Chip-to-Cloud Security Forum

UCL RIBS Resilient Infrastructure and Building Security

funded by EU FP7

Building and Transport Cards:
Attacks & Defences

Nicolas T. Courtois[1,2],
Daniel Hulme[1,2],
Kishan Gupta[1]

[1] University College London, UK

[2] NP-Complete Ltd, UK

satalia
the solve engine

UCL

Scope:

Most Popular Contact-less Smart Cards

- Building Access Control
- Public Transportation
  - and Other Small Payments

Their Security: Focus on Card Cloning

- Which cards are more/less secure

Philosophy

Security of Smart Cards

[Schneier and Schostack 1999 paper]

- splitting the security perimeter
- hardware barriers that cannot be breached by software,
- physical control of the card by the user,
- and trusting the entities involved in developing components of a secure system

RFID

This model somewhat breaks apart with RFID smart cards…

RFID => no user control.

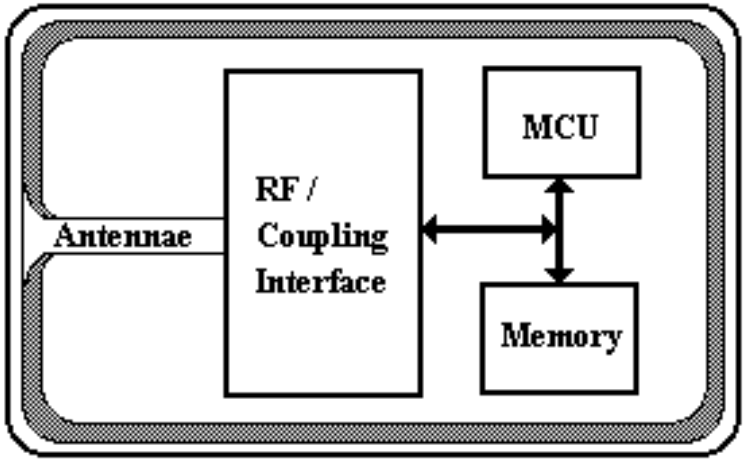
Secrecy

The secrecy of the product spec is:

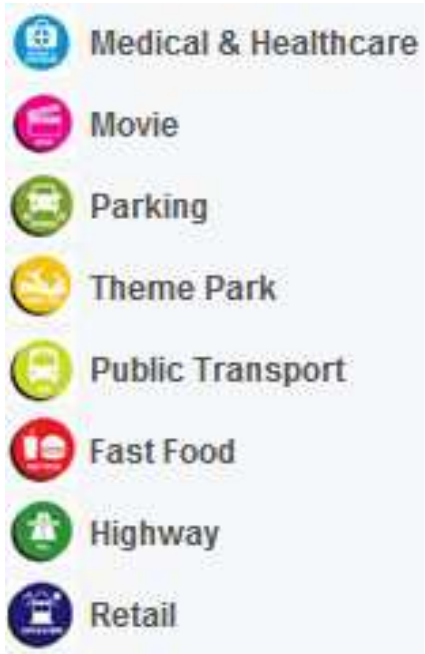
- not an extra security layer,
- but a source of unexpected and critical security vulnerabilities
  - that by the fact of being hidden give an utterly false sense of security

Contact-less Smart Card

- with RF transceiver
- 0.1 s transaction
  - less energy
  - less computing power



Building Transport and Small Payments



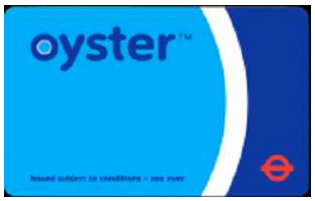
Malaysia

(MiFare Classic !)

Transport Card Systems

Main Standards:

- Calypso
  [France, Belgium]
- MiFare
  [UK, Holland,
  Etc..]
- Other standards exist.
  In Asia: Sony Felica
  [Japan,India,HongKong
  ,etc..]



Building Cards

Supply Chain Control and Segmentation

supply chain control: it is hard for criminals to get these systems for reverse engineering…

segmentation = additional security perimeter splits:

- In some systems a smart card used in one company CANNOT be re-programmed to work in another building.

But…

… However

Problem: Companies have little choice.

- If they are price sensitive they will be sold insecure systems.
- If they aren't they are still NOT sure that systems are secure,
  - because the market is not very competitive and security is taboo: you are expected to trust the supplier.

Our UK SURVEY 2012 Building Cards (only)

Survey [2012]

2012.

Survey conducted among
400 UK companies.

Some 20 has responded
to our questionnaire.

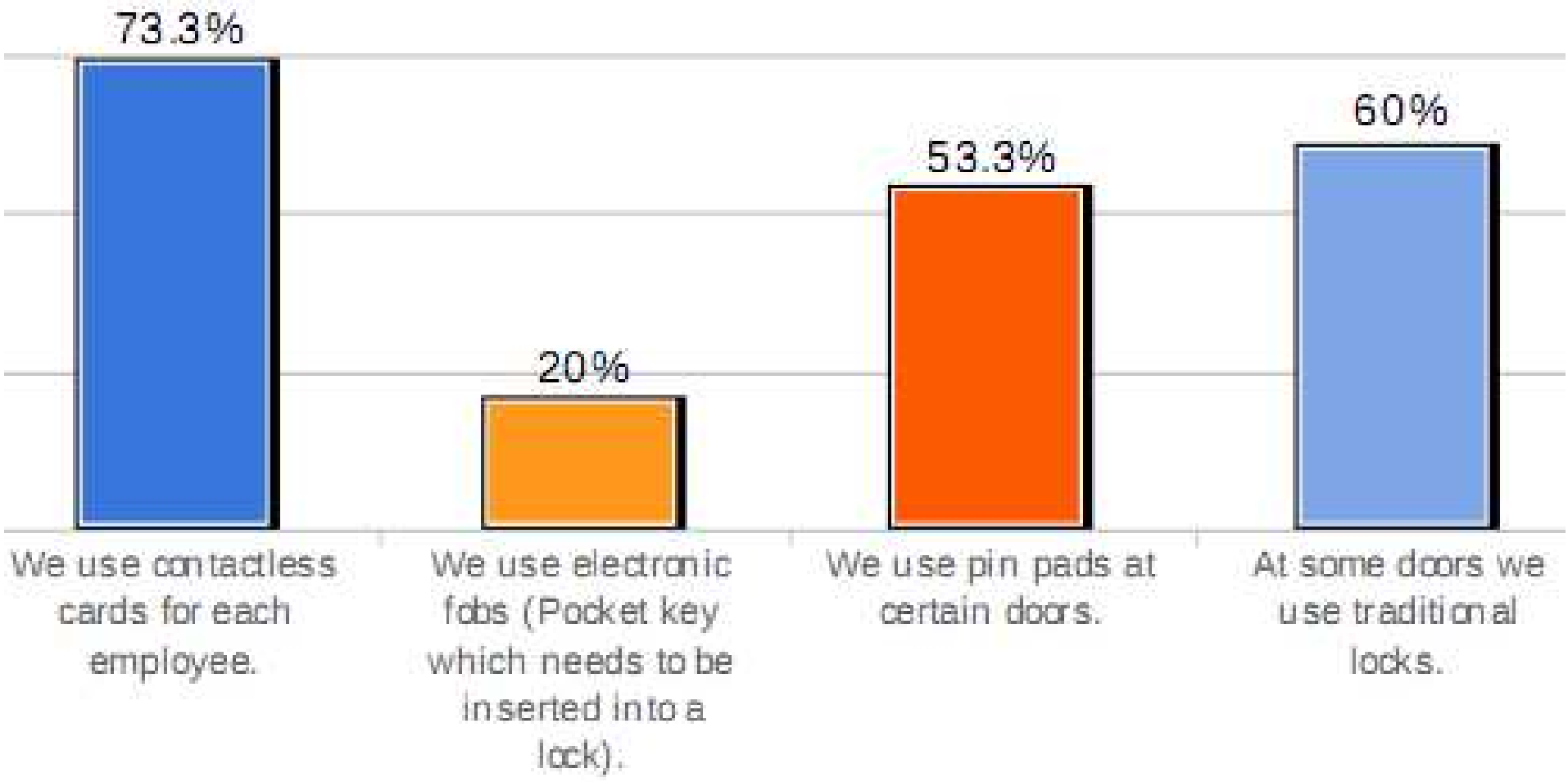
Sensitive questions, collected anonymously.

Details:

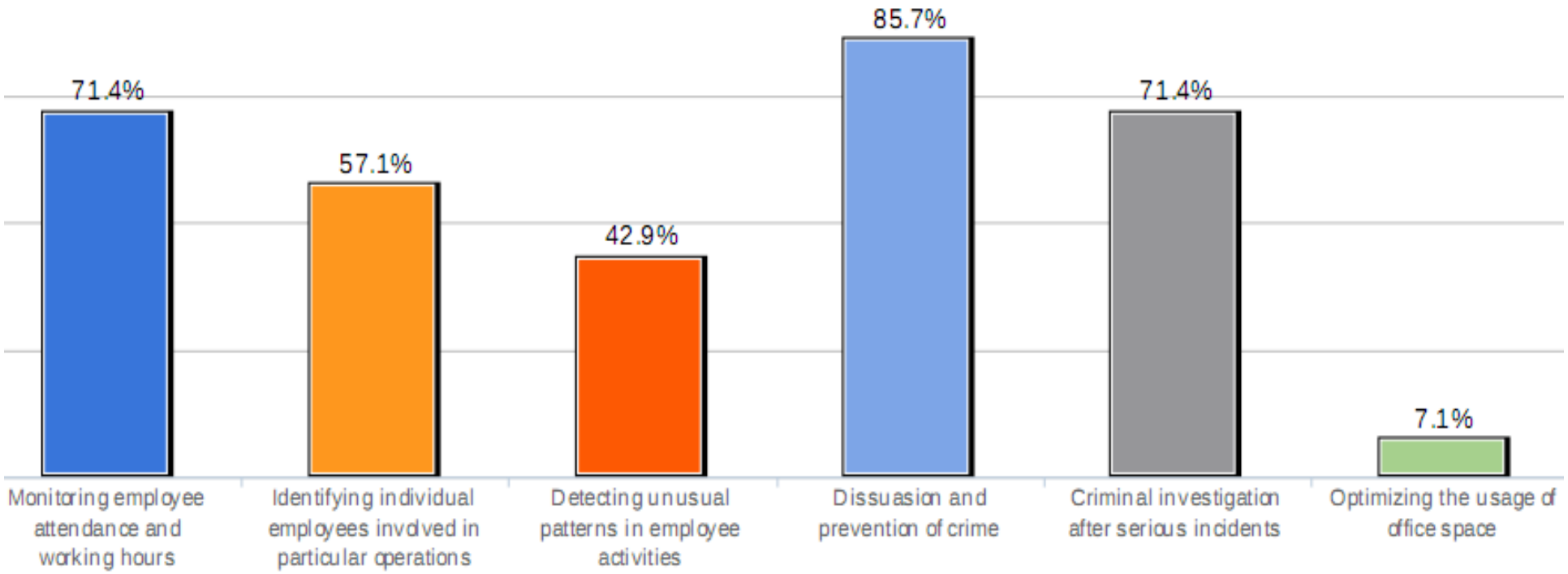
Master Thesis by Ayoade Adebanke,
M.Sc. Information Security,
University College London, September 2012

Key Findings

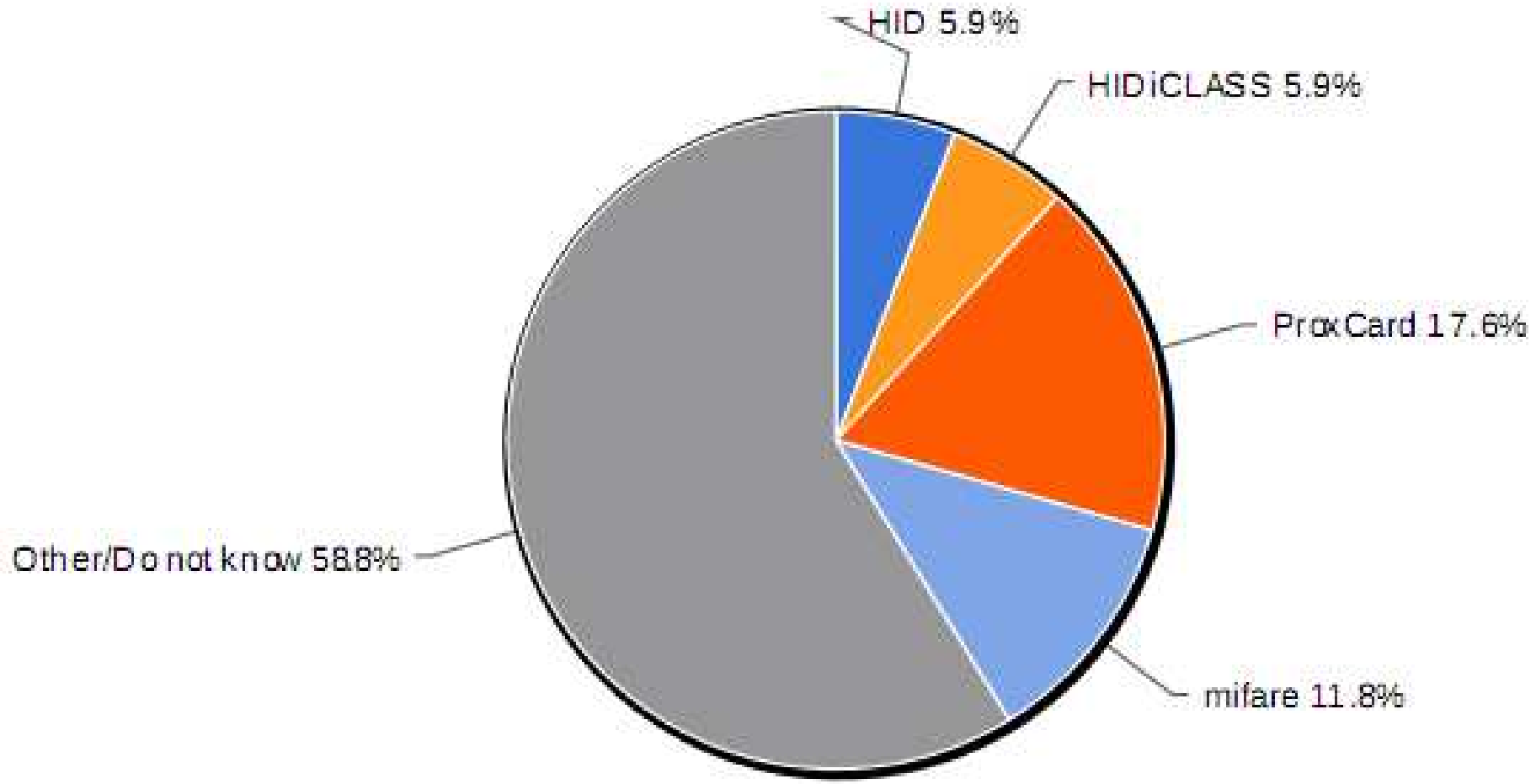
Smart Cards Are Popular in the UK



What Do We Need These Systems For?

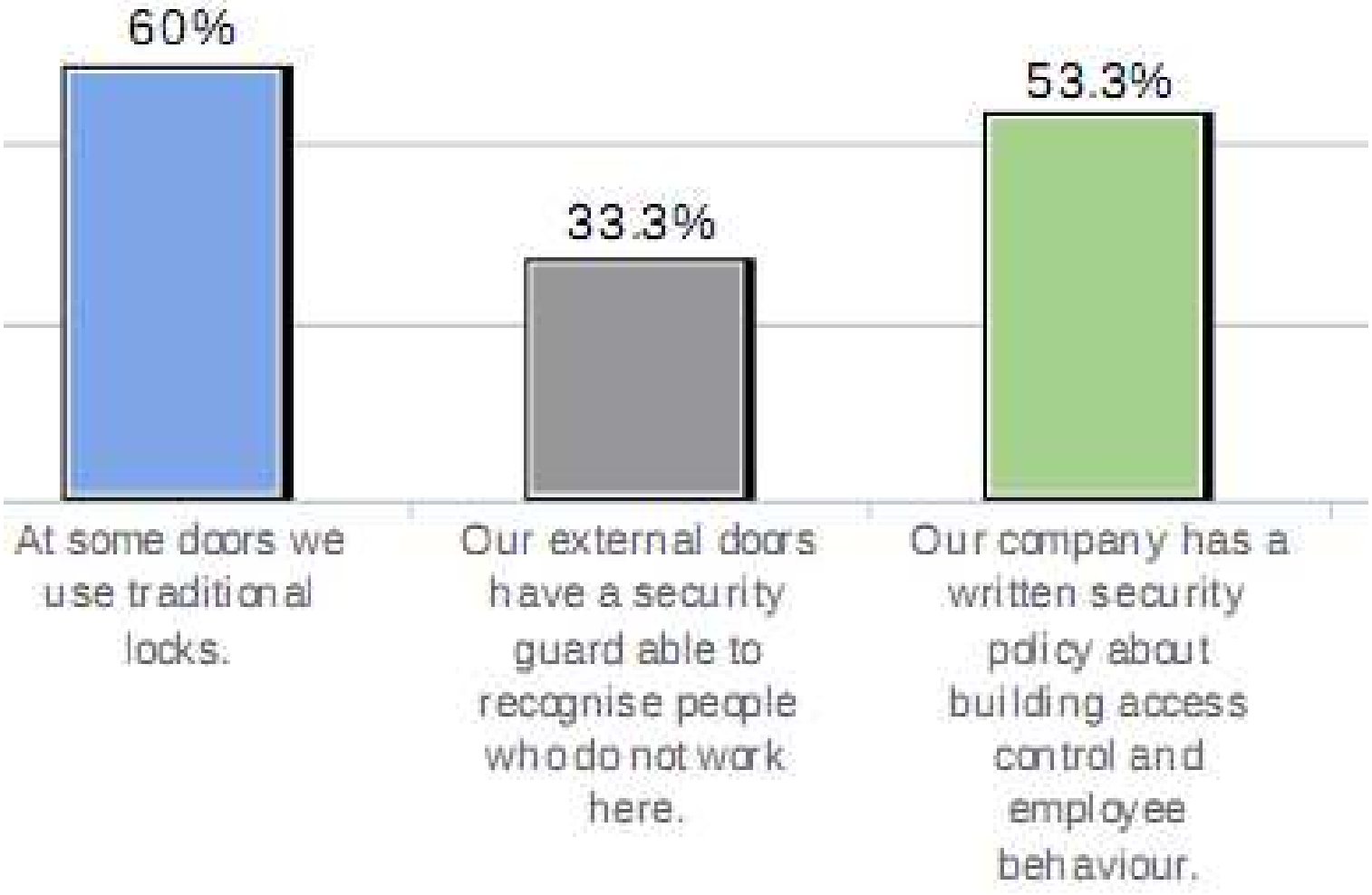


Not Know / Not Care / Obscure Reseller Brand

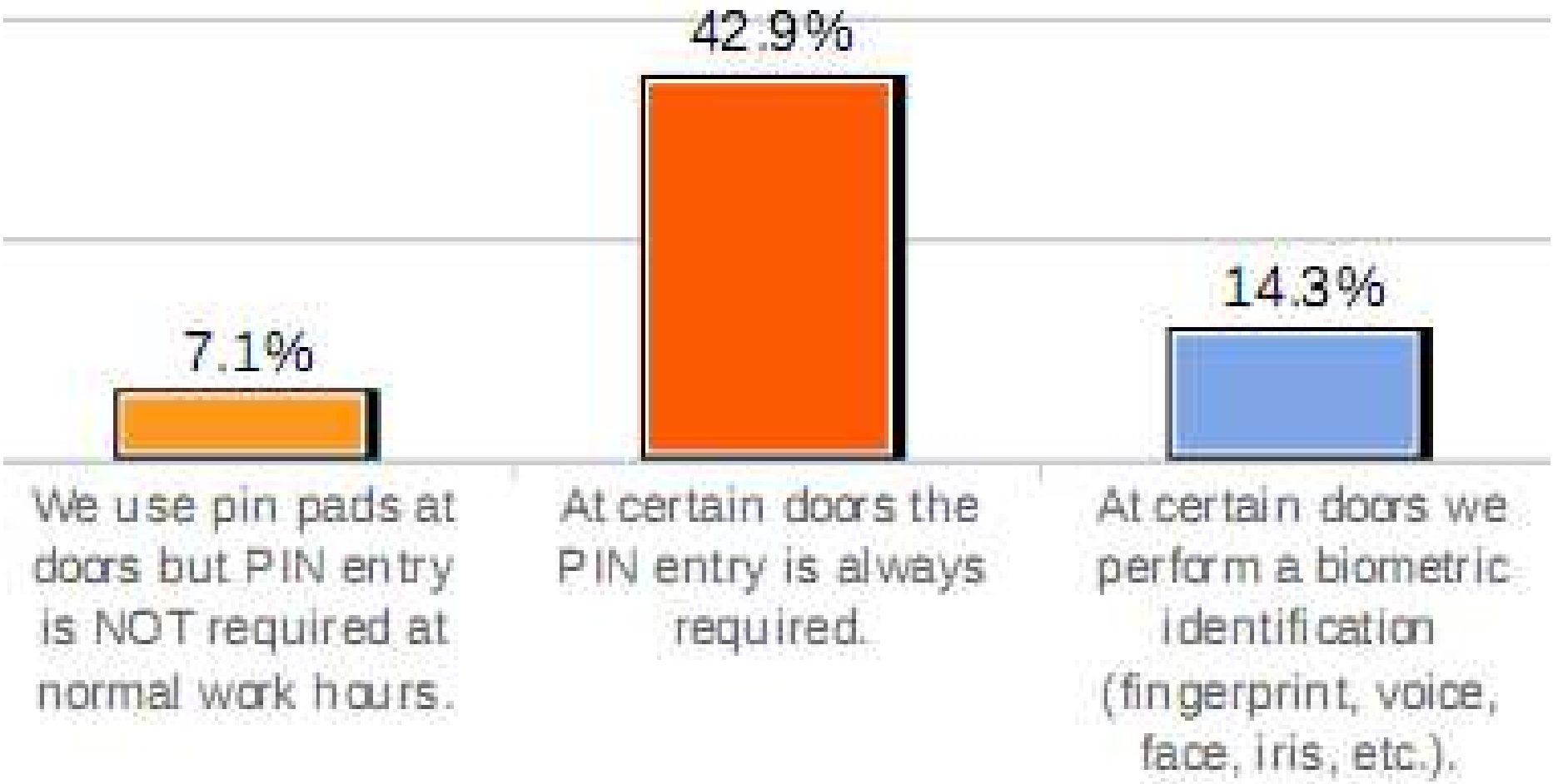


Security in Place

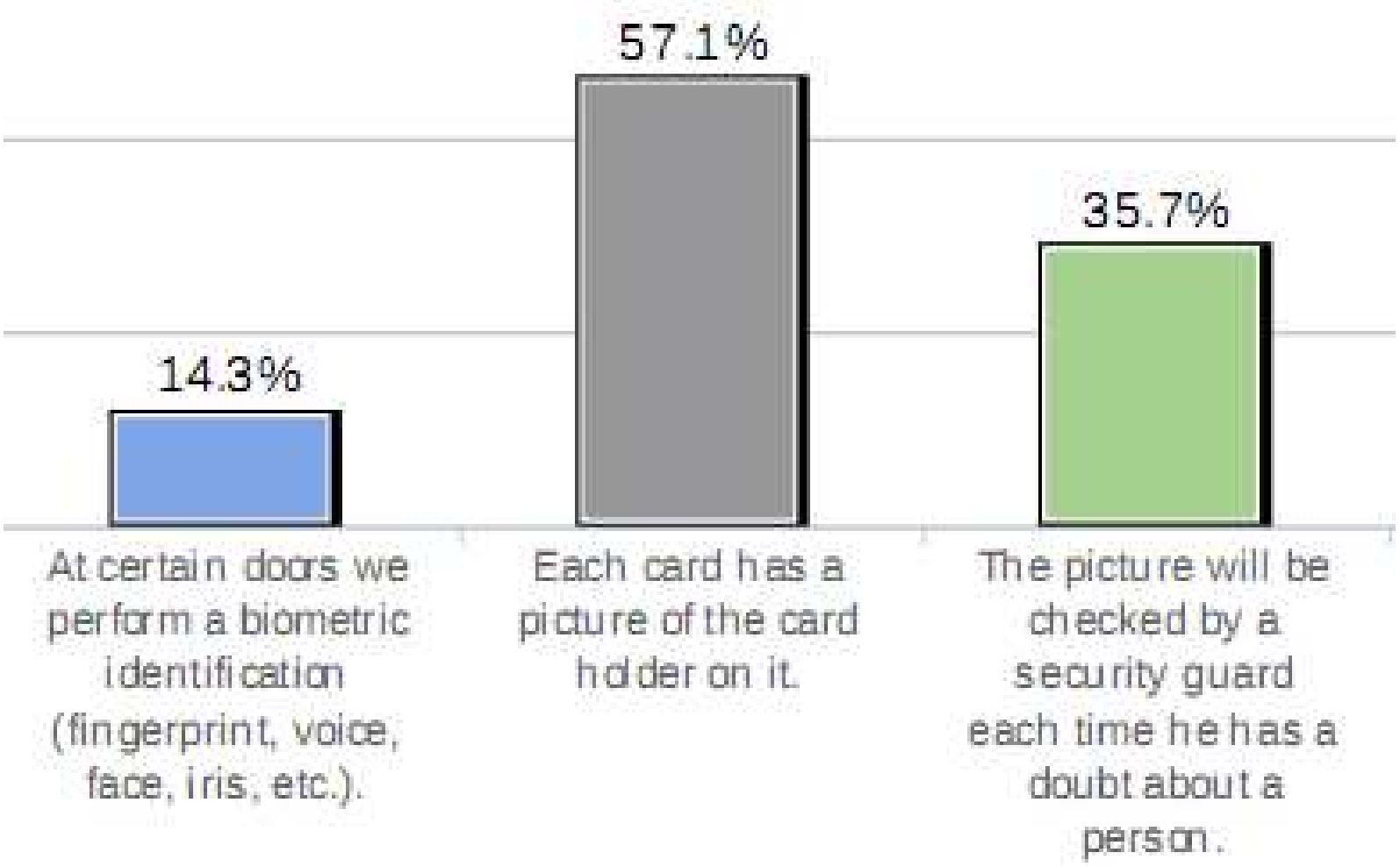
Cards + Extra Security



Card + PIN?


42.9%
7.1%
14.3%
We use pin pads at doors but PIN entry is NOT required at normal work hours.
At certain doors the PIN entry is always required.
At certain doors we perform a biometric identification (fingerprint, voice, face, iris, etc.).

Biometrics


57.1%
35.7%
14.3%
At certain doors we perform a biometric identification (fingerprint, voice, face, iris, etc.).
Each card has a picture of the card holder on it.
The picture will be checked by a security guard each time he has a doubt about a person.

Building/ID Cards Security, Cloning, Etc..

Building Cards – 2 Types

- RFID cards: Broadcast unique serial number

- More advanced cards with cryptography.

Building Cards – 2 Types

- RFID cards: Unique serial
  - Proprietary encoding of transmission
    - Initially hard to imitate
      - but eventually decoded recorded and replayed perfectly

---

- Cards with cryptography.
  - Mutual Authentication
  - Encrypted Communications
  - Tamper resistance: for data and cryptography.

Wiegand Interface

26-Bit Wiegand Format

Cryptographic Cards

Building Cards – 2 Types

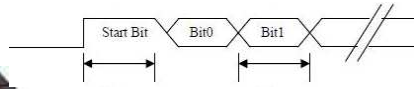
- RFID cards: Unique serial
  - Proprietary encoding of transmission
    - Initially hard to imitate
      - but eventually decoded recorded and replayed perfectly

---

- Cards with cryptography.
  - Mutual Authentication
  - Encrypted Communications
  - Tamper resistance: for data and cryptography.

Wiegand "Loophole"

may be secure..



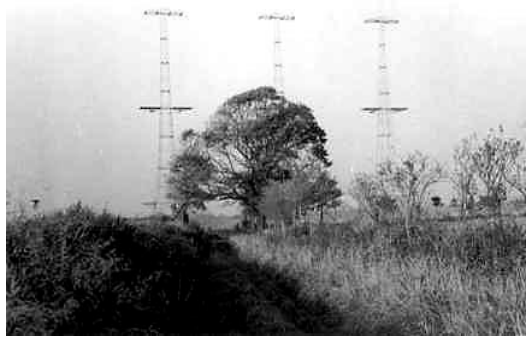
26 bits

cannot be very secure!

All data are NOT transmitted to the controller or the back-end system!

Contact-less Authentication - History

IFF: Identify Friend or Foe (1942)



Challenge-

-Response

problem: relay attacks

Hidden Cryptography!

Normal high-level access to data on the card.

GET CARD SERIAL NUMBER

CLA	INS	P1	P2	Le
FF	CA	00	00	00

LOAD KEY IN RAM REGISTERS

CLA	INS	P1	Kt	Le	Key
FF	82	20	00	06	FFFFFFFFFFFF

MIFARE CLASSIC AUTHENTICATE

CLA	INS	P1	P2	Nb	Kt
FF	88	00	3A	60	00

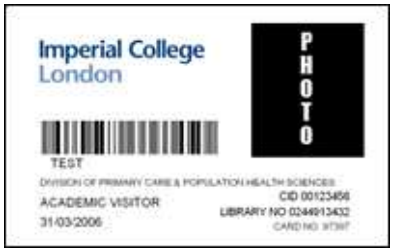
MIFARE CLASSIC READ

CLA	INS	P1	P2	Le
FF	B0	00	3A	10

MIFARE CLASSIC WRITE

CLA	INS	P1	P2	Lc	Data
FF	D6	00	3A	10	

Confidential crypto algorithm is implemented inside the reader, the developer will totally ignore it and may think that the security is very high, or very low, there is no way to tell!



Main "Crypto" Cards

MiFare Classic:

- >1 billion of these cards sold!
- 70 % of the contactless badge/ticketing market
- Oyster cards [all cards issued before 2010], UK Cabinet office, Cambridge uni, etc…

More recent Oyster cards [2010-now] are MiFare DesFire,

- No cryptographic attack yet, broken only by side channel attacks [cost: few thousands of dollars per card].
- No working card simulator on hacker market yet.

HID iClass

<> HID Prox: unique serial nb. no other security

HID iClass

Almost serious crypto
with DES and 3DES
but keys have been
”obtained” by reader firmware
hacking methods [Meriac 2011]

Clone Attacks

Cloning the Card

Is it feasible to
re-program the card itself?

Clone Oyster Card?

All card emitted before 2010 were MiFare Classic 1K ☹

?

BUT,

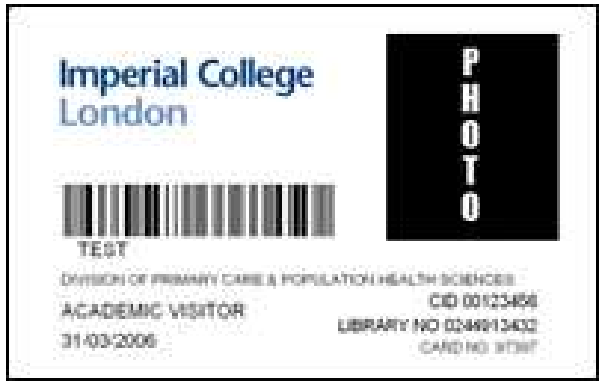
not so easy:

No blank cards on the market in which one can change the serial number.

Unique ID

MiFare Classic in sector 0.

Cannot be changed, not even by the manufacturer.

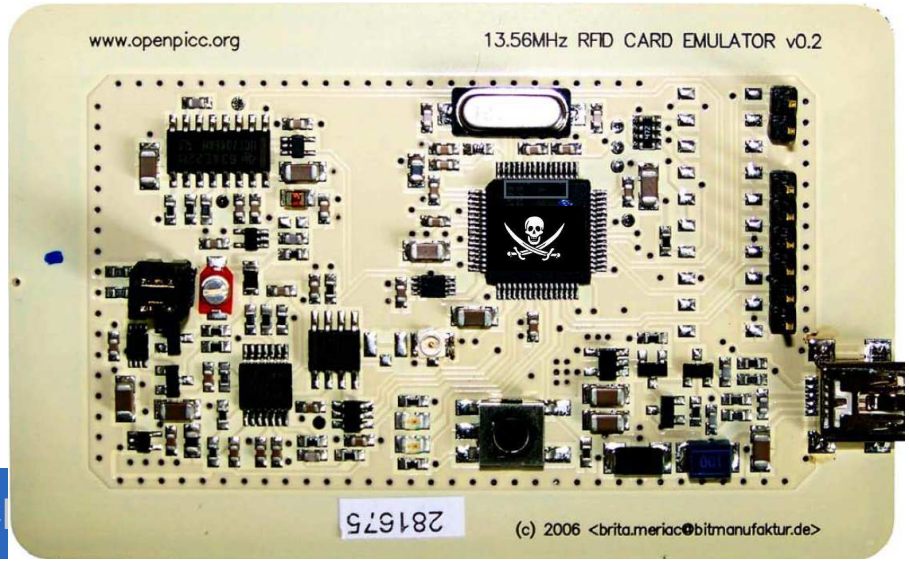


The only security in many building systems…

[Cambridge, Imperial, UCL, etc.]

Attack:

card simulation



Cloning the Card

Is it feasible to

re-program the card itself?

Sometimes it is!

Example 1:

HID Prox [1991-today]

- unique serial + proprietary encoding

no other security

Can be reprogrammed into another white card or tag,

–T5667R/W or Q5 are widely available.

Example 2:

HID iClass [2002-today]

- Crypto cards
  - Mutual Authentication
  - Encryption of Data

problem: reader firmware update procedure is insecure [Meriac 2010]

Hacking iClass Readers [2010]

Steps:

1. Get just one genuine reader like RW400 [100 GBP].
   - standard security: any reader!
   - high security version:
     - the same but the hacker needs to get hold of a reader from the same building
   - we were able to get one easily
2. Produce a custom debugging interface.
   - make a non-standard connector
   - build a non-standard firmware programmer

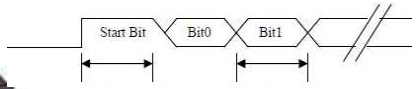
3. Execute 2 separate software exploits (half way between a boot virus and a Trojan) to dump a) the boot block b) the main program c) the EEPROM
4. The code contains 3DES keys in cleartext.
5. These keys are already in possession of German hackers since December 2010, cf. Milosh Meriac, CCC 2010 paper.

Hacking iClass Readers [Dec 2010]

3DES Key!

- read and write any card. We NEED ONLY:
  a standard publicly available reader [80 GBP]
  + free software provided by the manufacturer.
- only blocks 2,5 and 9 need to copied…
- this will NOT change the serial number BUT…

Imperfect Clone Works !?!



26 bits

data

Crypto:

- derive key
- authenticate
- read

- copy data blocks 5 and 9
- can be copied to ANOTHER ordinary card
- this will NOT change the serial number BUT…
- many door readers do NOT transmit the serial number!!! So the cloned card works!
  - card simulator not needed…

- different SN
- different key
- same data

What Makes Cloning Harder?

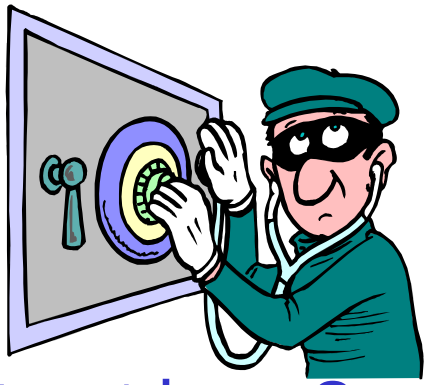
and how to get around it

Anti-Cloning Functionality?

- RFID cards: Unique serial
  - in hardware,

- Crypto cards
  - Mutual Authentication
  - Encryption of Data

} Secure crypto implementation



extract keys?

Crime Scripts – Cloning [1]

- RFID cards: Unique serial
  - in hardware, CANNOT be changed

record and decode

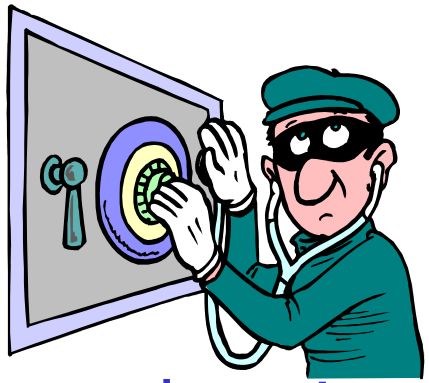
use a card simulator

Crime Scripts – Cloning [2]

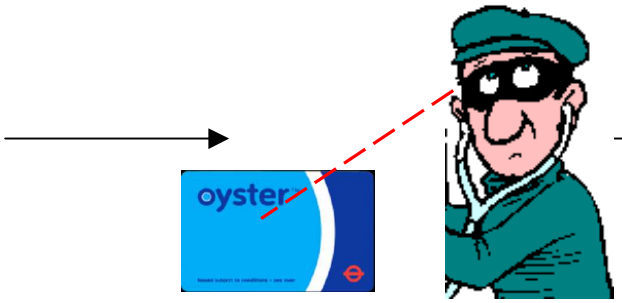
- RFID cards

–

- Crypto cards:



extract keys!



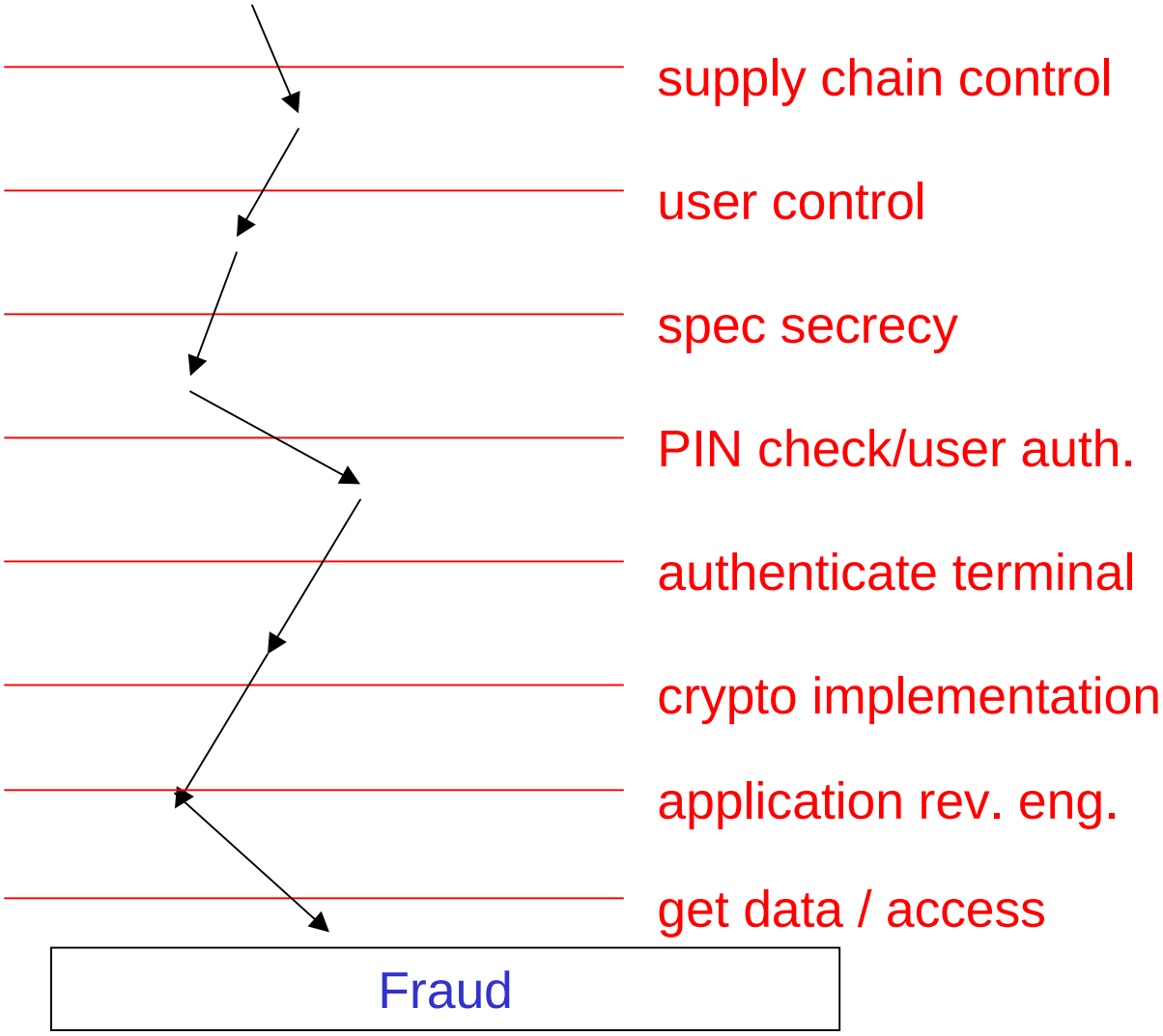
read the data

simulate

Defence in Depth Principle

Learn from the Military:
layer the defences.

Defenses of the Card

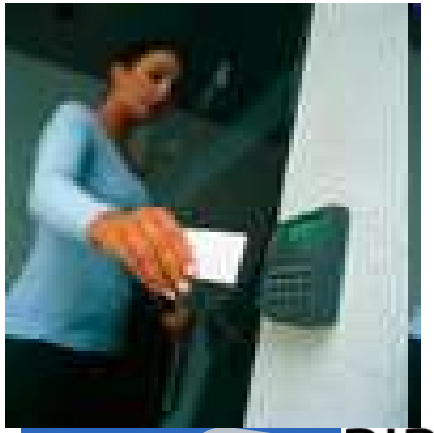


Crime Script

MiFare Classic Crypto-1

Stream cipher used in about 200 million RFID chips worldwide.

- Ticketing (e.g. London's Underground).
- Access to high-security buildings
- Etc.



Again: Not Like This

Cryptography is invisible

GET CARD SERIAL NUMBER

CLA	INS	P1	P2	Le
FF	CA	00	00	00

LOAD KEY IN RAM REGISTERS

CLA	INS	P1	Kt	Le	Key
FF	82	20	00	06	FFFFFFFFFFFF

MIFARE CLASSIC AUTHENTICATE

CLA	INS	P1	P2	Nb	Kt
FF	88	00	3A	60	00

MIFARE CLASSIC READ

CLA	INS	P1	P2	Le
FF	B0	00	3A	10

MIFARE CLASSIC WRITE

CLA	INS	P1	P2	Lc	Data
FF	D6	00	3A	10	

=> Cannot be broken like this.

Low Level Access

==

Commands sent over the air.

These boards + software work
and are widely available:

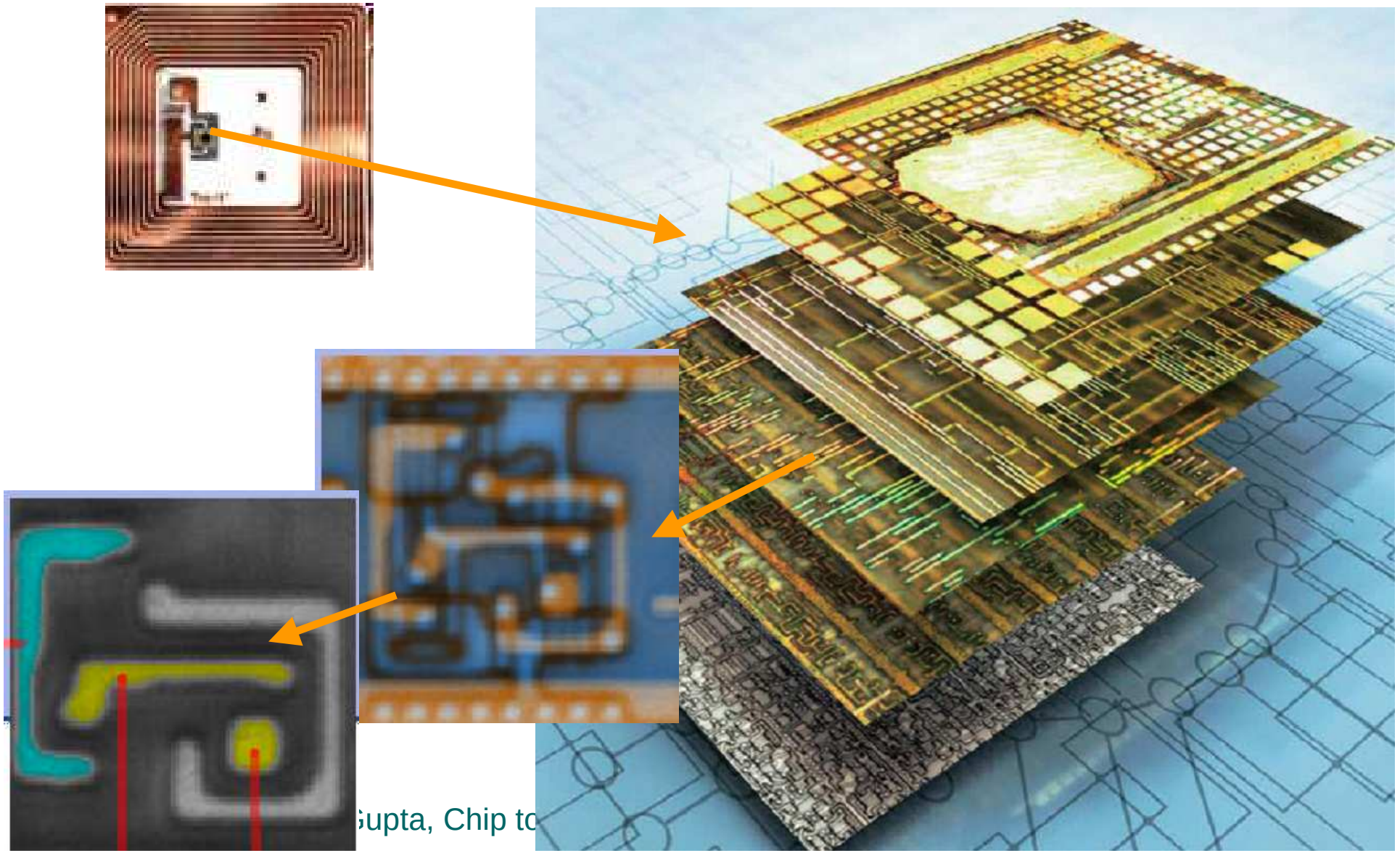
C++ + nfclib + ACR122

Example:

> 26
< 0400
> 9320
< CA1C46D141
> 9370CA1C46D141 (CRC)
< 08 (CRC)
> 6000(CRC)
< 24D2783A
> CF80E99F1AA2A1F1
> …

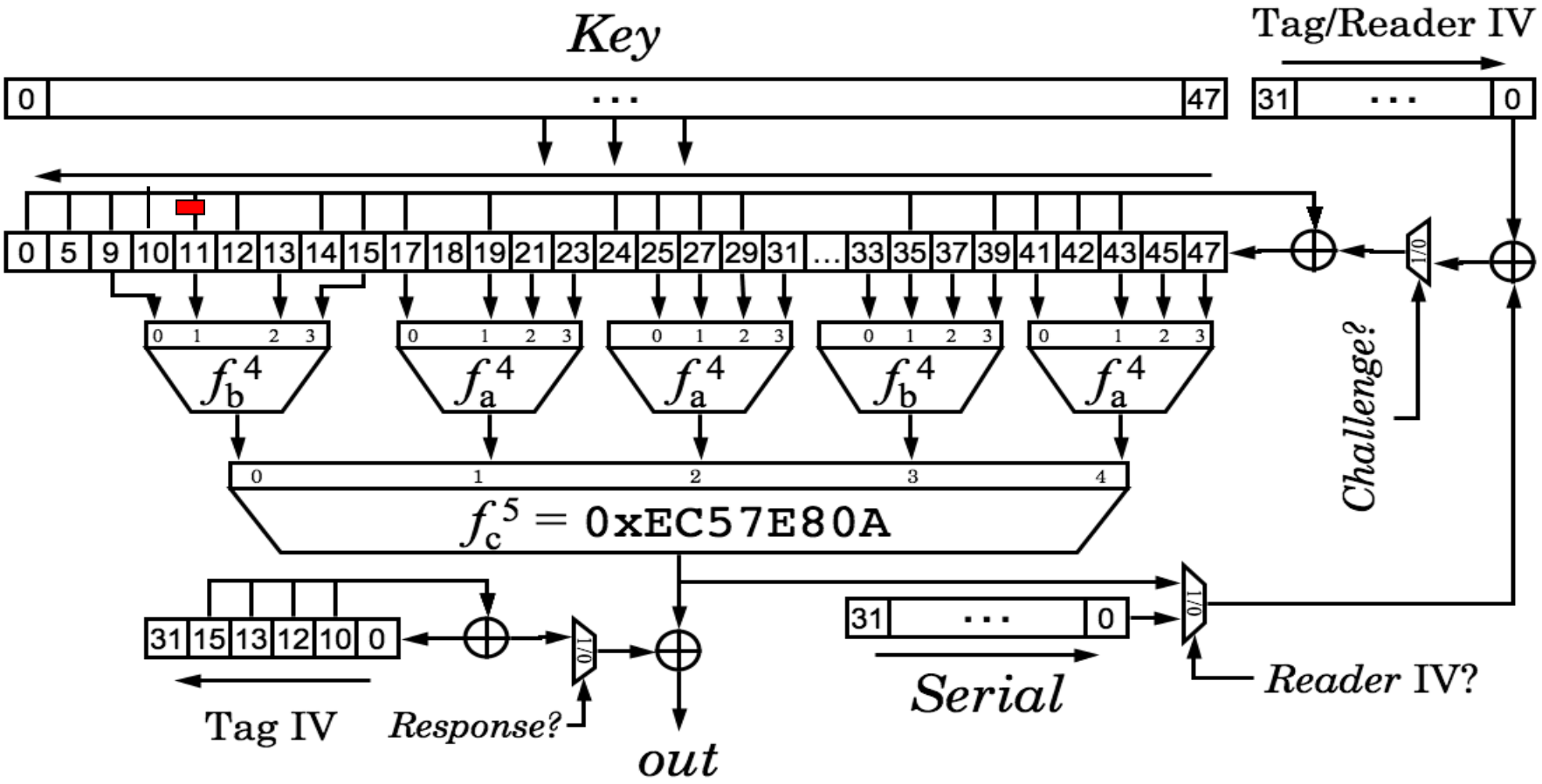
UID

Reverse-Engineering [Nohl et al.]



Gupta, Chip to

Crypto1 Cipher



$f_a^4 = 0x9E98 = (a+b)(c+1)(a+d)+(b+1)c+a$

$f_b^4 = 0xB48E = (a+c)(a+b+d)+(a+b)cd+b$

Tag IV ⊕ Serial is loaded first, then Reader IV ⊕ NFSR

Waste of Silicon

Internal bits are computed 2-3 times.

One could save half of the gates!

Terrible weakness:
super-strong self-similarity.

A monkey typing at random
would have designed a more secure cipher..

Easy To Break?

- 0.05 seconds.
  [de Koning Gans et al, Esorics 2008]

Requires recorded communications with a genuine reader.

- The hacker must already penetrate into the building.
- Small window of opportunity.
- CCTV, monitoring… etc…

Moreover: It is Illegal

Regulation of Investigatory Powers Act
RIPA [2000].

[…] "It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication in the course of its transmission " […]

In Contrast:

Reading somebody's card is
NOT explicitly illegal
[except in some US states,
new laws]

Card-Only Attacks

Card-Only Attacks

<u>The real security question is:</u>

Can I copy it, when I am sitting near the cardholder for a few minutes in the underground (contactless card queries).

Yes!

Card-Only Attacks

Danger is 24h/24:

Anybody that is sitting/standing next to you can steal your identity (or at least enter some very nice building…)

Card-Only Attacks Infeasible?

Yes, due to the protocol.

Sound engineering principle:

The card never ever answers anything related to the secret data, unless the reader sends a valid cryptogram on 8 bytes…

Card-Only Attacks: Infeasible => Possible?

or how MiFare Classic was broken anyway

[4 Attacks by Dutch Nijmegen group
+ the ‘Dark Side Attack’ by Courtois, 2009]

A Bug in MiFare Classic

Discovered accidentally.

- sometimes, under certain conditions, the card outputs a mysterious 4 bits…
- given the fact that many RFID readers are not 100 % reliable, it is easy to overlook it

The Bug?

Or maybe a backdoor?

Secure Product Development

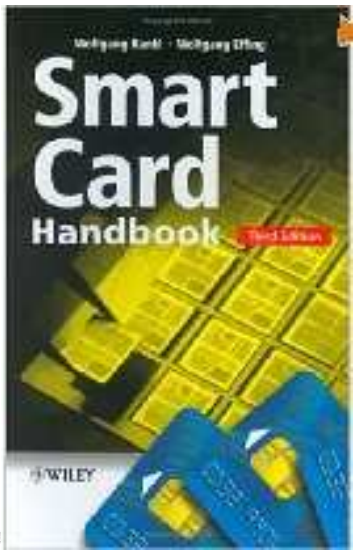
Secure Hardware Dev. Management

[In smart cards] one design criterion differs from the criteria used for standard chips but is nonetheless very important is that absolutely no undocumented mechanisms or functions must be present in the chip ('that's note a bug, that's a feature').

Since they are not documented, they can be unintentionally overlooked during the hardware evaluation and possibly be used later for attacks.

The use of such undocumented features is thus strictly prohibited [...]

[pages 518-519 in the Smart Card handbook
by Wolfgang Rankl and Wolfgang Effing,
1088 pages, Wiley, absolute reference in the industry]



The “Bug” was known…

Courtois was the first to circulate a paper that describes this vulnerability in March 2009.

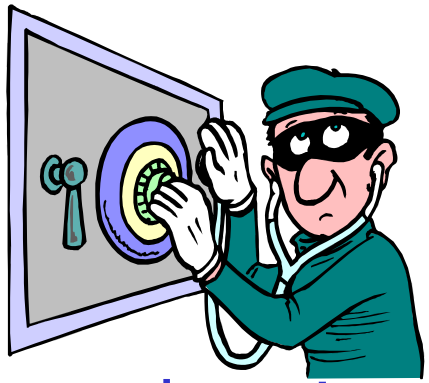
But in fact many researchers knew about it already…

Crime Scripts – Cloning [2]

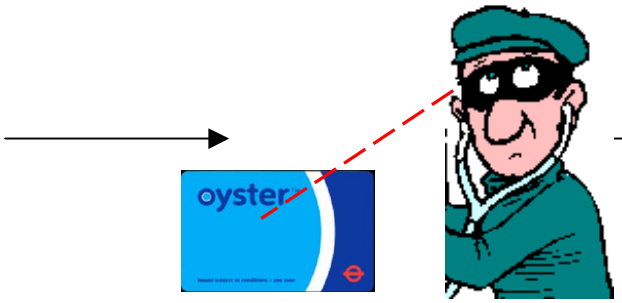
- RFID cards

–

- Crypto cards:



extract keys!



read the data

simulate

More Details:

Slides about MiFare Classic

www.nicolascourtois.com/papers/mifare_all.pdf

Full paper: SECRYPT 2009, see also eprint.iacr.org/2009/137/

Hack it at home:

step by step instructions:

http://www.nicolascourtois.com/MifareClassicHack.pdf

Embarrassing Discoveries

Strange Weaker Cards

Example: card used in Kiev, Ukraine underground [hosting Euro 2012].

- Unlicensed illegal clones of MiFare Classic.
  - nobody expected that there will ever be a HIDDEN method to distinguish?
    - normal functionality is identical
  - careful examination shows that they are Fudan Microelectronics FM11RF08 from Shanghai, China.
    - This card will ALWAYS answer the spoof attempt. Easier to clone…

More Strange Clones

There are other clones. Come from India, China and Russia (!). http://www.proxmark.org/forum/topic/169/mifare-classic-clones/

Remark: People/companies in Russia China and India

- did not advertise their hacking exploits,
- did NOT publish a nice paper at CARDIS or CHIP TO CLOUD conference…
- They just made clones…

Combined Attacks (ours + Nijmegen)

Best Attack in Practice

Use ‘Courtois Dark Side’ attack for one sector.

Then use Nested Authentication attack
[Nijmegen Oakland paper] for other sectors.

Google for MFCUK and MFOC software…

[provided by Costin and Nethemba]

Case Study: Oyster Cards vs. Warsaw Poland Metro/Bus/Parking Card

V3.co.uk

Tech Daily

News | Analysis | Comment | Reviews

Oyster cracker vows to clone cards

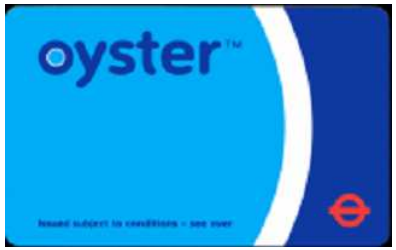
Cloning kit could sell for just £200, says researcher

Robert Blincoe, vnunet.com, 28 Jul 2008

Important Principle:

Making cards much harder to attack:

Diversify all keys for each card



- Done for every Oyster card
- Not done in many other countries, examples:
  - In Kiev, Ukraine, the first block uses the default Infineon key A0A1A2A3A4A5

Hall of Shame (1)

- In Warsaw, Poland, the first block uses the default Philips key FFFFFFFFFFFF,
- Then keys are THE SAME in every card

Hall of Shame (contd.)

- In Warsaw, Poland, the first block uses the default Philips key FFFFFFFFFFFF,
- Then keys are THE SAME in every card
- Moreover keys are NOT random, but human-generated.
  - for example many start with 898989, some end with 898989…
    - obsession with history?
      - in 1989 they had first “free” elections…

Conclusion

Anti-Cloning

- unique hardware serial number

+

- strong cryptography

are the main anti-cloning defences
in today's contact-less smart cards
used in buildings,
public transportation
and for small payments.

Key Management

With the same card

[MiFare Classic, badly broken]
the security can still be

- quite good [London], or
- very bad [Warsaw]:

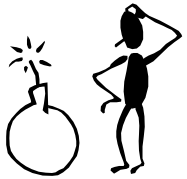
Break once => clone any card without special equipment

Key Management is Hard

Break the reader once
=> clone any card without special equipment…

- Works for HID iClass
  [Meriac 2011]

Help

Most of current cards 

have serious security flaws and need upgrades.

Explosion of hacker attacks:

2008-2012… Most cards are broken…

Cloning equipment is not hard to get…

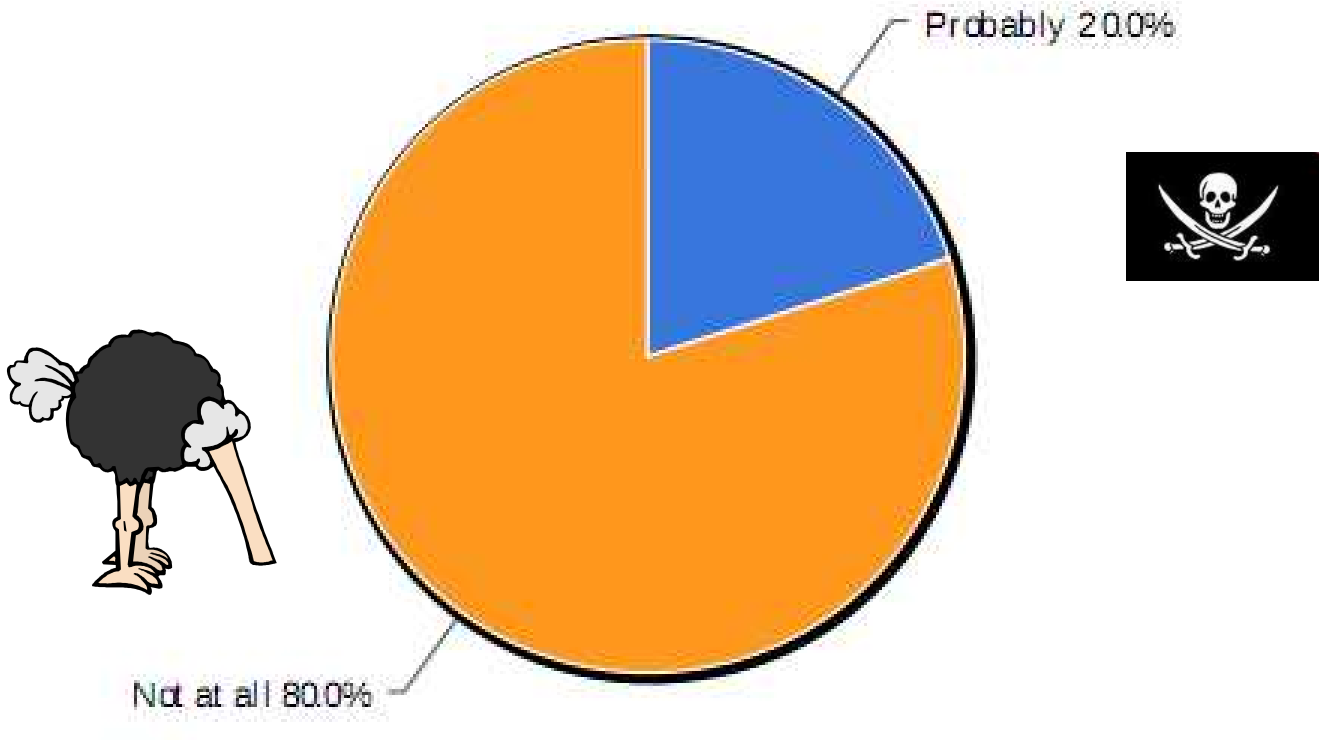
[Proxmark3 etc]

Did anybody notice?

Back to Our UK SURVEY 2012
Building Cards (only)

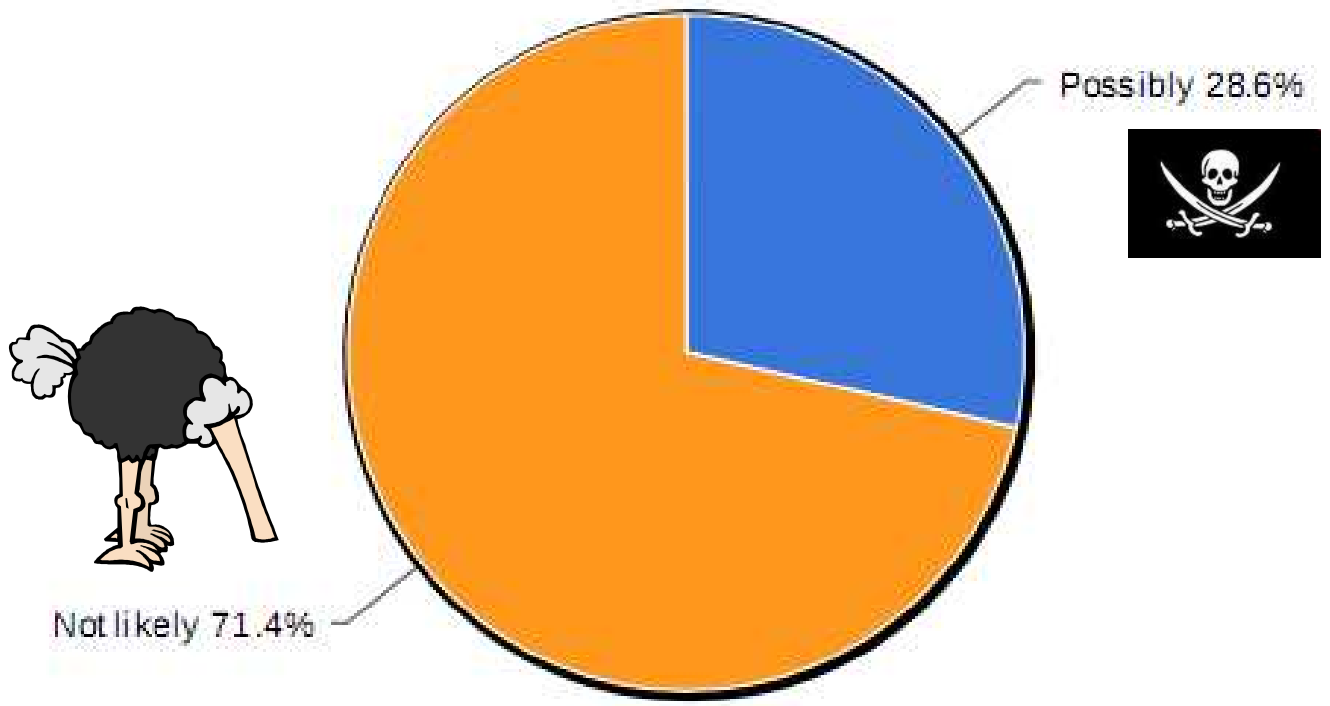
Afraid?Threat?Upgrade?

Has your company already identified a specific security threat which makes you consider that your current smart card systems are inadequate and need to be upgraded in the near future?



Card Cloning Specifically

Do you think your company should use another model of the smart card because you think hackers are already able to clone or simulate your current cards?



Spectacularly Naïve

Customers are spectacularly naïve
about the security of current systems.