



On **Bad Randomness** and Cloning of **Contactless** [Small] Payment and Building Smart Cards

Nicolas T. Courtois¹, Daniel Hulme¹, Kumail Hussain¹,
Jerzy Gawinecki², Marek Grajek³

¹ University College London, UK

² Military Univ. of Technology,
Warsaw, Poland

³ Independent cryptologist and writer



Roadmap

1. Historical background:
from pre-WW2 Enigma cipher clerks to modern passwords
2. Modern methods:
machine generated random numbers.
3. Smart Cards and RFID
4. A bit about HID smart cards in practice...
5. A lot about MiFare Classic smart cards
 - 70% of contactless cards worldwide
 - buildings and small payments)

Why Are We Doing This?

RIBS Project



Partners

Domains

News & Events

Join the RIBS community

Archive Papers

A low-angle, upward-looking photograph of a modern skyscraper with a glass facade, reflecting the sky and surrounding buildings. The image is used as a background for the main text block.

The RIBS PROJECT supports the design of effective and viable integrated security measures aimed at protecting buildings without impacting on their business dynamics

RIBS – Continued...

Domains >

Biological

Chemical

Explosive

Intruders - Insiders

RIBS Events >

JUN 05

Steering Committee meeting

All Day

Latest News >

UCL Computer Science department wins award

In 2012, UCL was one of eight UK universities awarded "Academic Centre of Excellence in Cyber Security Research" status by GCHQ. The department ranks within the top 20 UK university Computer Science departments.

Common Language
=> Crime Scripts
=> Data and Risk Management ...

UCL Datalab – How to share crime data?



Home » Launch of UCL secure data lab & Talk on Big Data

Launch of UCL secure data lab & Talk on Big Data

As you may know, UCL has just spent approx. £1m on helping us create the UCL JDI Laboratory, also known as the secure data lab. We have an INTERNAL launch for the lab scheduled on Wednesday 24 April, 11am-1pm. We now need your help to get as many UCL people (masters students, PhD students, postdocs, UCL staff – but not undergrads) to come to this as possible who have an interest in secure or sensitive data, or 'big data'. We expect interest from all over UCL, not just engineering, so feel free to invite people from other faculties. (Note: This event is not for any non-UCL people – that will come later in the year.)

Could you please (i) register yourself, if you intend to come, on the link below (ii) send the below to anyone you think should be at the event

'Do you use secure or sensitive data?' 'Do you work with 'big data'?'

If so, we would like to invite you to attend the "UCL Town Hall on Big Data"

This event is also the launch event for the UCL JDI Research Laboratory, a new £1m facility to be launched at UCL in the summer of 2013. The facility is a secure data analysis centre that allows sensitive and confidential datasets to be brought into the university so that they may be worked upon by researchers in a secure, controlled environment.

Date: Wednesday 24 April, 11am-1pm

Venue: Roberts G08, ROBERTS BUILDING, TORRINGTON PLACE, LONDON, WC1E 7JE

If you work with or have an interest in working with large datasets, particularly those that are confidential or sensitive, then we would like to hear about your research, and to introduce you to the new UCL JDI Research Laboratory.

11.00 – Arrival

11.05 – Introduction to the new UCL JDI Research Laboratory by Prof Richard Wortley, UCL Security and Crime Science

11.20 – Talk on "Big Data" – by Dr Daniel Hulme, UCL Computer Science

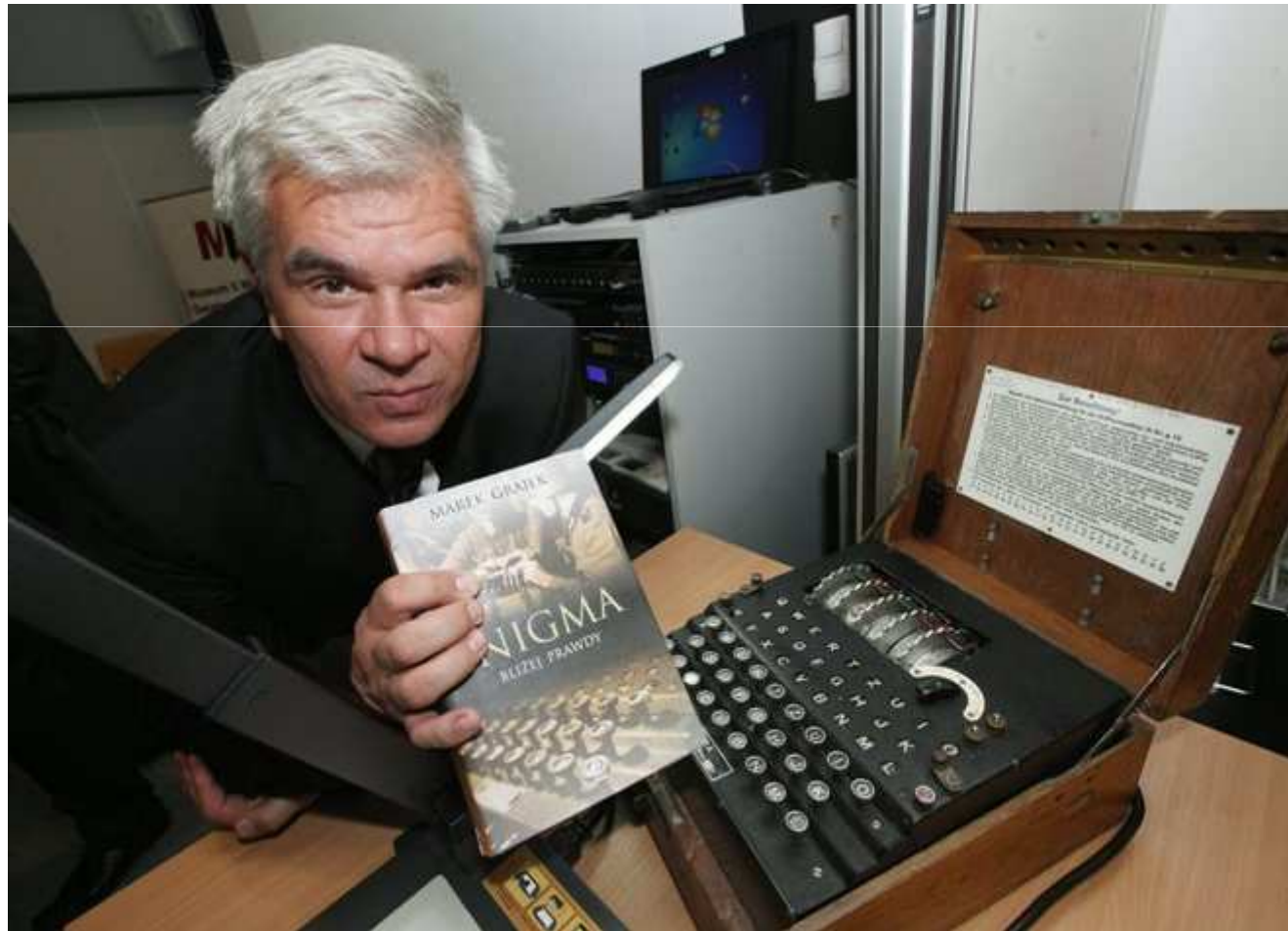
UCL Smart Cards Lab



- COMPGA12 **Applied Cryptography**:
- We run a **Smart Cards Lab** for students.



Who Said That History Does Not Repeat?



Before WW2 - Patterns in Message Keys

(should be 3
random letters)

~~AAA~~

~~XYZ~~

~~ASD~~

QAY



Operators always found a way to «degrade » their security

Old Stuff?

Not quite.

This is still happening
every day as we speak..

Modern Passwords

Main insight:

these mistakes do not die, they live forever,

=>absolutely EACH AND EVERY of these common mistakes or patterns is still present TODAY as a distinct patterns in real-life probability distributions on human-generated passwords.

Examples:

8.5% of people use 'password' or '123456'

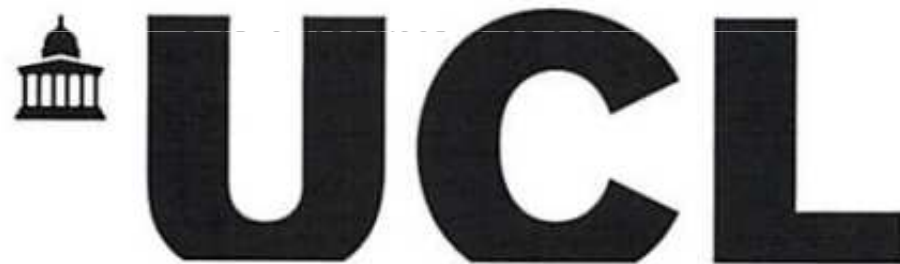
91% of people use one of top 1000 passwords

[source: xato.net]

Password Cracking – Our Experience...

UNIVERSITY CIPHER CHAMPION

March 2013



This certificate confirms University College London as the winner of
Cyber Security Challenge UK's first University Cipher Challenge 2013.

Bad News

These mistakes they live forever,

Need:

machine generated passwords
and random numbers (e.g. cryptographic keys)

Problem:

are they really random?

Smart Cards



Scope:

Most Popular Contact-less Smart Cards

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



Their Security with focus on faulty
Random Number Generators (RNG)
and impact on card cloning.

Why Card Cloning?

Main attack:

- ⇒ Does ALWAYS work, even though the system is online
- ⇒ Half of the time it will be the legitimate user who will be rejected or accused of fraud...



Important Buildings

Remark:

I wouldn't care that much about hackers that get free rides on the Tube.

- What about the UK Cabinet Office, big banks, etc...
 - It seems that most buildings actually use MiFare Classic (**70 %** market share)
 - Many other use **even less secure** Low Frequency systems which can be recorded and replayed (no cryptographic authentication).



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 developers...



RFID

This model somewhat breaks apart
with RFID smart cards...

RFID => no user control.



Bug Or Backdoor?

The security perimeter splits that occur in smart cards have a double effect:

- they can prevent one entity from compromising other people's security... hardware barriers can be very effective
- they can also conceal a subversive functionality:
 - A bug, backdoor etc.

Schneier-Shostack'99 advocate more transparency...

But secrecy is here to stay!

open source == utopia and a fallacy, helps criminals

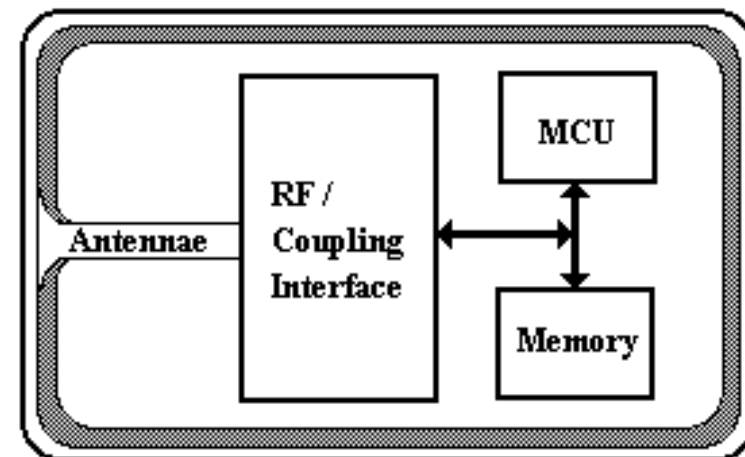
Crypto Subversion

The hidden powers of crypto developers are particularly dangerous:

- **large scale** compromise
- impossibility to prove the intent: **perfect crime**
- impossibility to prove fraud:
 - **no forensic traces whatsoever** if I update your card wirelessly with a monthly ticket / parking credit, perfect **fraud**.

Contact-less Smart Card

- with RF transceiver
- 0.1 s transaction
 - tiny computing power to implement (costly) cryptographic authentication...



Form Factors

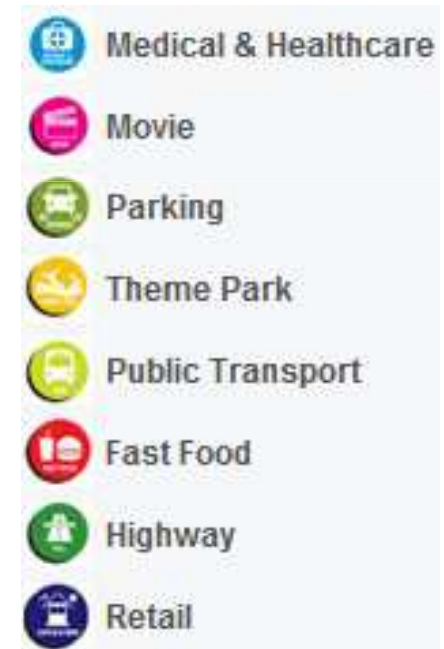


key fob



corporate badge

Building Transport and Small Payments



Malaysia
(MiFare Classic !)

Transport Card Systems

Main Standards:

- Calypso
[France, Belgium]
- MiFare
[UK, Holland, Poland,
Ukraine, U.S., Etc..]
- Other standards exist.
In Asia: e.g. Felica
[Japan, HongKong, etc..]



Building Cards – Business Issues



Building Cards – Business Model

B2B Model:

Example: banks in a given country will typically have a choice of VERY FEW companies (system integrators) which provide security systems with smart cards, badge printers, software, back-end systems, CCTV cameras, door locks etc.

Is it good or bad?

Interesting Advantage

1. Good: in one country one CAN impose higher security standards...

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.

Building Cards





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:

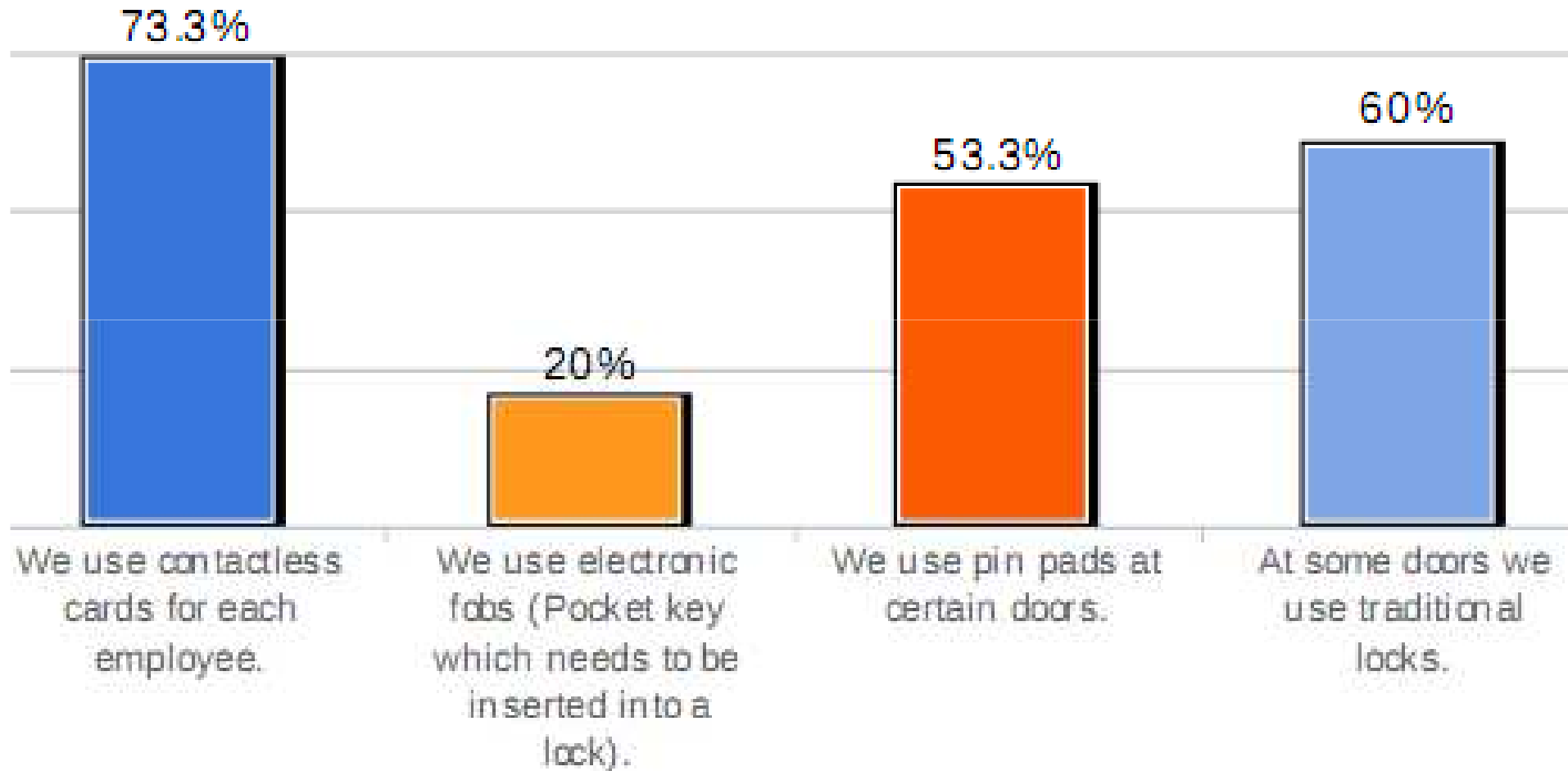
Master Thesis by Ayoade Adebanye,
M.Sc. Information Security,
University College London, September 2012



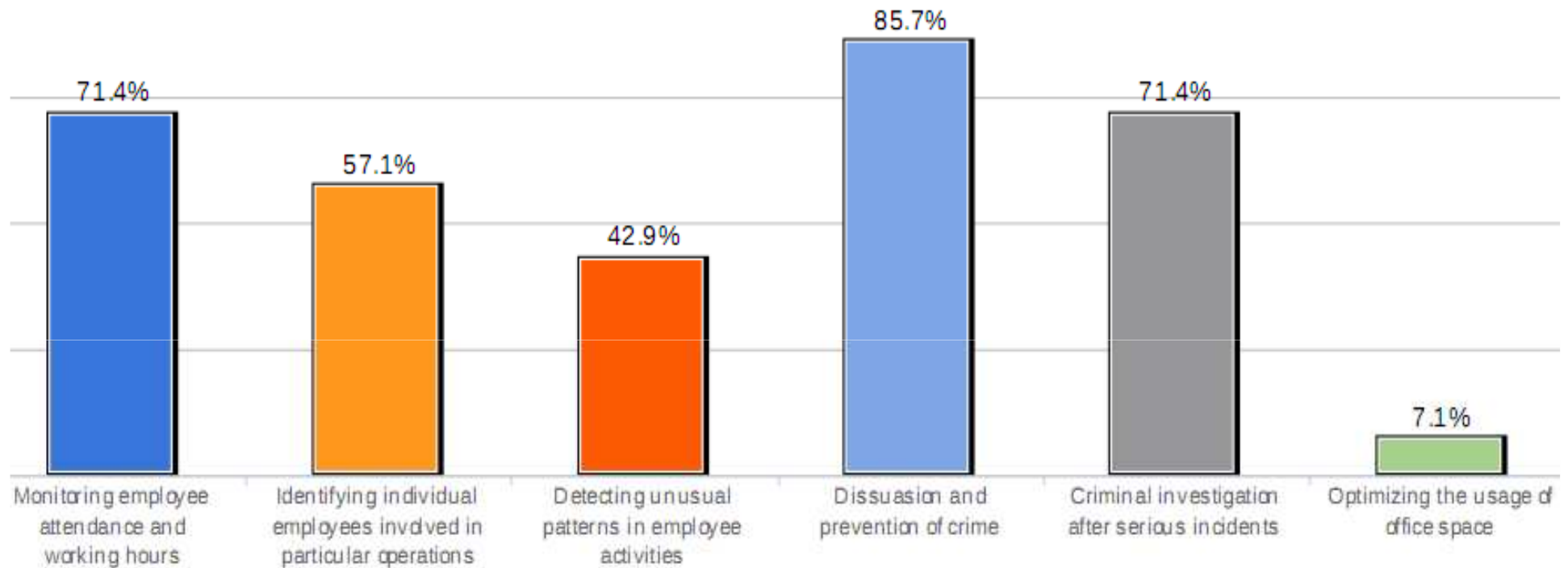
Key Findings



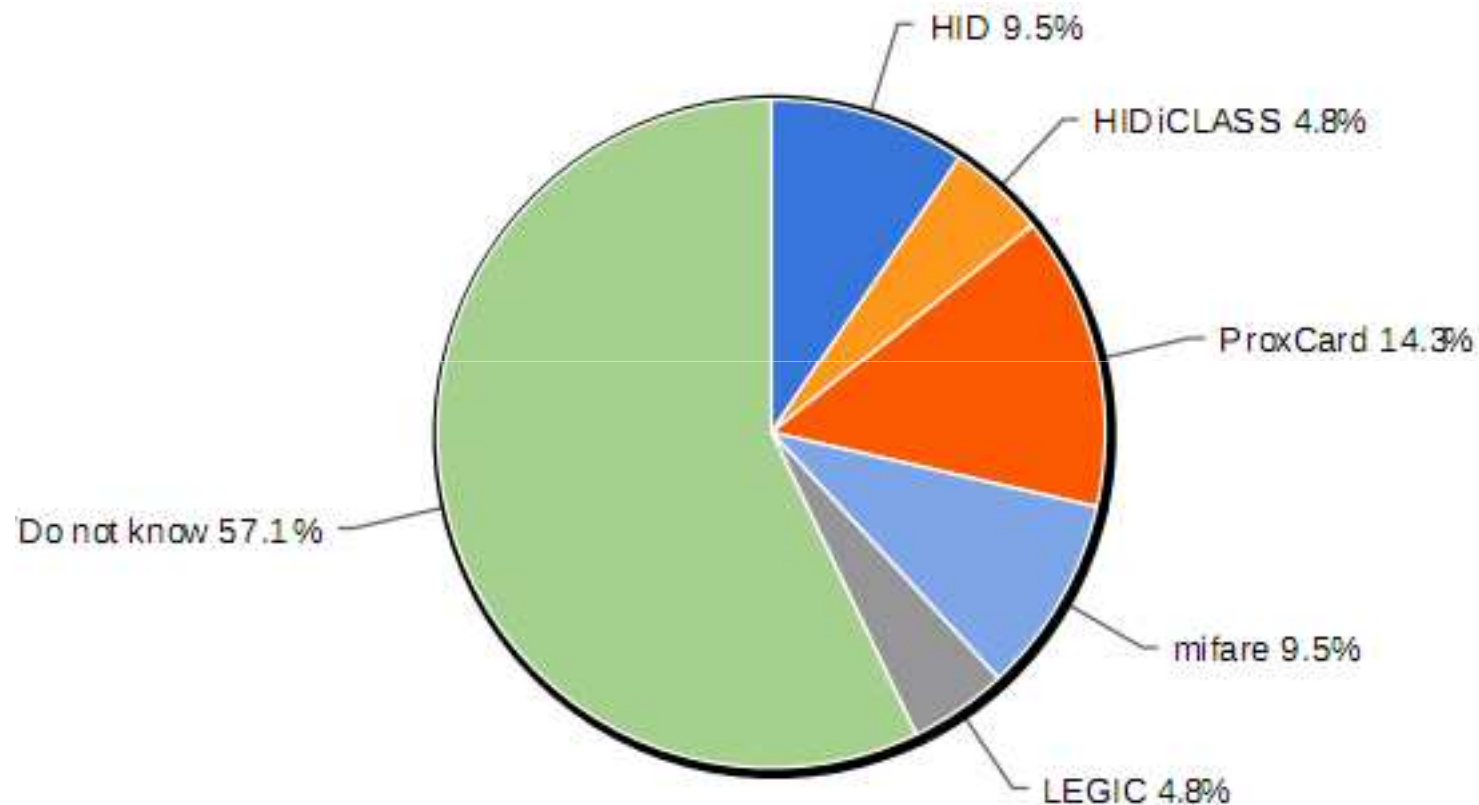
Smart Cards Are Popular in the UK



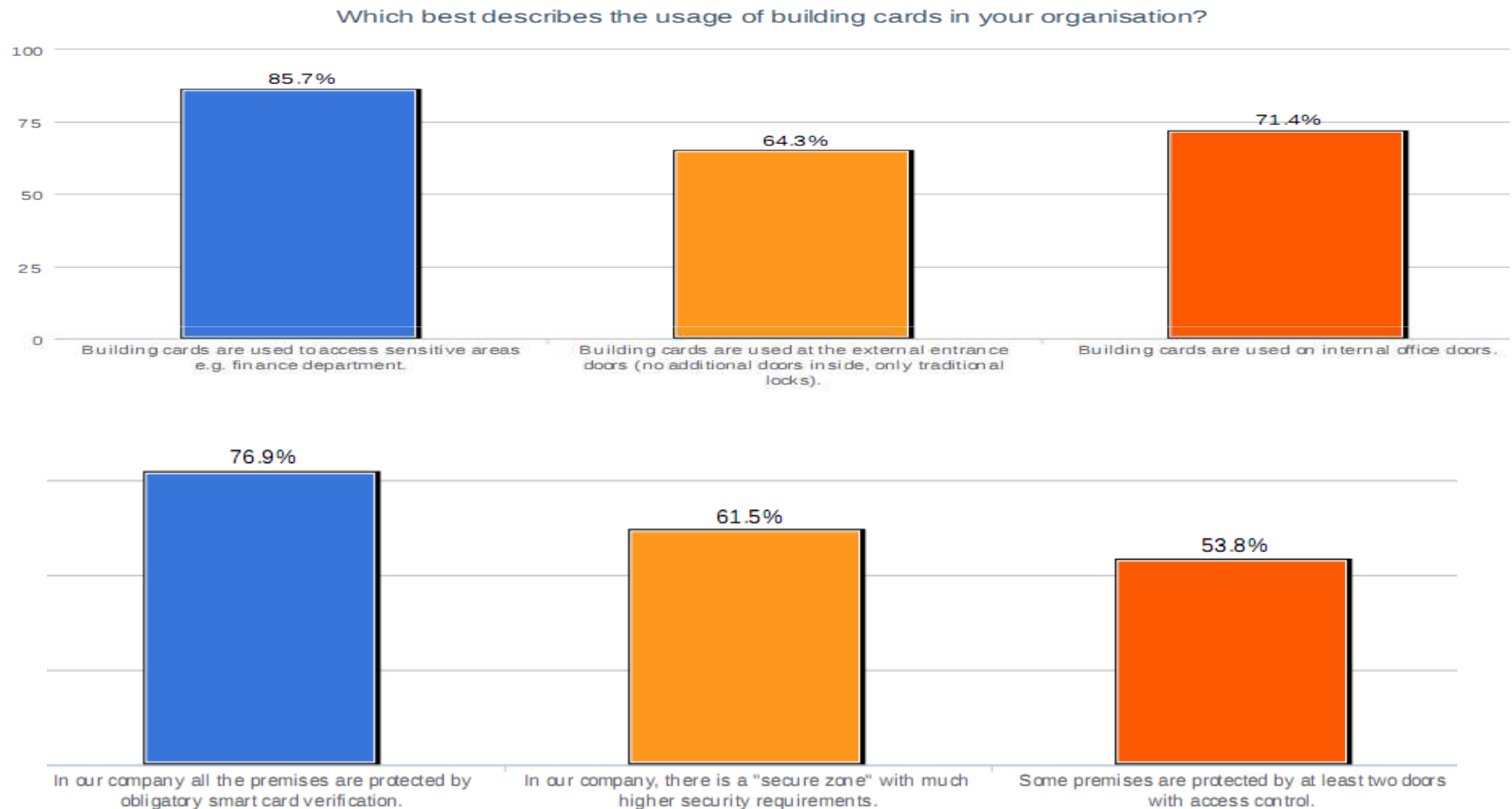
What Do We Need These Systems For?



Not Know / Not Care / Obscure Reseller Brand



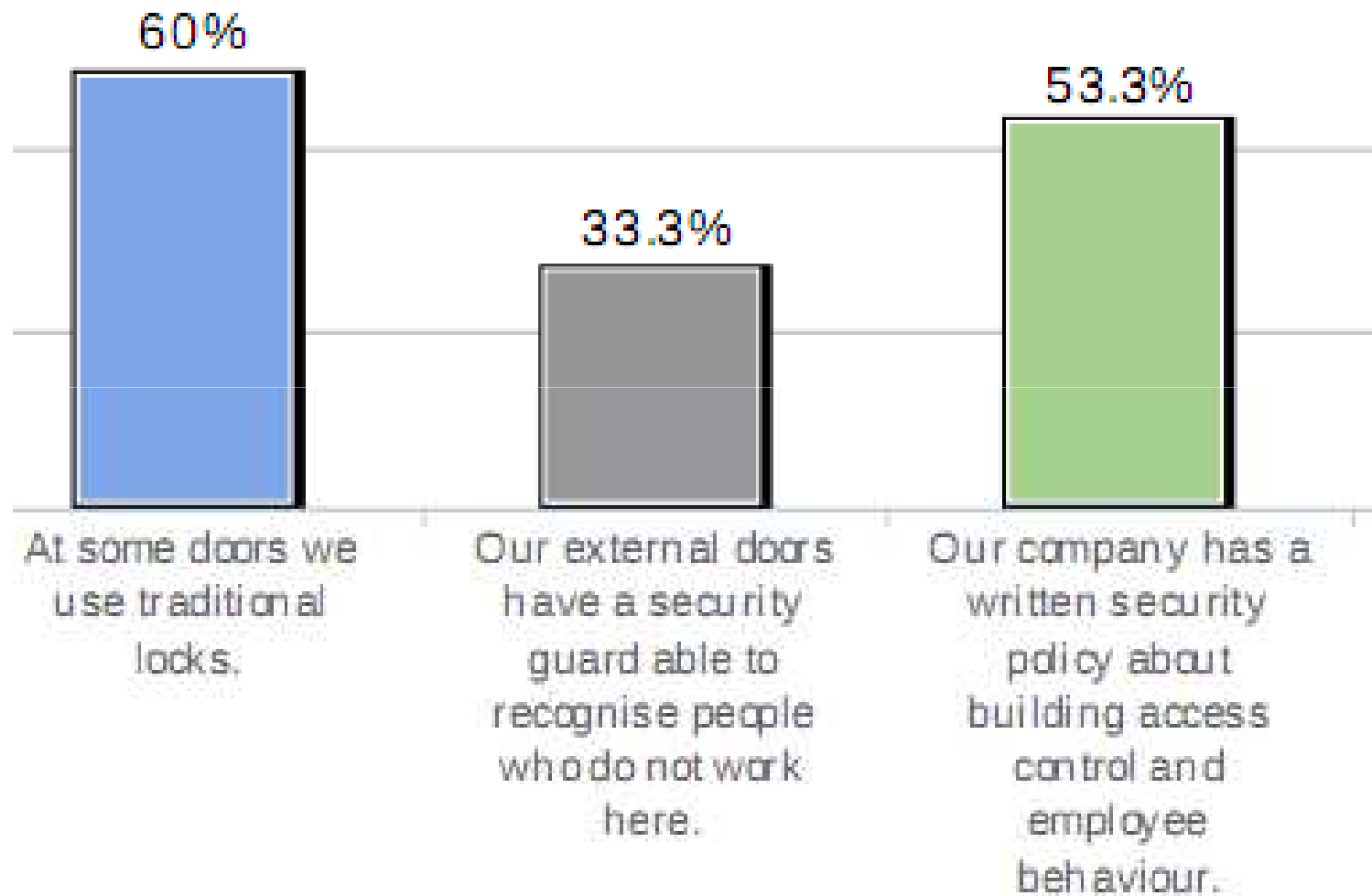
Areas/Doors



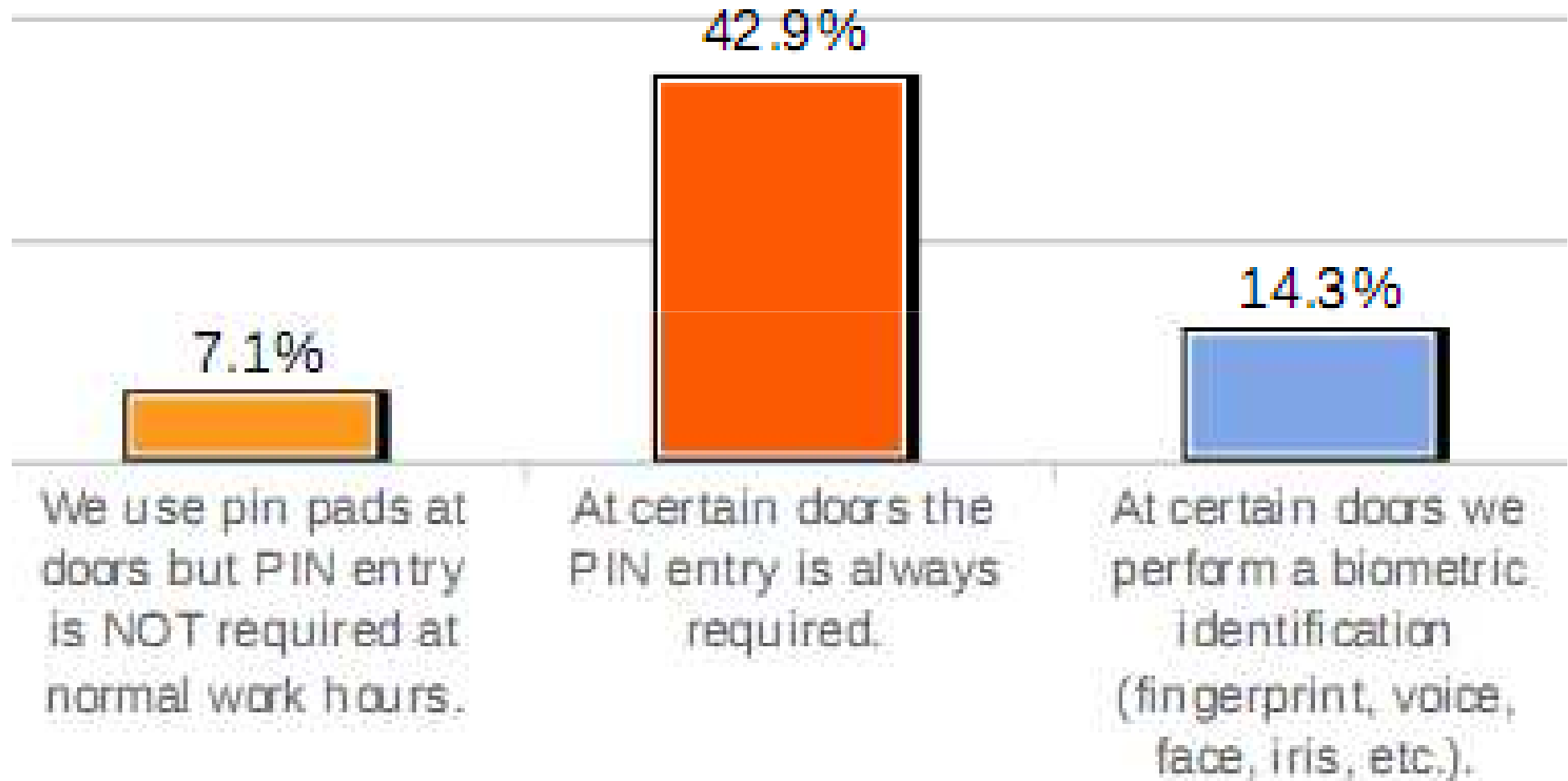
Security in Place



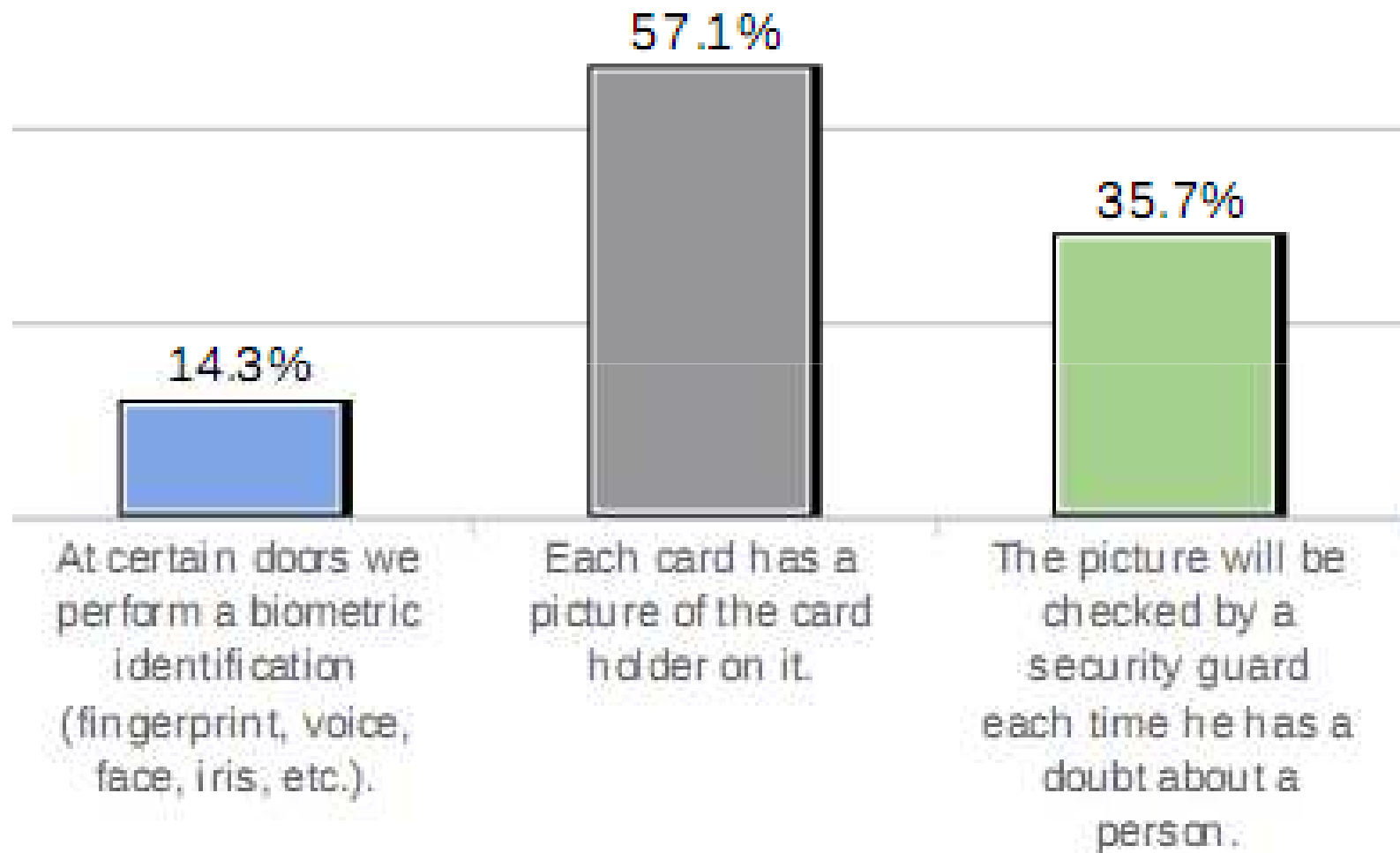
Cards + Extra Security



Card + PIN?



Biometrics



Building/ID Cards Security, Cloning, Etc..



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.

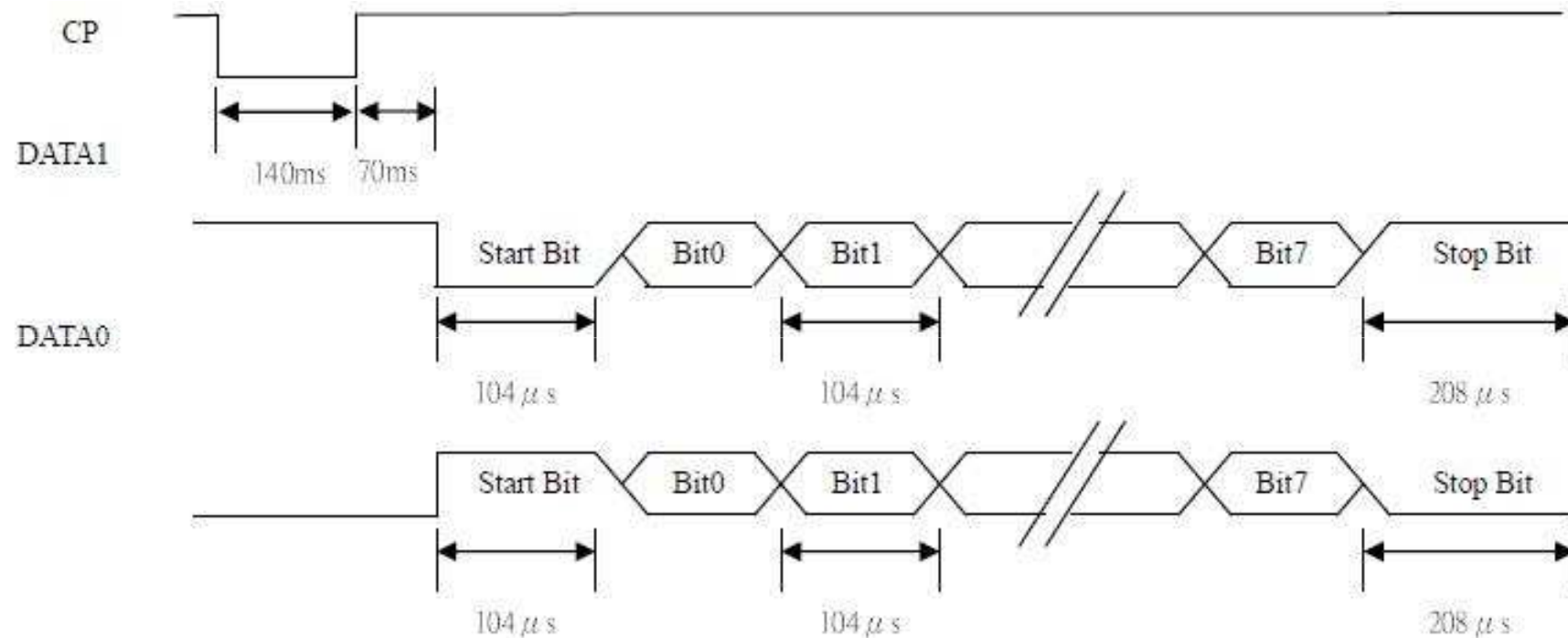
Building Cards – 2 Types

- **RFID** cards: Broadcast unique serial number
- More advanced cards with **cryptography**.

Wiegand Interface

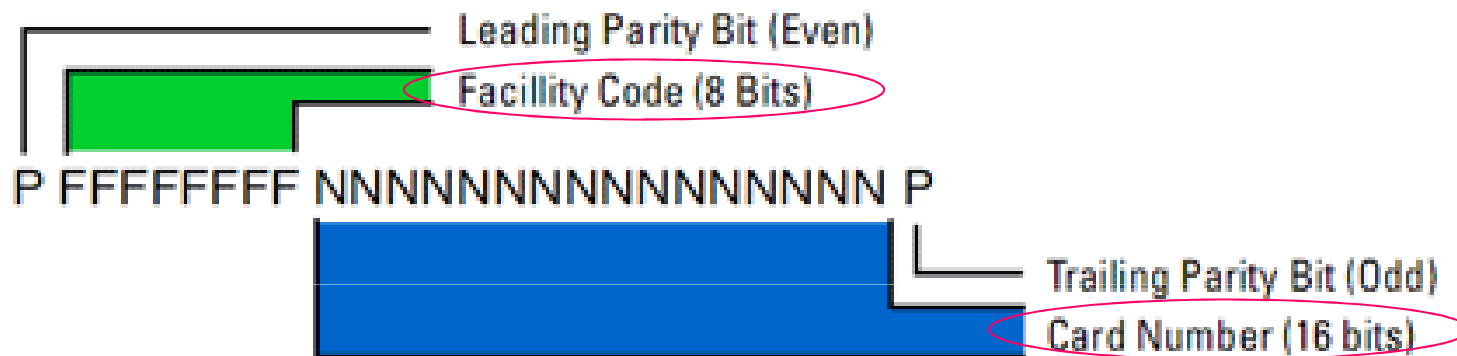


2 Wires



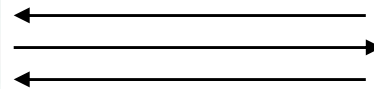
26-Bit Wiegand Format

"Standard" 26-Bit Wiegand Format

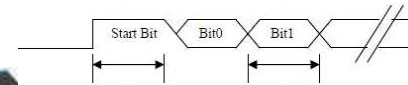




Wiegand “Loophole”



may be
secure..



26 bits

cannot be
very
secure!

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

Fact:

Neither the facility code 8 bits nor card number 16 bits are random in practice.

Their entropy is very low.

Example 1

We have compared

- a few HID iClass cards which are sold to individual users of laptops
- one Prox card from a bank.

To our horror both cards had the same facility code!

Example 1 – contd.

Laptops card vs. a card from a bank.

- same facility code
- Are serial numbers on 16 bits distinct?

Not at all, the difference was about $100 \ll 2^{16}$

By birthday paradox we expect collisions to occur purely by accident if we have just 10 people:

=> enter the bank with the card from your laptop...

=> no proof that this works but it should.

Example 2

Cards from an airport in a EU country.
Even though they have a very standard facility code
(which is likely to repeat elsewhere),
the entropy of the serial numbers seems to be at least
12 bits out of 16.

Example 2 – contd.

Unfortunately these numbers were **consecutive** for different cards.

- This decreases the amount of data which may be available to forensic investigators.
- The attacker could easily copy a card of one employee, modify the number within a certain interval, obtain another valid card, and penetrate into the building without leaving any traces and without the possibility to connect this incident to any concrete card belonging to a concrete person.

Cryptographic Cards



Building Cards – 2 Types

- RFID cards: Unique serial

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

Barriers For Attackers


For many smart card products:

- The spec of the product is secret
- The protocol is secret
- The cipher is secret.
- The vulnerabilities (or backdoors..) need to be discovered one by one...
- Recover the key of each card
- Then we can:
 - read the data
 - clone / simulate the card
 - travel for free/enter the building...
 - or publish the result

start
work



can be
very
complex



Contact-less Authentication - History

IFF: Identify Friend or Foe (1942)

Challenge-



-Response

British WW2
invention!

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	



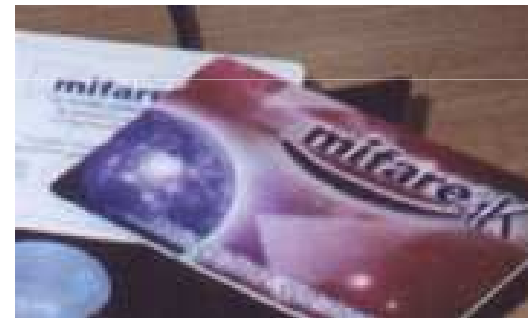
Confidential crypto algorithm is implemented inside the reader, the developer will totally **ignore** it and may think that the security is very high, or very low, there is no way to tell!

Most Popular Models [UK and worldwide]

- RFID cards: Unique serial



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



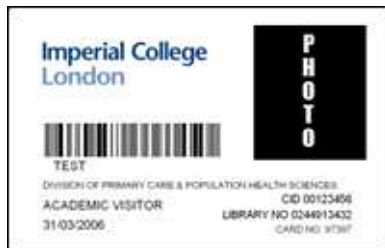
Legic



prime



advant



Main “Crypto” Cards



MiFare Classic:

- >1 billion of these cards sold!
- 70 % of the contactless badge/ticketing market
- London 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.

Legic

Old model: early 1990s:

So called “Legic Encryption claimed”.

Later found to be totally bogus:

- Cf. Nohl and Plötz, cf. CCC’2009 conf. In Berlin
- No security at all.



New models: since 2000s:

- Serious crypto: 3DES or AES. No attack 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.





Clone Attacks

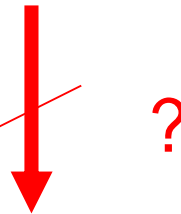
Cloning the Card

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.



Card Simulation

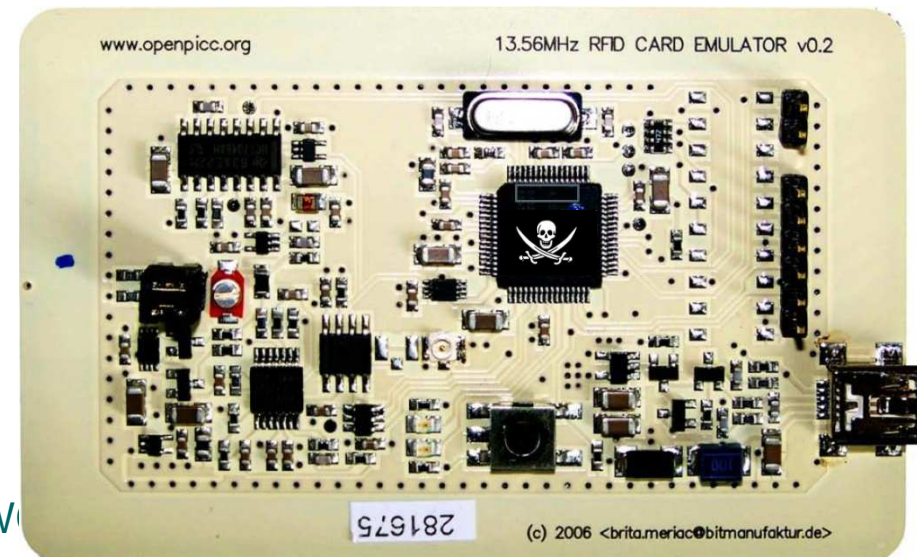
MiFare Classic in sector 0.

Cannot be changed, not even
by the manufacturer.

The only security in
many building systems...

[Cambridge,
Imperial, UCL, etc.]

Attack:
card simulation



Blank card?

re-program the card?

Sometimes it is possible!



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, 300M sold]



- **Crypto** cards
 - Mutual Authentication
 - Encryption of Data

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



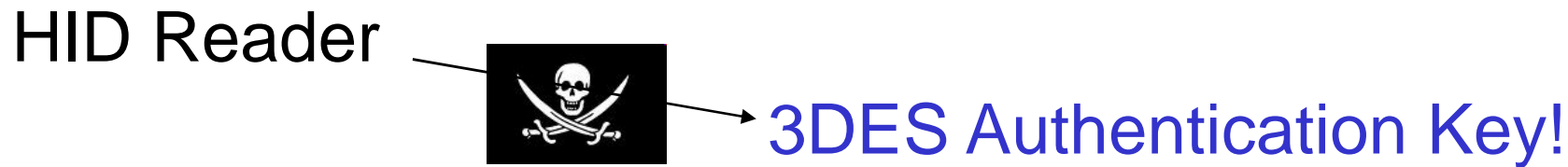
*Hacking iClass Readers [2010]

Steps:

1. Get just one **genuine** reader like RW400 [100 GBP].
 - we were able to get one easily
2. Produce a custom debugging interface.
3. Execute 2 separate software exploits
4. The code contains 3DES keys in cleartext.
5. These keys are already in possession of hackers...
cf. Meriac, CCC 2010.



Hacking iClass Readers [Dec 2010]



[Meriac CCC 2010]

Chaos Communications Congress,
by far the biggest hacker event in Europe,
>3000 participants...

Hacking iClass Readers [Dec 2010]

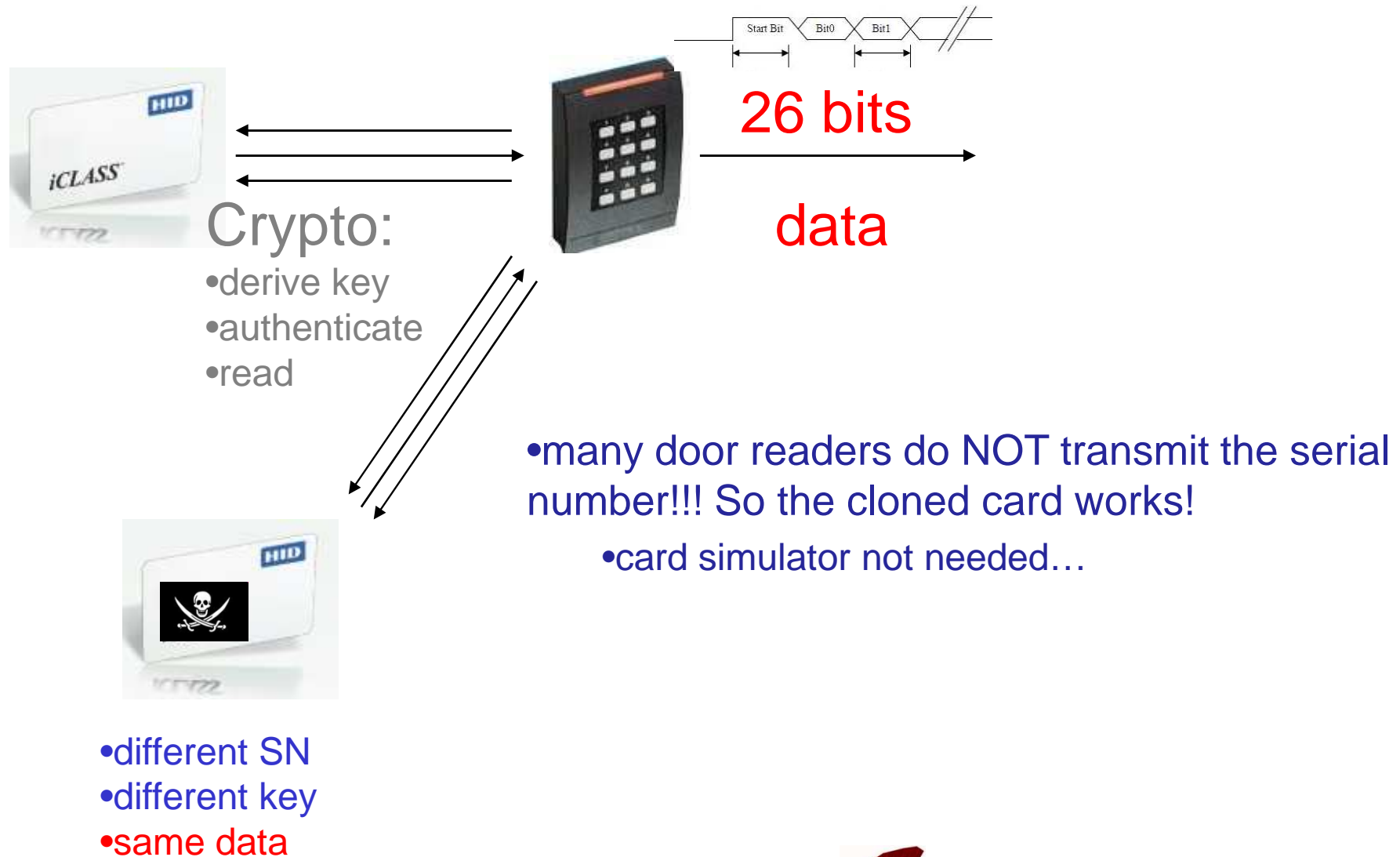


3DES Key!



- 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 !



What Makes Cloning Harder?

and how to get around it

What is My Anti-Clone Functionality?

- RFID cards: Unique serial

Crime Scripts – Cloning [1]

- RFID cards: Unique serial

– in hardware, **CANNOT** be changed

record and
decode

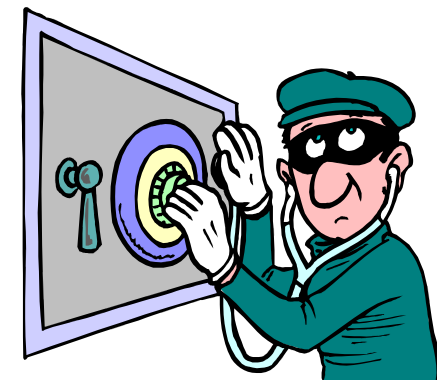
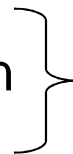
use a
card simulator



What is My Anti-Clone Functionality?

- RFID cards: Unique serial

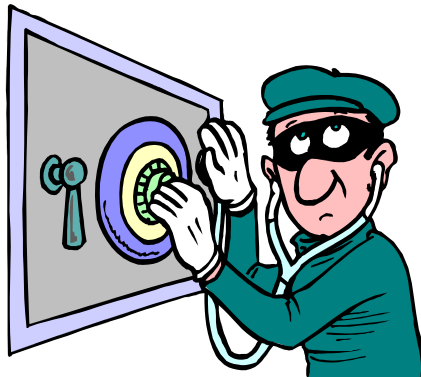
- Crypto cards
 - Mutual Authentication



extract keys?

Crime Scripts – Cloning [2]

- **Crypto** cards:



extract keys!



read the data



simulate

Defence in Depth Principle

Learn from the Military:
layer the defences.



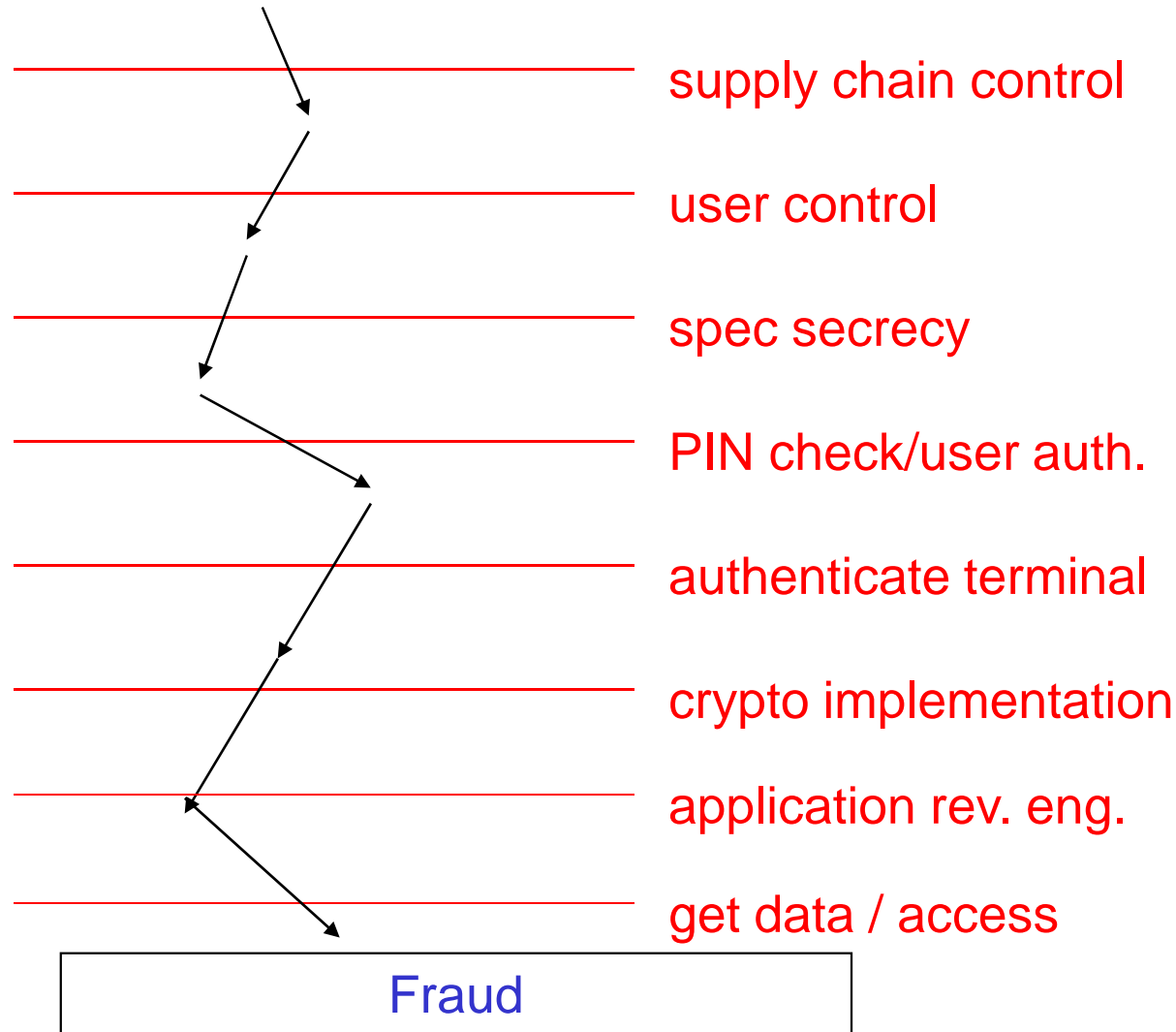
MiFare Classic Crypto-1

Stream cipher used in about 200 million RFID chips worldwide.

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



Defenses of Smart Cards



Crime
Script

Not Like This – USB Port

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	FFFFFFFFFFFFFF

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.

Can be done with ACR122, the cheapest reader on the market.

C++ + nfclib + ACR122

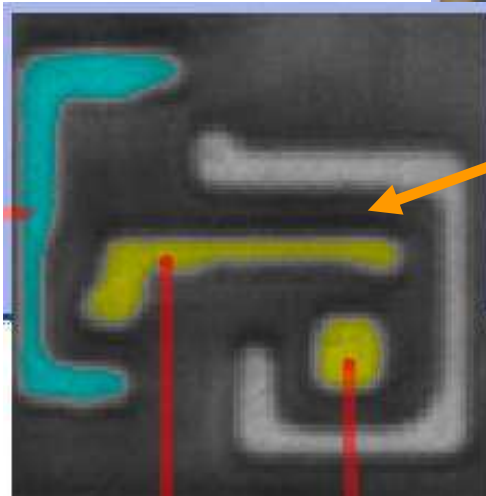
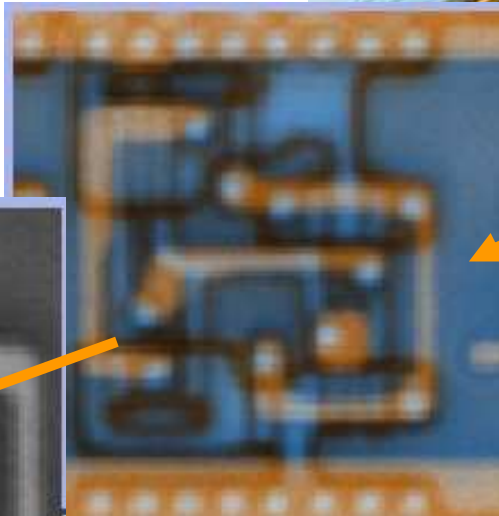
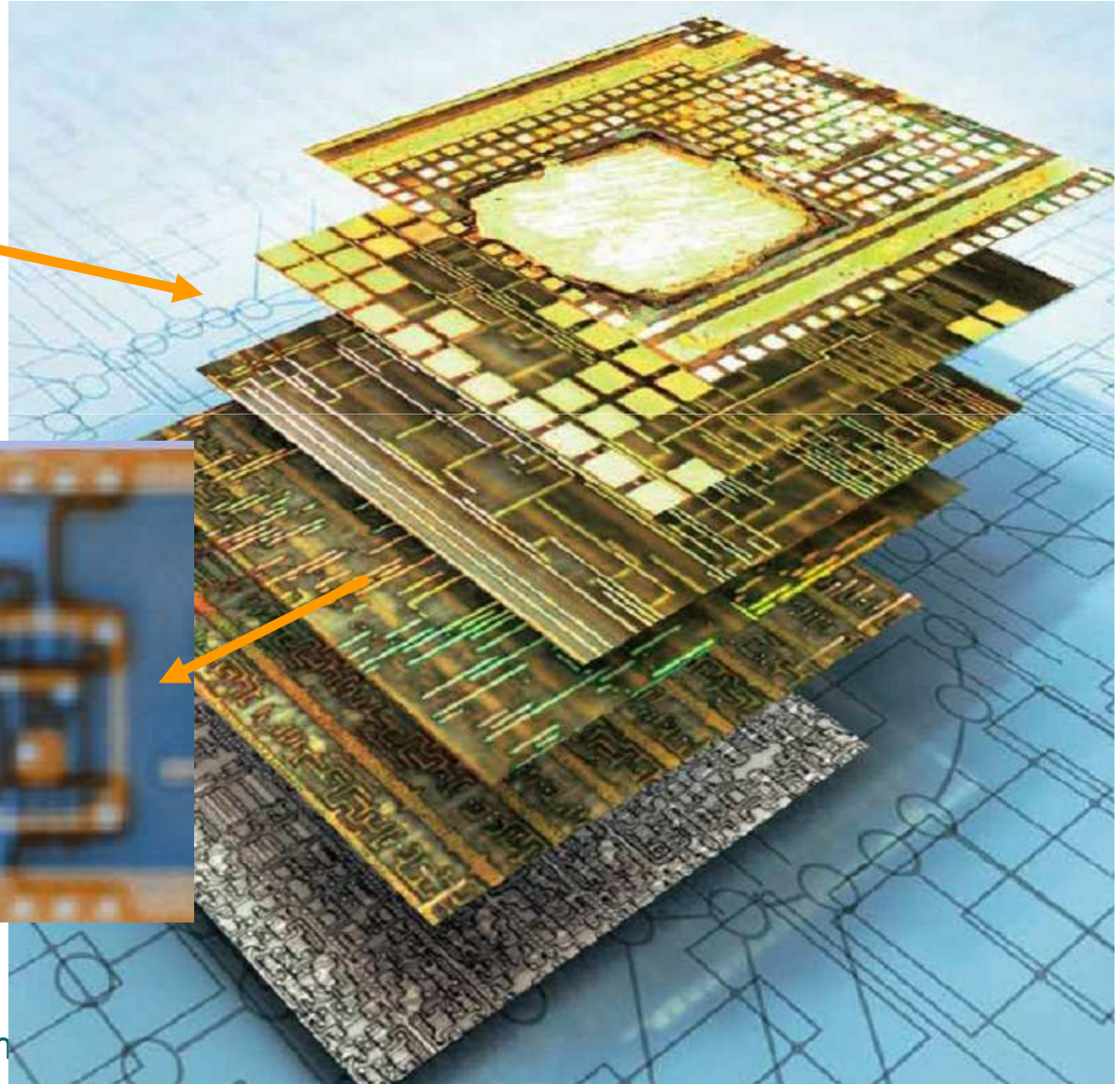
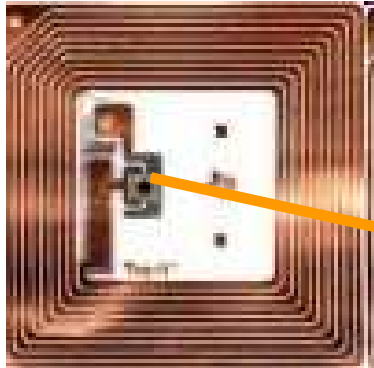
Example:

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

UID

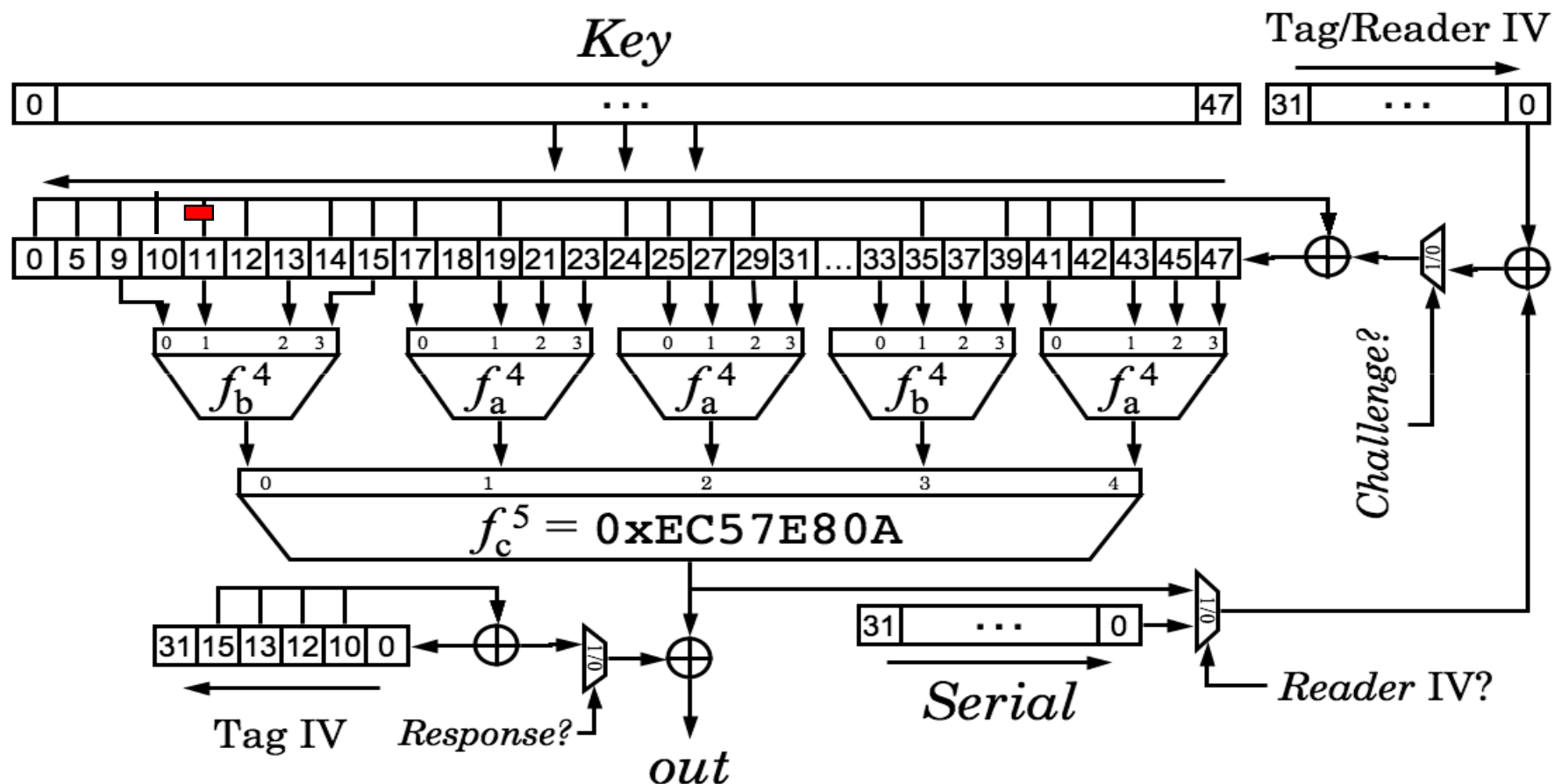


Reverse-Engineering [Nohl et al.]



Grajek Hulm

Crypto1 Cipher



$$f_a^4 = 0\text{x9E98} = (a+b)(c+1)(a+d)+(b+1)c+a$$

$$f_b^4 = 0\text{xB48E} = (a+c)(a+b+d)+(a+b)cd+b$$

Tag IV \oplus Serial is loaded first, then Reader IV \oplus NFSR

Waste of Silicon

Internal bits are computed 2-3 times.

One could save half of the gates!

And terrible weakness: super-strong self-similarity.

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

Key Size = 48 Bits

Claim: 48 bits can still be
a SECURE key size in 2010.

- in authentication only:
 - extra randomness effectively prevents brute force attacks!

So brute force attacks are infeasible

WHAT???? Yes.

Brute Force?

- Requires recorded communications with a genuine reader.
- The hacker must already penetrate into the building.
- **Small window of opportunity.**
- CCTV is usually present
- other monitoring techniques...



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

The real security question is:

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

The attacker needs to sit next to the victim for a number of seconds / minutes.

- On a train, on a plane...

Then the hacker steals your identity:
make a clone of your card,

- and later penetrate the building.
- or re-sell the working card to a petty criminal

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...)



Brute Force 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 \Rightarrow 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

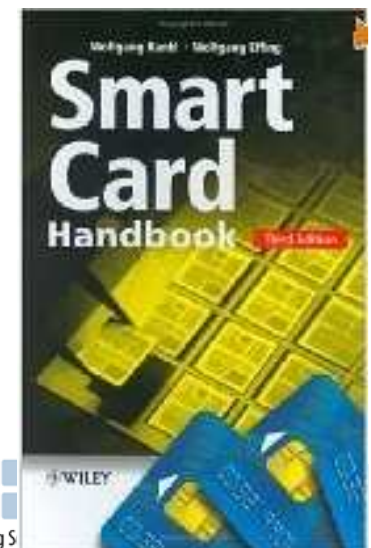
Secure Hardware Dev. Management

[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 not 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.

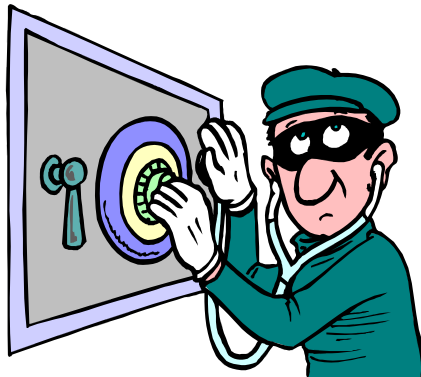
But in fact Dutch and German researchers knew about it already...

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: SECRIPT 2009, see also eprint.iacr.org/2009/137/

Hack it at home:

step by step instructions:

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



Embarrassing Discoveries

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

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/>

Why Russia and India have manufactured smart cards for which

- the spec was NOT publicly known
 - are NOT widely used in Russia/India?
 - 200 millions of these cards are in circulation worldwide
 - They did not advertise their hacking exploits, did not advertise their products either.
- Rumours:
some of these cards
would allow one to change
the unique serial number
and be fully reprogrammed
to emulate any other card...





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 software...

Best Attack Speed

Use 'Courtois Dark Side' attack for one sector.
Then use Nested Authentication attack
[Nijmegen Oakland paper] for other sectors.

- >10 minutes with our current equipment.
- Should take **10 SECOND TOTAL** with a better implementation.
 - Example: Proxmark3 can then directly be used to act as a clone.

Is It Really Feasible?

It isn't. Or it is.

The devil is in the details.

=>This motivated this paper.

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



Key Management

With the **same card**

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

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

Break card once => clone any card
without special equipment



DOES THE Courtois Dark Side Attack ACTUALLY WORK IN PRACTICE?

Innocent Assumption...

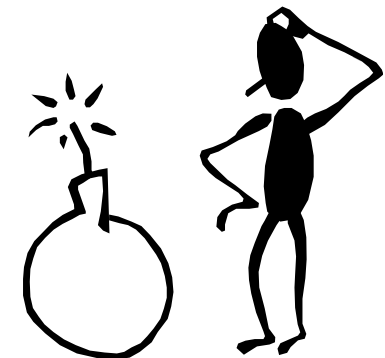
In Usenix Security 2008

Nohl, Evans, Starbug, and Plotz claimed that a **strict control of timing** allows either to **predict** the card random at a moment in time, or even to **produce the desired random** at will for the attacker.

We say “claimed” because our investigation never fully confirmed this!

Is The Assumption Correct?

Without this assumption our attacks fail!



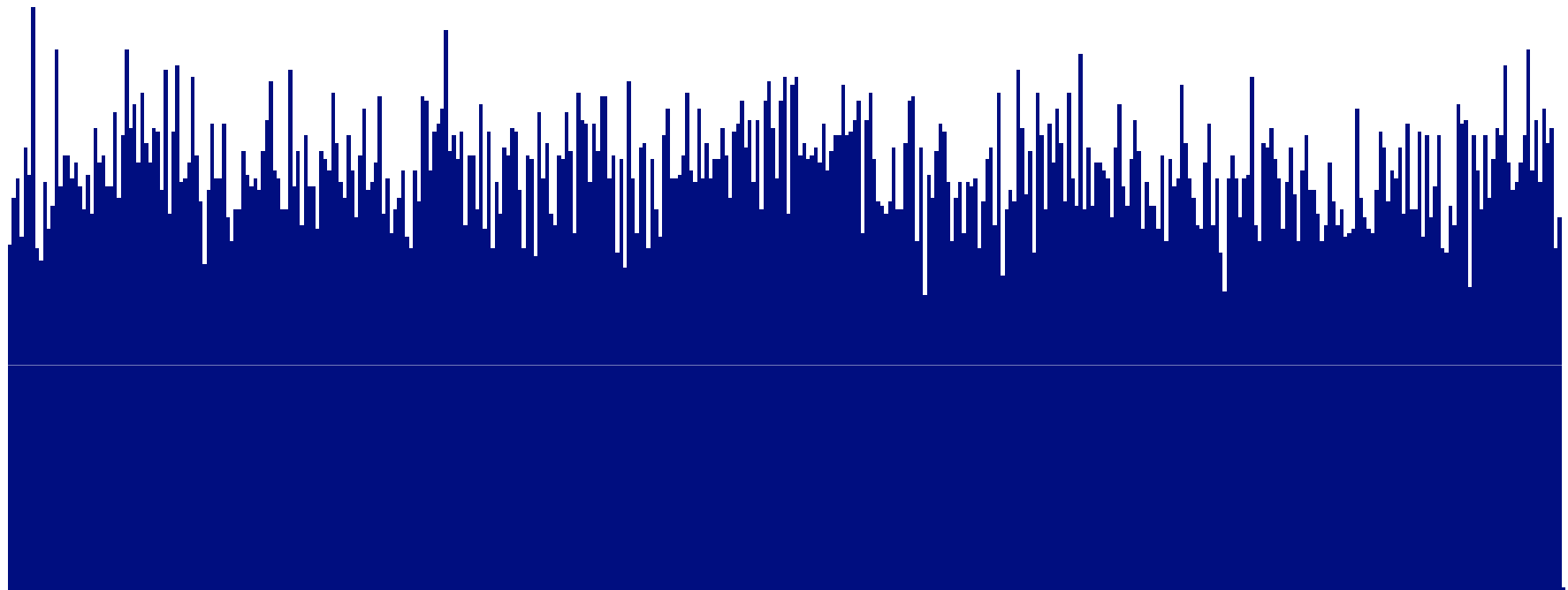
Facts:

- There are only 2^{16} randoms instead of 2^{32} .
- Somewhat deterministic as $f(\text{time})$...

Further claims:

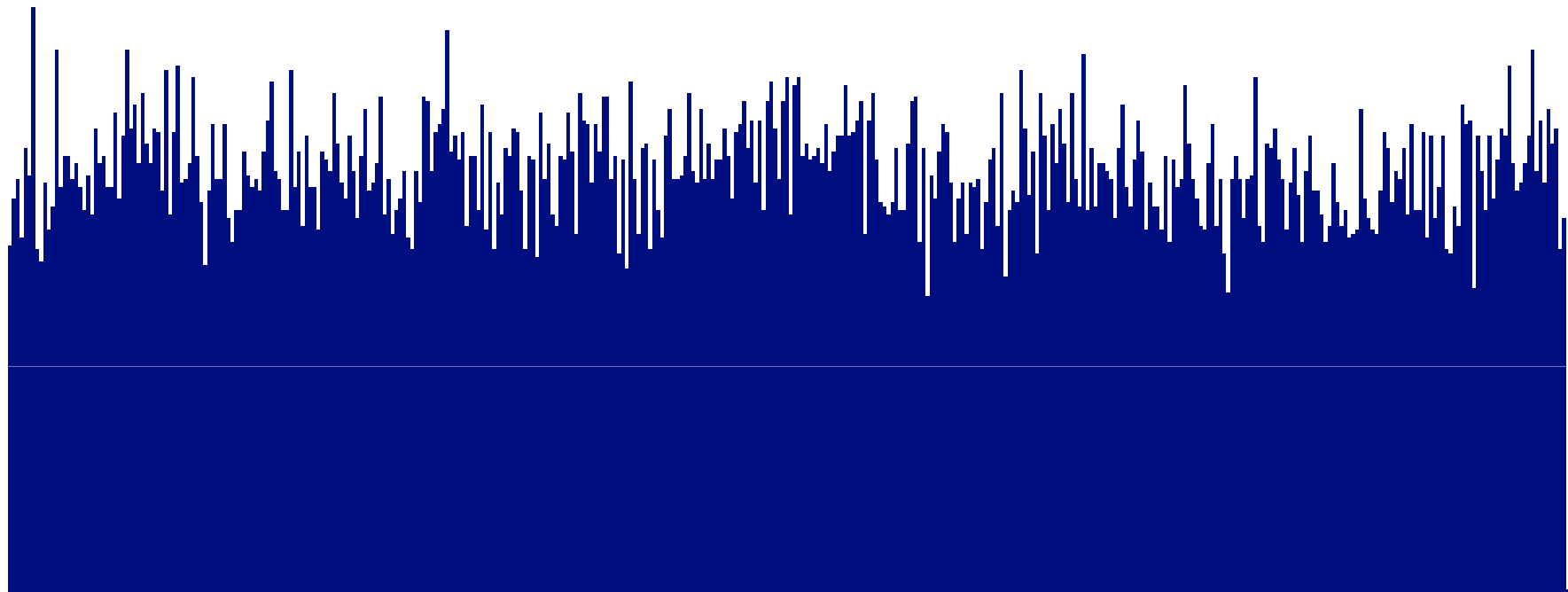
- The connection polynomial of the LFSR is claimed to be $x^{16} + x^{14} + x^{13} + x^{11} + 1$. Interestingly it could be different in different cards.
- Further, it is claimed that the clocking is regular and the LFSR is clocked at 106 kHz and wraps around every 0.6 seconds, after generating all 65,535 possible output values.

Experiment 1 – London University Card



- Looks nearly random
- We prove it is not random, see the paper.

Hard to Break...



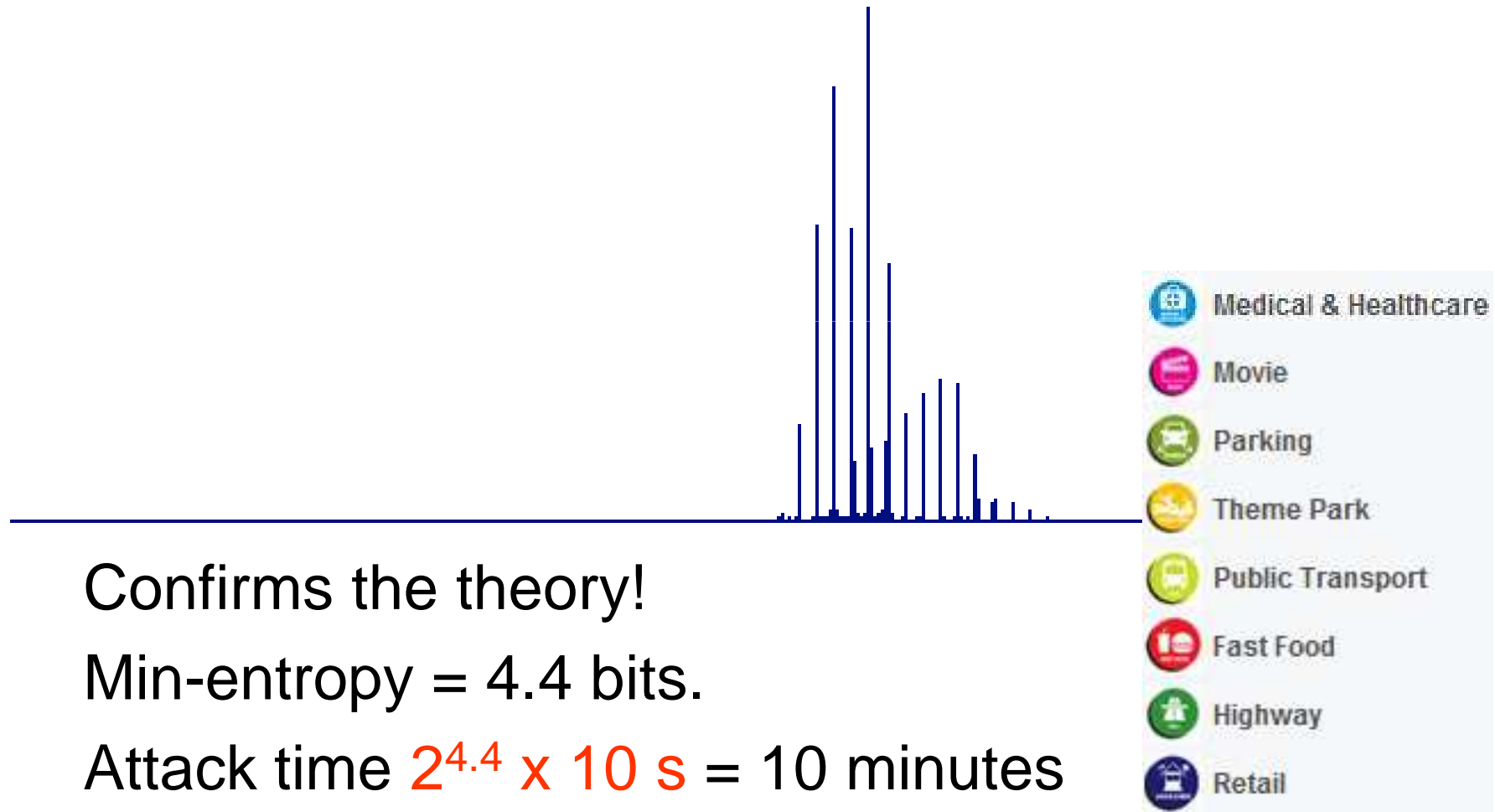
- Min-entropy = def=
 $\log_2(\text{most likely card random}) = 12.4 \text{ bits}$
 \Rightarrow Attack takes very roughly $2^{12.4} \times 10 \text{ s} = 1 \text{ day/key}$.

Does It Confirm The Theory?

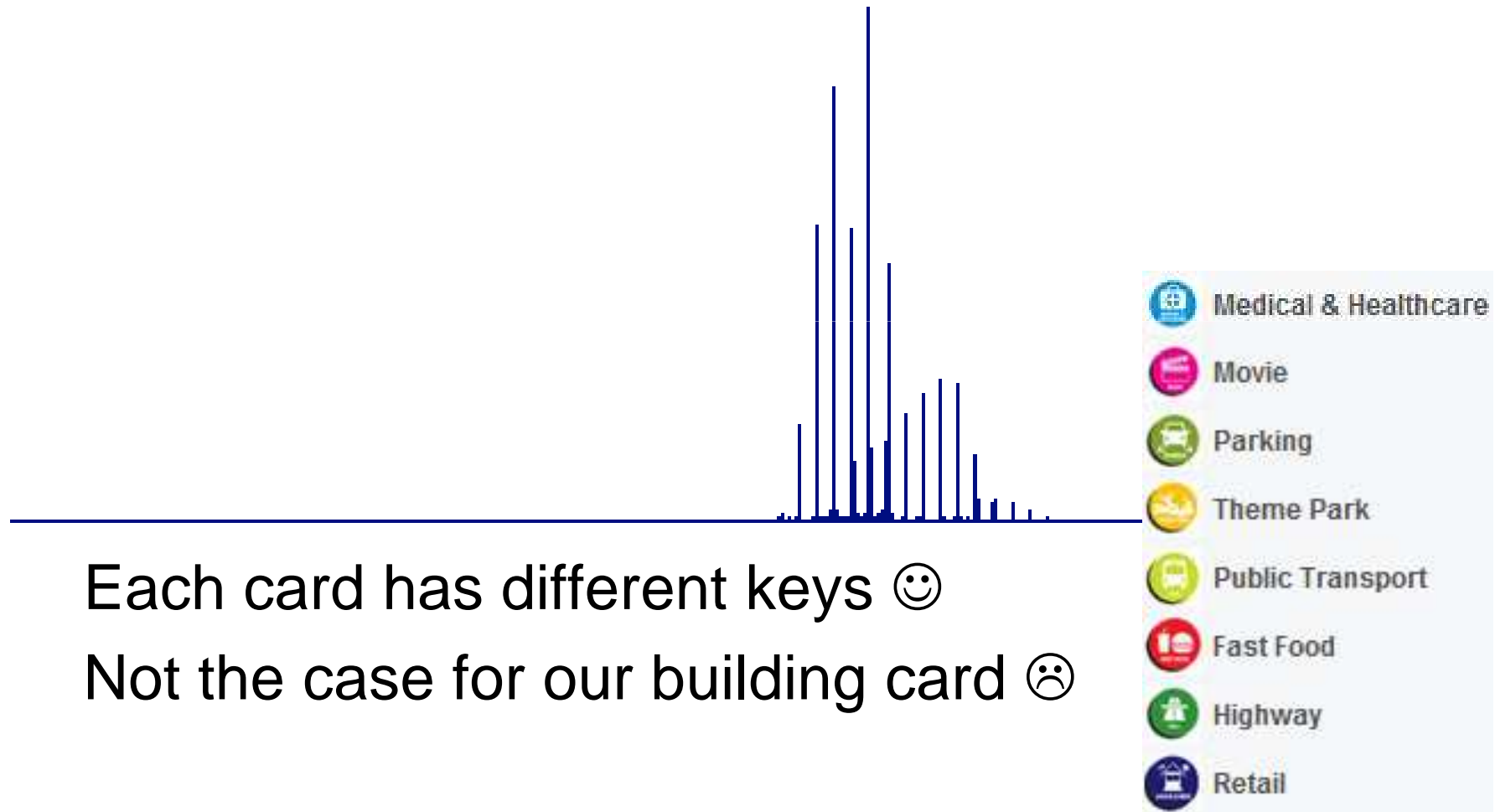
Not at all, just shows that the output random is somewhat correlated with this LFSR...

This RNG probably has additional complexity.

Experiment 2 – Malaysia Payment Card

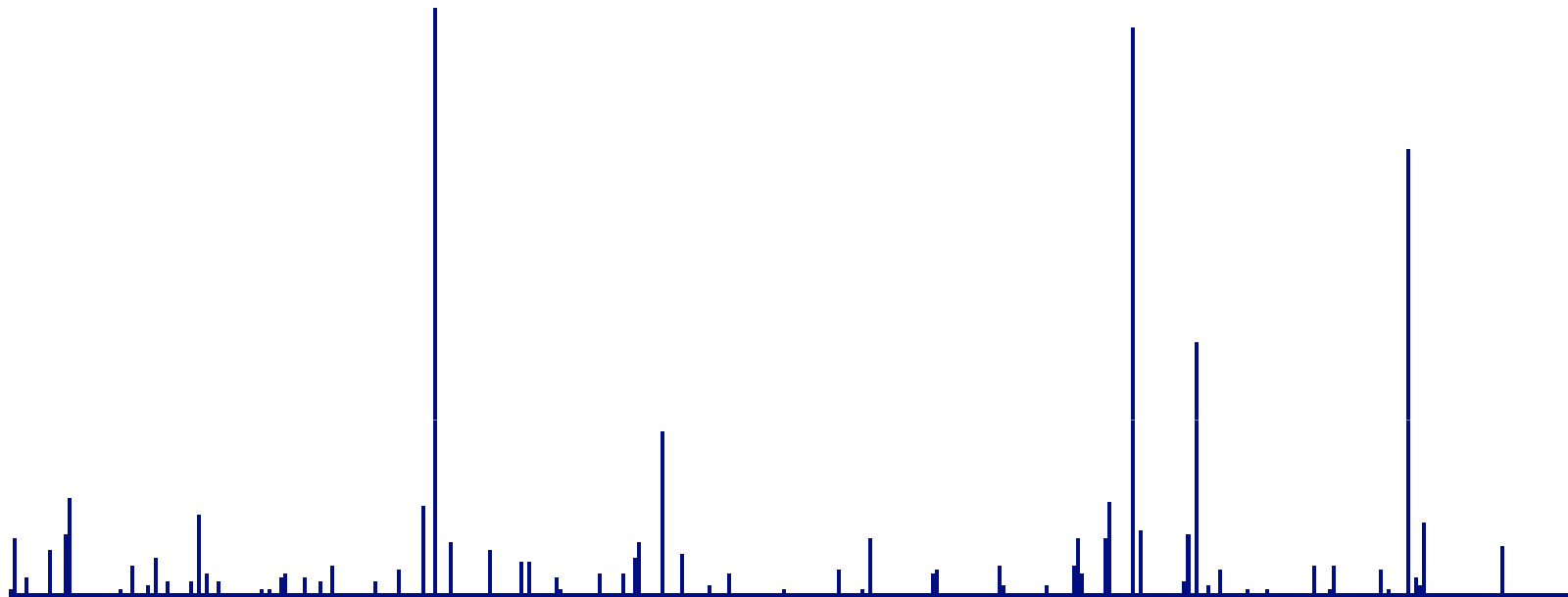


Malaysia – Good News



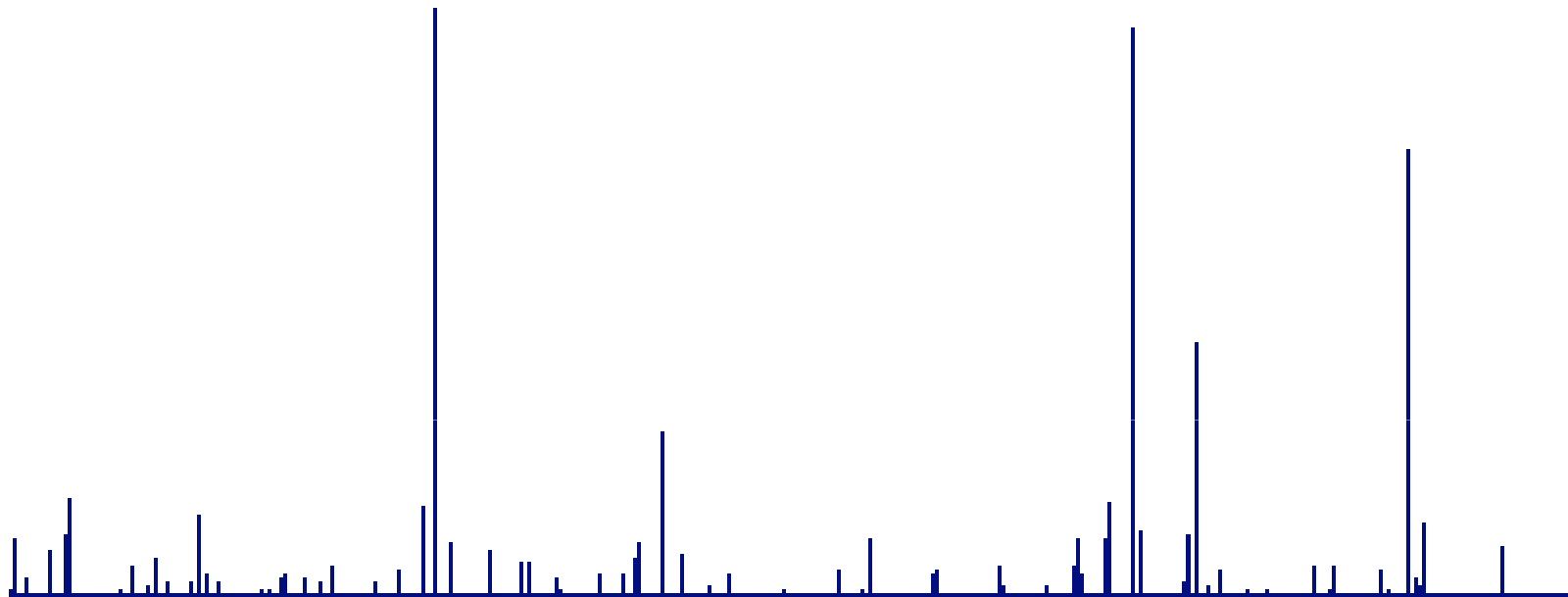
- Each card has different keys 😊
- Not the case for our building card ☹️

London Oyster Card From 2006



- Min-entropy = 2.8 bits.
- Attack time $2^{2.8} \times 10^5 \text{ s} = 3 \text{ minutes}$
-

London Oyster Card – Good News



- Each card has different keys 😊, online fraud detection, 2007 cards already more secure, but this one still in use ☹️

Horror Story: Warsaw Poland Metro/Bus/Parking Card

Hall of Shame (1)

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



Hall of Shame (contd.)

- In Warsaw, Poland, the first block uses the default Philips key FFFFFFFFFFFFFFFF,
- 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...

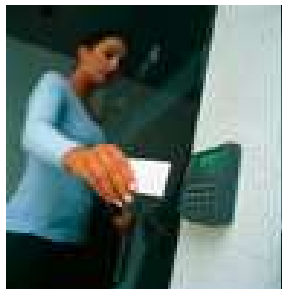




Back To Our UK SURVEY 2012 Building Cards (only)

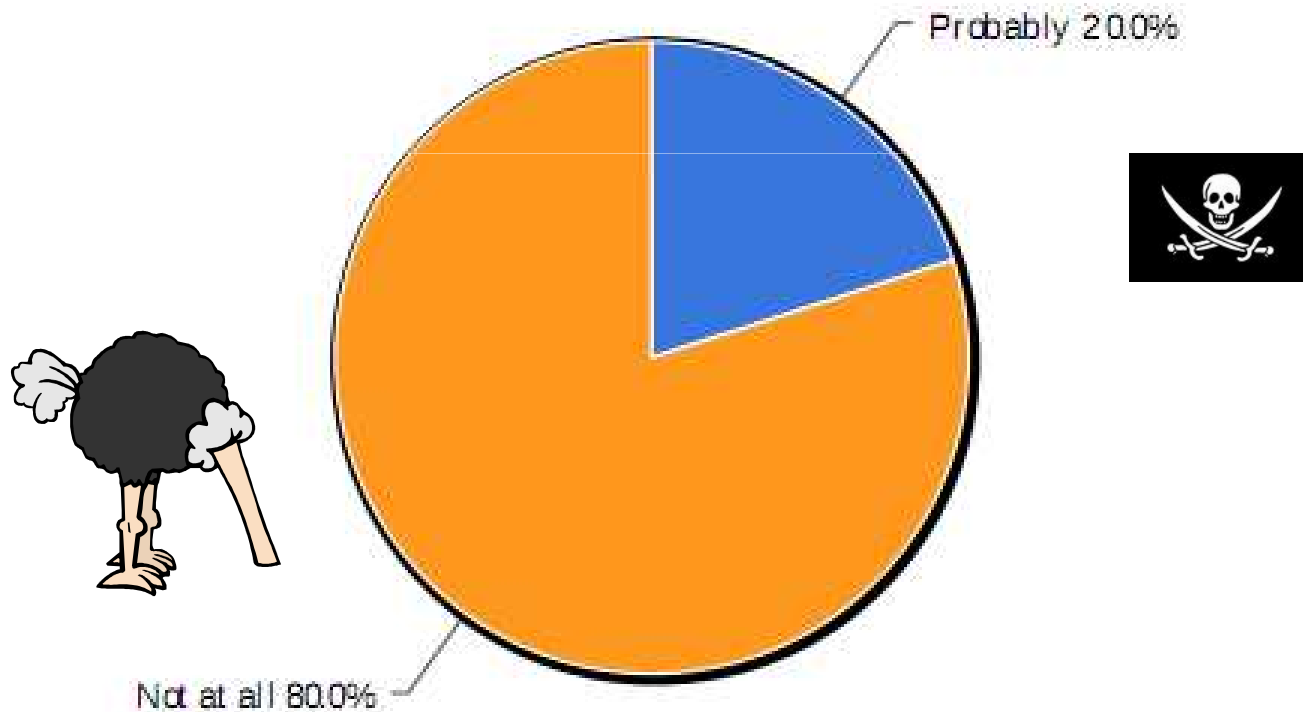


What's Wrong?



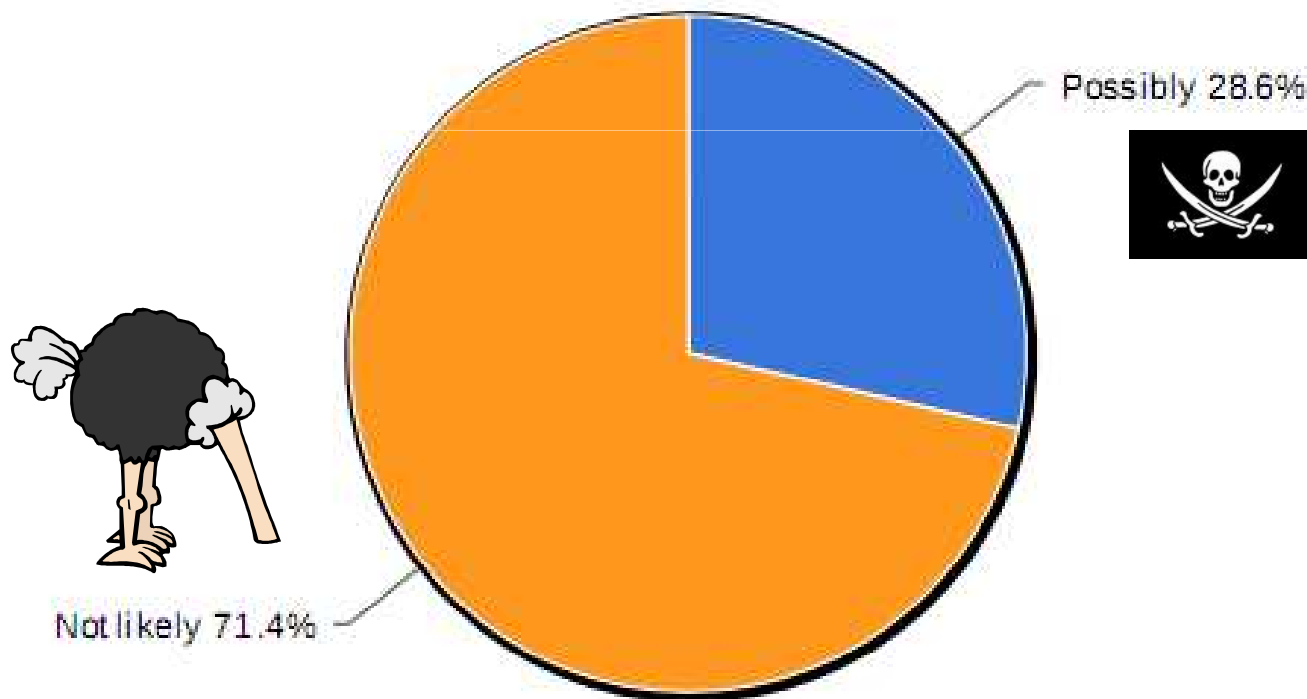
Afraid? Threat? Upgrade?

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?



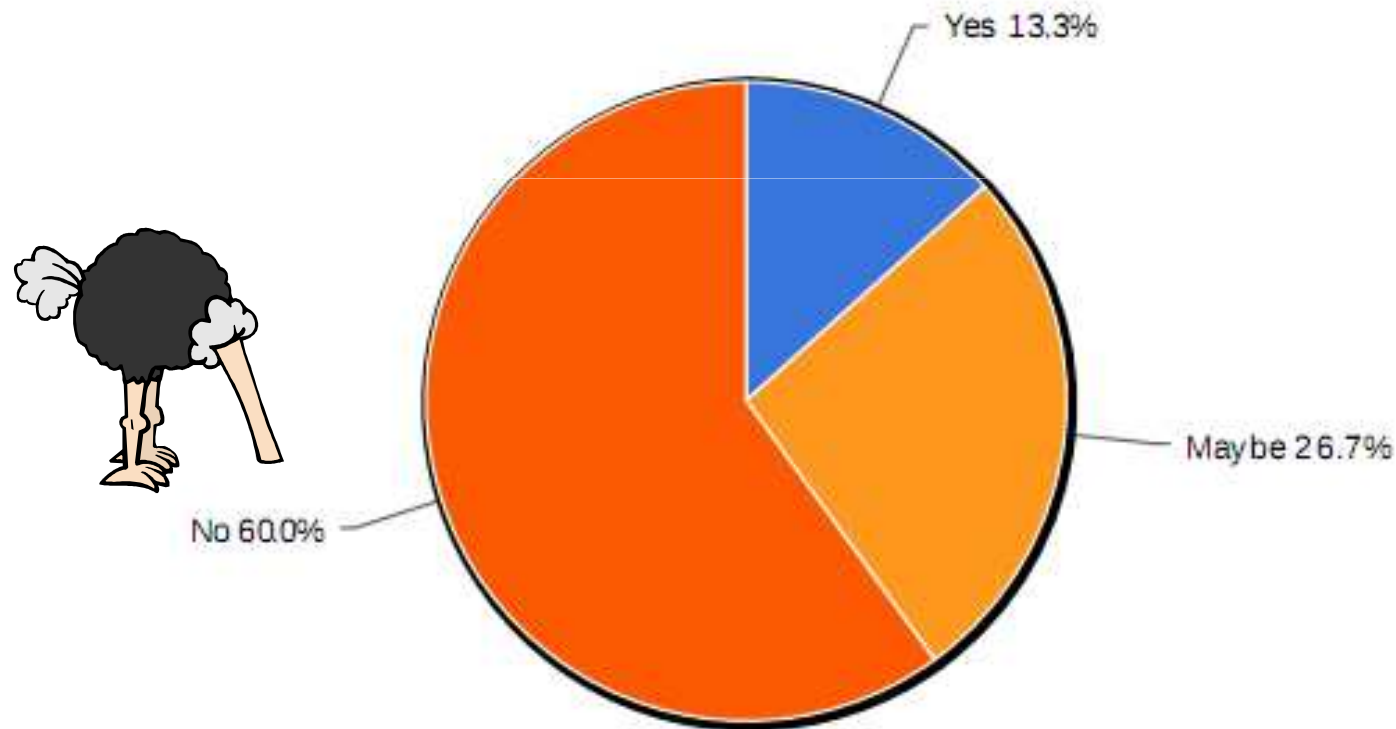
Card Cloning Specifically

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?



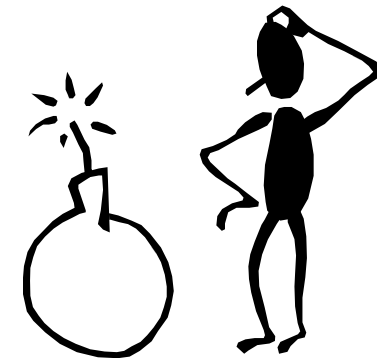
Unwilling to Upgrade

Do you think your building access control system is not currently meeting all your business needs and you would like to upgrade to another product?



Spectacularly Naïve

Not all attacks actually work,
sometimes they just don't ,



HOWEVER

Customers are spectacularly naïve
about the security of current systems.



Bad RNG...

Neither humans nor devices
can be trusted to generate
quality random numbers...

Do NOT assume that they are random...

Without good random numbers cryptographic
protections fail.