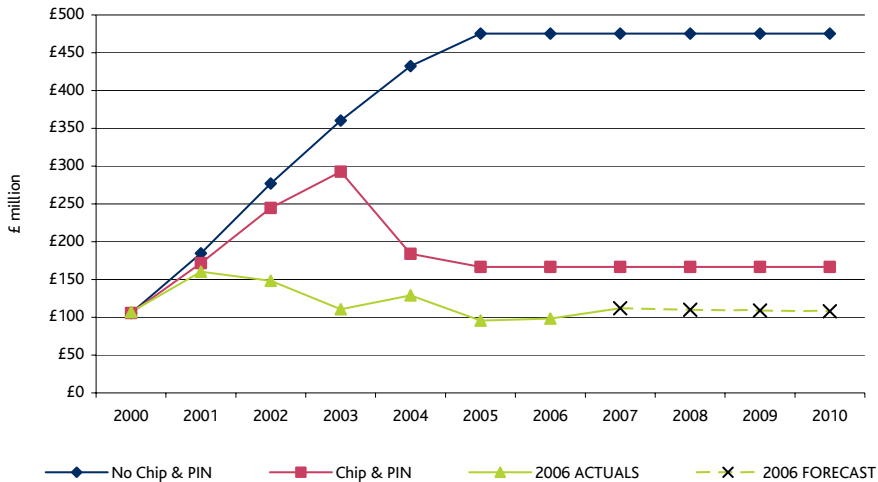
- EMV is extremely complicated
- Difficult to make it work at all, let alone secure
- There have been many small glitches and incompatibilities
- A large one was when 20m German “EC” cards from Gemalto stopped working on January 1, 2010
- Fortunately, the magstrip still was on cards and could be used until a fix was found



## Was Chip and PIN worthwhile?

- Deploying Chip and PIN in the UK cost £1–2 billion
- Was it worth it?
- Fraud went up
- But maybe, had Chip and PIN not been deployed, fraud would have gone up much more
- UK banks consider Chip and PIN a success
- We can never be certain whether they are correct
- Fraud figures are not the whole story: reduced value of stolen cards likely reduced violent crime

# Counterfeit fraud in the UK



Source: UK Chip & PIN report (2007), APACS

## Effect on consumers

- There was some minor resistance to Chip and PIN
- After deployment, the question of liability became important
- Before Chip and PIN, banks generally refunded victims of fraud, because it was well known that magstrip cards could be cloned and signature forged
- After Chip and PIN, banks took the position that if the chip and PIN were used, the customer must have been negligent and hence liable (level of proof is low)
- The industry does not keep statistics, but a survey from the Consumer Association found that 20% of fraud victims do not get their money bank
- UK costs rules and regulatory regime makes fixing this difficult

## Options for deploying EMV in the US

- Do nothing: stay with magstrip cards
- Use full EMV suite
  - Complex, but has been done before
  - Would be prudent to avoid same mistakes (use iCVV, fix no-PIN vulnerability, use CDA or force online operation)
- Use simple EMV subset
  - Drop offline operation (massively simplifies system, avoids cost of building and running a PKI)
  - Dealing with the PIN is a more difficult choice
- Build something new
  - Use modern design principles and experience to build a better system (EMV is over 15 years old)
  - Probably more expensive in short term, but cheaper eventually

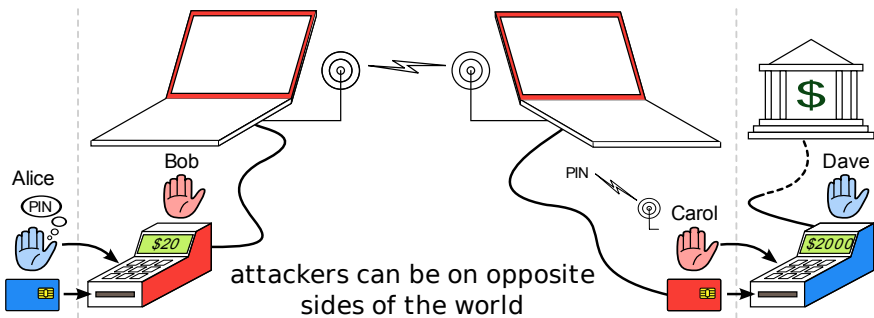
More: <http://www.cl.cam.ac.uk/research/security/banking/>

The relay attack: Alice thinks she is paying \$20, but is actually charged \$2 000 for a purchase elsewhere



Honest cardholder Alice and merchant Dave are unwitting participants in the relay attack

## The relay attack: Alice thinks she is paying \$20, but is actually charged \$2 000 for a purchase elsewhere



Alice inserts her card into Bob's *fake* terminal, while Carol inserts a fake card into Dave's *real* terminal. Using wireless communication the \$2 000 purchase is debited from Alice's account