

# Not-so-smart cards and not such close proximity: the cost of a cashless society

Denis A Nicole

# Abstract

"A not very technical review of the vulnerabilities of the current mainstream technologies driving the cashless society. Scissors<sup>†</sup> will be provided if you decide to cut up your cards here and now. Almost no new research will be presented."

† The ISO14443 standard says that you can disable a proximity card by cutting to where the Chip *would* be if it were a Chip & PIN...

# Scope

Practical attacks on the two most popular eMoney systems:

- CHIP & PIN
  - ISO14443/mifare: Oyster, Passports etc.
- ...with lots of thanks to Ross Anderson's group at Cambridge:

<http://www.lightbluetouchpaper.org>

# CHIP & PIN

## Background:

- It's hard to clone a chip
- It's easy to clone a magstripe
- Currently, most fraud is claimed to be of the *Card not Present* type, eg the innocent victims of *Operation Ore*—there is more than your money at stake.
- There are also a lot of foreign ATM transactions.

## No evidence against man in child porn inquiry who 'killed himself'

By Ian Herbert

Published: 01 October 2005

The [credibility of a major investigation](#) into child pornography came under renewed scrutiny yesterday after an inquest into the death of a naval officer who was suspended by the Royal Navy despite a lack of evidence against him.

The Navy suspended Commodore David White, commander of British forces in Gibraltar, after police placed him under investigation over allegations that he bought pornographic images from a website in the US. Within 24 hours he was found dead at the bottom of the swimming pool at his home in Mount Barbary.

The inquest into his death heard that computer equipment and a camera memory chip belonging to Commodore White had yielded no evidence that he downloaded child pornography, and a letter was written by Ministry of Defence police to Naval Command on 5 January this year indicating that there were "no substantive criminal offences" to warrant pressing charges. But the Second Sea Lord, Sir James Burnell-Nugent, feared that the media would report the case and on 7 January removed him from his post anyway.

Despite accepting the news in a "steady fashion", the commodore was dead the next day. His brother Rupert told the inquest that the news of his removal had caused his "mental collapse", and that he was in "a state of catatonic shock".

Of course, if you're not driven to suicide your [neighbours might kill you](#) when your identity is leaked.

# CHIP & PIN: Fundamental problems

- Multiple protocols: Chip, magstripe, CVV2
- Man in the middle
- Short PINs, entered in public

# Credit card protocols 1: CVV2

- Account + CVV2, used for *card not present*: easily skimmed by the dumbest crook.

Why is the CVV2 printed on the card?

- *card not present* is not a problem for the Banks. If you don't notice, they keep the 2%<sup>†</sup>; if you do, they *charge back* from the business and charge it another<sup>‡</sup> fee.

† <http://www.actinicexpress.co.uk/overview/online-payment-services.htm>

‡ *Fraud Frenzy*, Tonight with Trevor M<sup>c</sup>Donald, 2007-05-04

# And you have no recourse



thisislondon.co.uk  
the entertainment guide

from the  
Evening  
Standard

LONDON  
**Lite**

## **Fraud victims told: Go to the bank, NOT the police**

30.03.07

Victim of fraud: Don't bother reporting it to the police

Hundreds of thousands of people who fall victim to credit or debit card fraud have been told to no longer bother reporting it the police.

From Sunday a change in the law, which has been approved by the Home Office, means victims should go to their bank rather than the police station.

The move has been condemned as "astounding" by security experts who suggest it amounts to the privatisation of the justice system.

They say it appears an attempt by the Government, the police and the banks to push the crime, which costs the nation £428 million a year, under the carpet.

The changes are contained in the small print of the 2006 Fraud Act, which comes into force on April 1 - April Fools' Day.

<http://www.thisislondon.co.uk/news/article-23390837-details/Fraud%20victims%20told:%20Go%20to%20the%20bank,%20NOT%20the%20police/article.do>



# Credit card protocols 2: Magstripe

There are three tracks on the magstripe. Each track is .110-inch wide. The ISO/IEC standard 7811, which is used by banks, specifies:

- Track one is 210 bits per inch (bpi), and holds 79 six-bit plus parity bit read-only characters.
- Track two is 75 bpi, and holds 40 four-bit plus parity bit characters.
- Track three is 210 bpi, and holds 107 four-bit plus parity bit characters. Most cheap readers do not read this track.

Easy for all to read and write: my unit cost £5.

**Throw away everything you thought you knew about credit card readers.** You've found the IntelliSwipe CC -- the smart, easy-to-use credit card reader that anyone can use. Just plug it into any USB port and swipe a card, and the information will be typed into any application as if entered on the keyboard, in the format you specify (we offer a few different output formats you can choose when ordering).



# Track 1

- Start sentinel="%" -- 1 character
- Format code="B" -- 1 character (alpha only)
- Primary account number -- up to 19 characters
- Separator="^" -- 1 character
- Country code="826" -- 3 characters
- Name -- 2-26 characters
- Separator="^" -- 1 character
- Expiration date -- 4 characters or 1 character
- Discretionary data -- enough characters to fill out maximum record length (79 characters total), this includes the CVV1
- End sentinel="?" -- 1 character
- Longitudinal Redundancy Check -- 1 character

<http://www.gae.ucm.es/~padilla/extrawork/tracks.html>

The PIN offset is on tracks 2 and 3.

# And easy to rip off

- UK ATMs continued to use mag stripe after retailers were “forced”<sup>†</sup> to switch to Chip & PIN.
- Many current systems will fall back to the stripe if the Chip has failed.
- Foreign ATMs still use the stripe.
- Stripe data can be reconstructed from open data on the Chip.

Why does the mag stripe have the same PIN as the Chip?

† On Valentine’s day 2006 responsibility for fraudulent transactions was transferred to the merchants if they didn’t have Chip & PIN.

# Grabbing a PIN

- PINs used to be used only in the “controlled” environment of an ATM.
- Most shop readers are overlooked by PoS CCTV.
- It’s almost impossible to conceal button presses as keypads differ between machines. They’re also starting to wear out, so you need to be able to see the screen while *concealing* the keypad.

Why no standard key shapes?

# PIN machine in the middle

- The machines are tamper evident *to the Bank*, not to *you*.
- Buy one on Ebay



The screenshot shows an eBay listing for a Verifone Omni 3750 Chip Pin credit card PDQ POS terminal. The listing includes a navigation bar with links for home, pay, register, sign in, and site map, along with buttons for Buy, Sell, My eBay, Community, and Help. The item title is "Verifone Omni 3750 Chip Pin credit card PDQ POS". The current bid is £40.00, with 7 bids and a high bidder of mas5252 (92 stars). The end time is 8 hours 50 mins (09-May-07 20:46:33 BST). The postage cost is £10.00, and the item is located in Manchester, Lancashire, United Kingdom. The listing also shows a "Supersize" button, a "Watch This Item" button, and a "Get alerts via IM" button. The listing and payment details are shown at the bottom, including the starting time, starting bid, duration, and payment methods (PayPal).

home | pay | register | sign in | site map

Buy Sell My eBay Community Help

← Back to list of items Listed in category: Business, Office & Industrial > Retail & Shop Fitting > Point of Sale

**Verifone Omni 3750 Chip Pin credit card PDQ POS**

Bidder or seller of this item? [Sign in](#) for your status



Current bid: **£40.00** [Place Bid >](#)

End time: **8 hours 50 mins** (09-May-07 20:46:33 BST)

Postage costs: **£10.00**  
Seller's Standard Rate  
Service to [United Kingdom](#)

Post to: United Kingdom

Item location: manchester, Lancashire, United Kingdom

History: [7 bids](#)

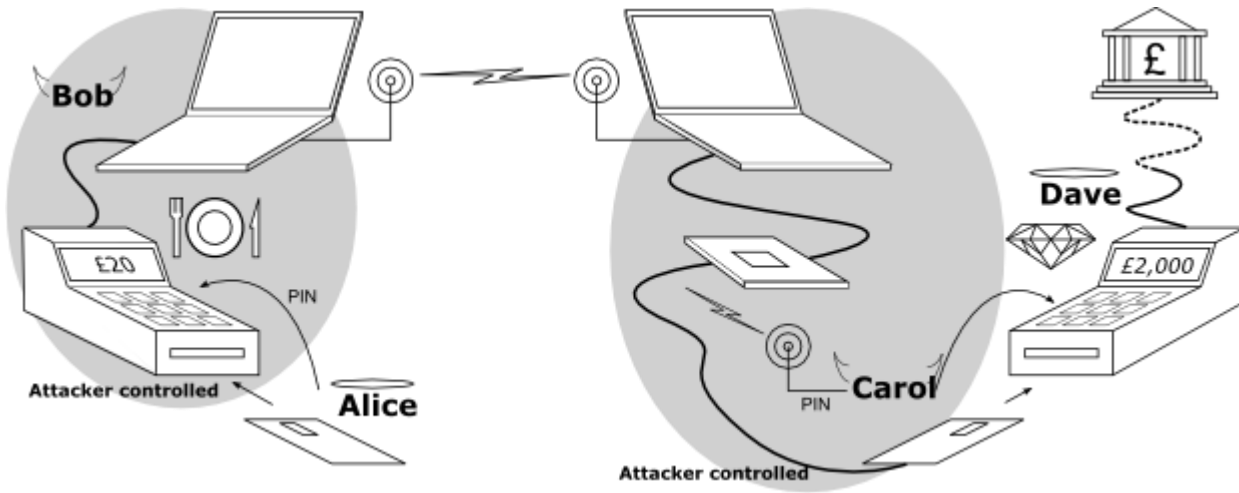
High bidder: [mas5252](#) (92 ★)

You can also: [Watch This Item](#)

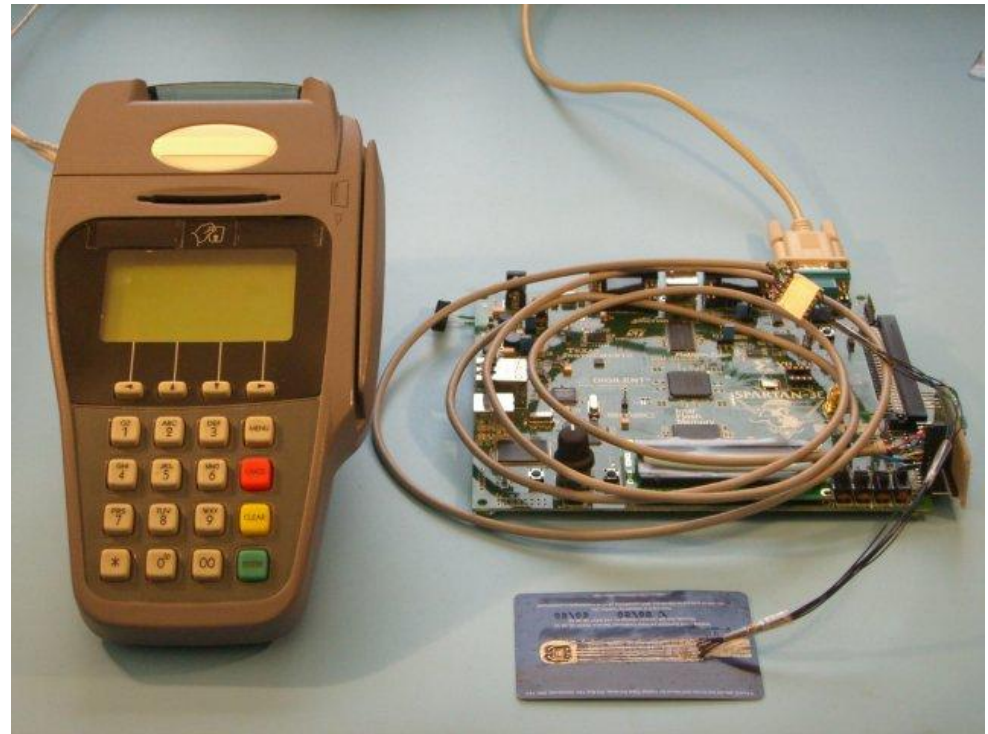
Get alerts via [IM](#)  
[Email to a friend](#)

Listing and payment details: [Hide](#)

Starting time: 06-May-07 20:46:33 BST Payment methods: **PayPal**  
Starting bid: £1.00 [See details](#)  
Duration: 3-day listing



Either add a transaction, or steal stripe data and PIN: your choice



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

# Looking for YouTube

Or just have  
fun

Chip & PIN terminal playing Tetris



<http://www.youtube.com/watch?v=wWTzkD9M0sU>

# Tesco and B&Q relay for you

- Both merchants use separated card reader and PIN entry, On UK cards, the PIN is not encrypted on the wire to the card. In the jargon, we use SDA, not DDA, 'cos it's cheaper.
- Halfords take a swipe for good measure *after* the transaction.



# They reply

Our Ref: 7769617

7 May 2007

Mr Denis Nicole

**TESCO**

Customer Service Centre  
Baird Avenue  
Dundee  
DD2 3TN  
Freephone 0800 505555

Dear Mr Nicole

Thank you for contacting us about Chip and PIN.

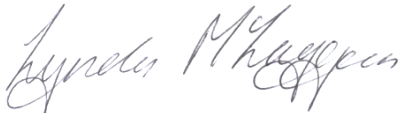
The swiping of cards is perfectly legitimate and accepted by CHIP & Pin

Our tills have not been set up to take chip and pin cards as yet, with the exception of Self Service checkouts. We hope to have all tills set up with the option of putting cards into the reader towards the end of this year

For more information on this subject please go to: <http://www.chipandpin.co.uk>.

Thank you for your enquiry.

Yours sincerely  
For and on behalf of Tesco Stores Ltd



Lynda McIlaggan  
Customer Service Manager

Halfords Limited  
Customer Services  
Redditch  
Worcestershire  
B98 0DE  
United Kingdom

Telephone:  
08450 579000

Facsimile:  
01527 513529

DX No: 714550  
Redditch 5

Web:  
[halfords.com](http://halfords.com)



Our Ref 21747

30<sup>th</sup> April 2007

Denis A Nicole

Dear Mr Nicole,

We confirm receipt of your letter on the 23<sup>rd</sup> April 2007 regarding your recent purchase at Halfords. In your letter you are concerned about our card swiping procedure.

As an anti-fraud measure to protect our customer and ourselves we need to capture card data on our tills. Many retailers are able to process the transaction using the till alone – hence only one swipe. Unfortunately we cannot do this and have to use a separate Streamline machine to process the payment. Therefore, we swipe the card into the till as well to capture the data but it does not feed into any other payment mechanism.

We now have 70 stores with CCTV, which means the police are pleased that we can identify who tried to use a stolen card. Unless we capture the card data on the till we could not do this.

In summary, we appreciate that this is not ideal, however the advantages to customer and ourselves outweigh this small disadvantage and we are planning to implement more modern tills in the future.

Thank you for taking the time to contact us regarding this matter and please be assured of our best intention at all times.

Yours sincerely,



Miss E Sanders  
Halfords Customer Services



## B&Q you can do it

Mr Nicole

MIS123 / 16384-308904

26 April, 2007

Dear Mr Nicole

I am writing in response to your recent letter regarding B&Q's Chip and PIN payment process.

I have discussed the issue with a Project Manager employed by B&Q who has been primarily involved in the Chip and PIN implementation in B&Q. He has advised at each till we have 2 operational Chip and PIN devices – the Pin Entry Device where you can “dip” your card and enter your PIN and the Swipe and Park which is attached to the side of the screen. Both devices are fully accredited by our acquirers.

With regards to your primary concern that as part of the Card Payment Process, I can confirm that we OFFER to take the customers card for processing, for the following customer service reasons (this list is not exhaustive):

- The Card must only be entered into the Pin Entry Device or Swipe and Park when the operator has pressed the correct buttons on the screen and received the correct prompts to proceed. If the card is entered or removed from either device – at the wrong time – then this can delay the whole payment process and cause delays at the checkouts, which inevitably lead to queues. The operator is therefore best placed to process the card.
- If the Payment card is not ICC or If the Chip on a Card is damaged, then the magnetic stripe details are used – Using the Swipe and Park device the till will automatically do this and the customer will be requested to sign. If the PED was to be used instead it would require removing the cards from the PED and swiped and parked through the device at the side of the screen. By using the Swipe and Park we cut out that additional process should the card not be ICC or there be any damage to the Chip in the card.

Working together to protect the environment. Cardano 5000 recycled fibre. 100% recycled fibre.



## B&Q you can do it

- We accept a number of discount cards that must be swiped and parked. Typically it is easier for the customer to hand over both cards and allow us to process both, rather than separate them out and offer one but not the other.
- The Till Software has been designed so that the next transaction can not be started, until the card has been removed from the swipe and park. This aids the customer as we will always give the card back to the customer before starting the next transaction thereby minimising the risk of the card being left in a device.

**N.B. Although we offer to take a customers card for processing, if a customer wishes to “dip” their own card in the PED then they have the options to do that by communicating their intentions with the operator – hence the reason why we obtained accreditation on two devices – to give the customer the choice**

With regards to your experiences in our stores when trying to use the PED to “dip” your card, this is difficult to explain but is certainly something that I will begin investigating and re-educating if necessary. As to the suggestion that we could be illegally capturing customer details I can confirm that this is NOT how B&Q operates. I can also say that for the system you describe to work in any kind of beneficial manner, then it would involve the banks and credit card companies supplying individual personal details over the payment card network to each retailer – which is quite incomprehensible.

Lastly I would also say that after being one of the last Level 1 Merchants to implement Chip and PIN we have been somewhat under the spotlight with our acquirers who provide our accreditation. I can confirm that they have raised no issues with regards to any concerns that you have outlined in your letter.

I hope that this letter constitutes a complete answer to your queries, and I trust that you will remain a valued customer of B&Q.

Yours sincerely

  
Laura Goatley  
Customer Services Advisor

Working together to protect the environment. Cardano 5000 recycled fibre. 100% recycled fibre.

# Bank 'security'

- Some anti-skimming devices on ATMs just jiggle the card; so learn DSP.
- PINsentry...



## Barclays' chip and PIN readers will work for other banks PINsentry will read all APACS-standard cards

By OUT-LAW.COM

Published Monday 23rd April 2007 09:20 GMT

Barclays Bank is introducing a handheld chip and PIN card reader for the home in an escalation of its online banking security. Other chip and PIN cards will work with the Barclays device, not just cards issued by Barclays.

Barclays has designed its system in accordance with standards issued by payment association APACS. Barclays says it will be the first deployment of its kind in the UK for personal banking customers. By conforming to the APACS standard the reader can be used as part of any system also using those standards. Not all chip and PIN cards conform to the standard at present.

In July the bank will begin sending half a million card readers to its home users. It is not charging customers for the devices, which it is calling PINsentry. They will be compulsory for those who wish to transfer money to third party bank accounts.

"The remaining customers will not need PINsentry at this stage – it will only be needed by those who use online banking to set up payments out of their account to a new third party for the first time," said a Barclays statement. "Customers who simply wish to use online banking to view their accounts and pay bills or established payees will be able to continue to use online banking as normal without the need for PINsentry."

A Barclays spokesman told OUT-LAW that the card readers, manufactured by Dutch security specialist Gemalto, will be sent to other customers who request one, even if they do not transfer money to third party bank accounts.

First transactions to third party accounts are being targeted for extra security because that is the outlet for any stolen money should a thief break into someone's online bank account.

When a customer inserts a card into the PINsentry reader and enters the correct PIN, the device will generate an eight digit number. That number must be typed in to the bank's website. For security, the card reader will not connect to a computer. For visually-impaired users, a larger card reader will be available that includes a loud speaker and a headphone jack.

PINsentry users will be asked to enter the eight digit number at login, even just to view account details. This means that to access their account details at work, customers must carry the readers with them. Upon instructing a transfer to a third party account for the first time, the user will be asked to generate another number and enter that number too.

# won't help...

- If it uses the **same** class of eight digit code for an initial login and to authorize a new third party...
- ...all the man-in-the-middle has to do is simulate a dropped session and request a new login.

# The Bank might just be inept



## How ATM fraud nearly brought down British banking Phantoms and rogue banks

By Charles Arthur

Published Friday 21st October 2005 09:52 GMT

This is the story of how the UK banking system could have collapsed in the early 1990s, but for the forbearance of a junior barrister who also happened to be an expert in computer law - and who discovered that at that time the computing department of one of the banks issuing ATM cards had "gone rogue", cracking PINs and taking money from customers' accounts with abandon.

...

"Stone had been working with building access systems using cards with magnetic stripes, and one day he thought he'd see what it could read of his ATM card. Then he tried it with his wife's." Stone figured that the stream of digits was probably an encrypted PIN.

"Then, because you can change the content of the magnetic strip, he wondered what would happen if he changed the number on his card to match his wife's. He found he could get money out using his old PIN." The high street bank Stone used (The Register knows which one) had not used the account number to encrypt the PIN on the card - meaning that any card for that bank could be changed and used to make withdrawals on any other account in it, providing you knew the right details (such as branch sort code and account number. The name of the card holder of course was unimportant, because it was not on the stripe.)

...

# Or corrupt

...

On 22 June 1993, Judge Hicks gave judgement, mostly in favour of the motion by Kelman, who expected the banks to simply settle.

But a few days later [Kelman](#) heard something that worried him deeply. The computing staff at one bank - the Rogue bank - had discovered through the dummy accounts how to fix the PIN generator so that it would only generate three different PINs in *all* the PINs issued. By creating a number of dummy accounts and getting new PINs issued for them, they could capture the sequence. Then all that was needed was to recode the cards so they would point to different account numbers, try the three PINs (ATMs gave you three chances) and they were away.



# mifare

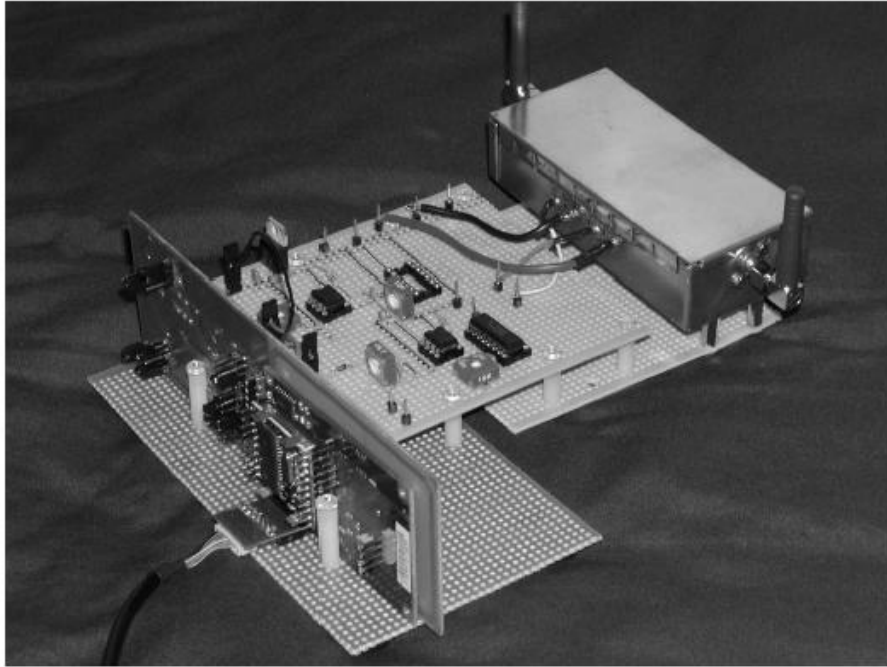
- The standard ISO14443 protocol for 13.56MHz proximity cards
- Widely used: Oyster, passports
- There isn't much power, so the cards use a Philips proprietary symmetric stream cipher: CRYPTO1; there are some rumours it has been reverse engineered in China. Other rumours suggest it is triple-DES-like.
- Philips also *try* to restrict access to the reader chip specs...but not the [CL RC632](#)



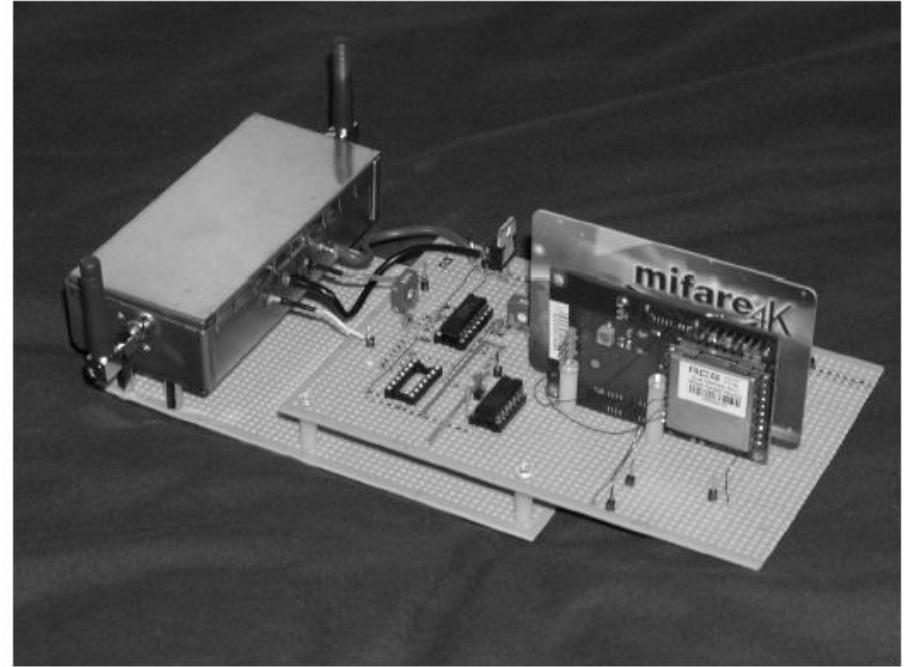
# Access control

- Much access control relies on the card ID, part of the public protocol, like a MAC address. Just build your own card...easy with a battery.
- Passports use a randomised ID to discourage people-tracking.

# General thievery



(a) Proxy



(b) Mole

*A Practical Relay Attack on ISO 14443 Proximity Cards,*  
Gerhard Hancke

<http://www.cl.cam.ac.uk/~gh275/relay.pdf>

# Is there a legitimate use for a keylogger?

LM892 | UNBRANDED | Computer Hardware & Interface Cards | Mechanical, Office & Workplace

http://onecall.farnell.com/jsp/Mechanical,+Office+&+Workplace/Computer+Hardware+&+Interface+Cards+Mechanical,+Office+&+Workplace.jsp

LM892 | UNBRANDED | Computer Hardware & Interface Cards

**onecall**  
Working in partnership with NUWPEC

Product Search


RoHS compliant items only

HOME ONLINE CATALOGUE MY BASKET MY ACCOUNT SERVICES ELECTRONICS DEPARTMENT

Username  Password  [LOG IN](#) [Register Here](#)  
[Forgotten your password?](#)

Back to [Mechanical, Office & Workplace](#) > [Office - Computer Products & Stationery](#) >

**LM892 — UNBRANDED — KEY SHARK** New



**Manufacturer:** UNBRANDED  
**Order Code:** CS1425901  
**Manufacturer Part No:** LM892  
**RoHS Compliance:**  Yes

**Description**

- KEY SHARK
- Colour:Black
- Interface type:PS/2
- Length / Height, external:53mm
- Memory size:2MB
- Width, external:12mm

*Image is for illustrative purposes only.  
Please refer to product description*

LM932 | UNBRANDED | Computer Hardware & Interface Cards | Mechanical, Office & Workplace

http://onecall.farnell.com/jsp/Mechanical,+Office+&+Workplace/Computer+Hardware+&+Interface+Cards+Mechanical,+Office+&+Workplace.jsp

LM932 | UNBRANDED | Computer Hardware & Interface Cards

**onecall**  
Working in partnership with NUWPEC

Product Search


RoHS compliant items only

HOME ONLINE CATALOGUE MY BASKET MY ACCOUNT SERVICES ELECTRONICS DEPARTMENT

Username  Password  [LOG IN](#) [Register Here](#)  
[Forgotten your password?](#)

Back to [Mechanical, Office & Workplace](#) > [Office - Computer Products & Stationery](#) >

**LM932 — UNBRANDED — USB KEY LOG** New



**Manufacturer:** UNBRANDED  
**Order Code:** CS1425801  
**Manufacturer Part No:** LM932  
**RoHS Compliance:**  Yes

**Description**

- USB KEY LOG
- Colour:Black
- Depth, external:38mm
- Interface type:USB
- Length / Height, external:17mm
- Memory size:2MB
- Width, external:20mm

*Image is for illustrative purposes only.  
Please refer to product description*

The print catalogue says: *You should not use this device to intercept data you are not authorised to possess, especially passwords, banking data, confidential correspondence etc. Most countries recognise this as a crime...*

# More links

- A generic reader:

<http://cq.cx/proxmark3.pl>

- Some software:

<http://www.rf-dump.org/>

<http://openmrtid.org/projects/librfid/>

<http://www.rfidiot.org/>

<http://www.rfidguardian.org/>

- E-Passports:

<http://www.wired.com/science/discoveries/news/2006/08/71521>

- Banking Organisations:

EMVCo: Europay, Mastercard and Visa,  
publishers of the Chip & PIN standards.

Society for Worldwide Interbank Financial Telecommunication  
APACS