Analysis of RFID e-passport protocols

Tom Chothia

Overview

- Traceability/Unlinkability in the applied pi-calculus.

  with Arapinis, Ritter and Ryan

- A traceability attack against e-passports

  with Smirnov

Traceability

Portability devices lead to new kinds of attacks.

If a secure device you carry with you can be identified then it can be used to trace you.

A ***traceability attack*** is one where the attack can link two runs of the same device.

The Applied pi-Calculus

The Applied pi-Calculus is a micro language for modelling protocols:

P ::= in (x).P
out <M>.P
new n.P
!P
P|Q
0

plus any user defined equations e.g.
dec(enc (m,k) , k) = m

Checking Systems Using the Applied pi-Calculus

We can check secrecy by testing equality:

M is kept secret in the Protocol P if:

$$P(M) = P(M')$$

A System in Our Model

We want to trace agent A in a system:

System = new cs.(Env | !new names.Init.!A)

Env = the environment
names = are the new channels and data of A.
Init = the initiation process for A
A = the body of the agent..

A System in Our Model

In the case of RFID tags:

System =new db(DataBase | !Reader |
!new tagID.Init.!Tag)

tagID = the tags unique (secret) ID
Init = Logs tagID in the database over db
T = models the RFID tag

Strong Untracability

A process is strongly untraceable if a run where tags repeat, looks the same as a run where tags never repeat.

Strong Untracability

A process is strongly untraceable if a run where tags repeat, looks the same as a run where tags never repeat:

new cs.(Env | !new names.Init.!A)

= new cs.(Env | !new names.Init.A)

Strong Untracability

A process is strongly untraceable if a run where tags repeat, looks the same as a run where tags never repeat:

no ! here

new cs.(Env | !new names.Init.!A)

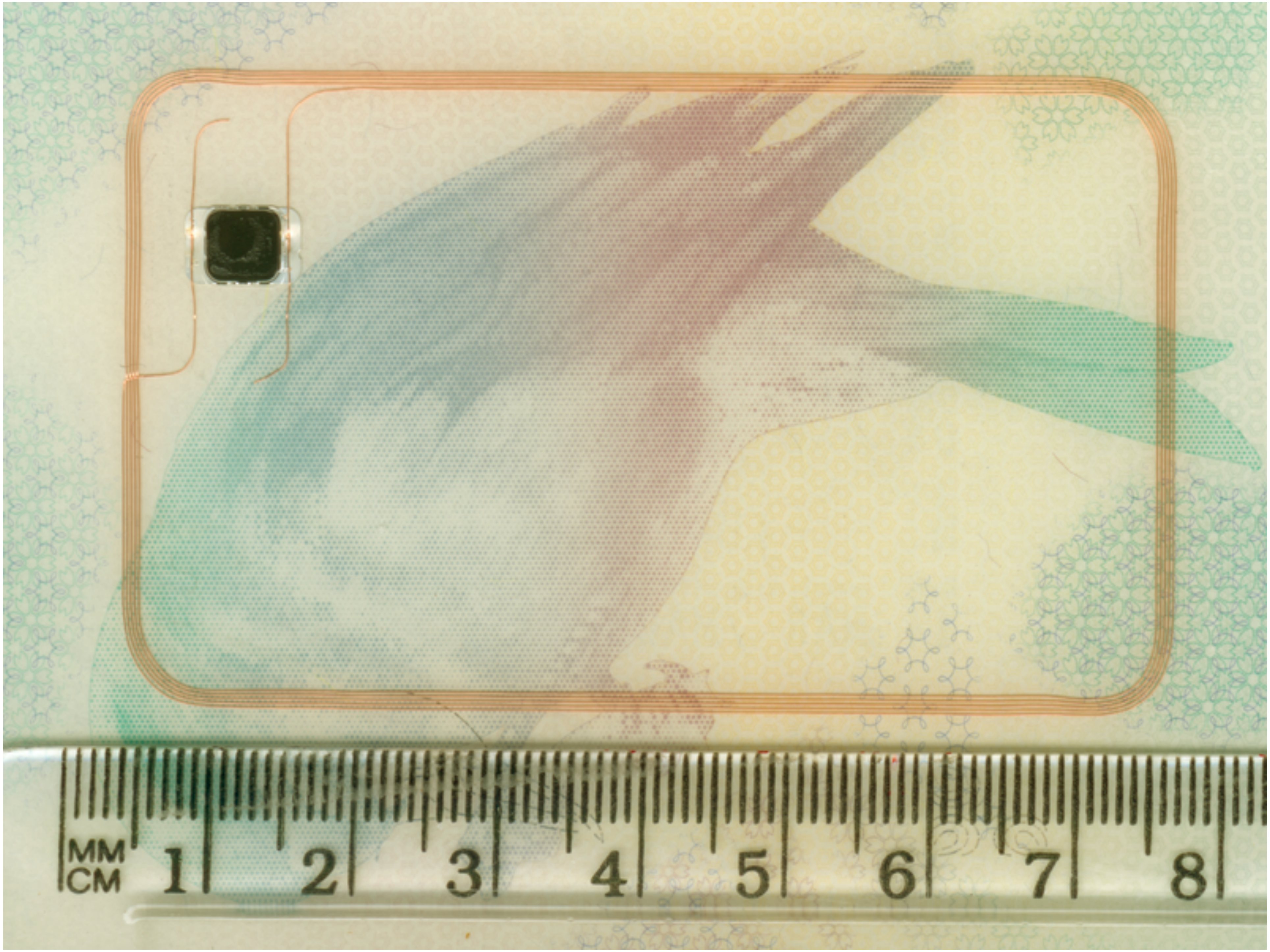
= new cs.(Env | !new names.Init.A)

More work on linkability/ traceability

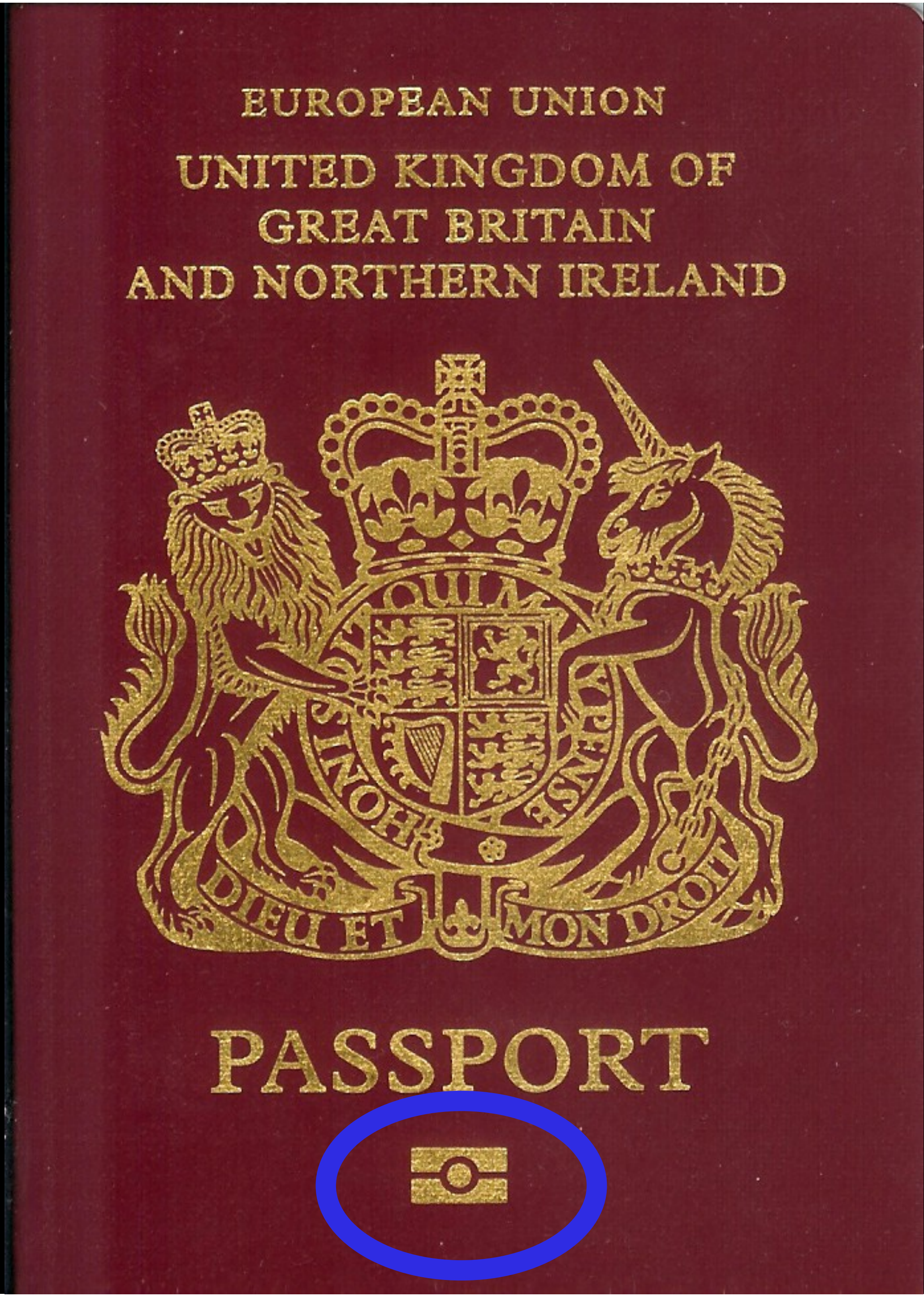
- In a paper with Arapinis, Ritter and Ryan, we also define a weak definition of unlinkability/untraceability.

- Failure of weak unlinkability implies a practical attack.

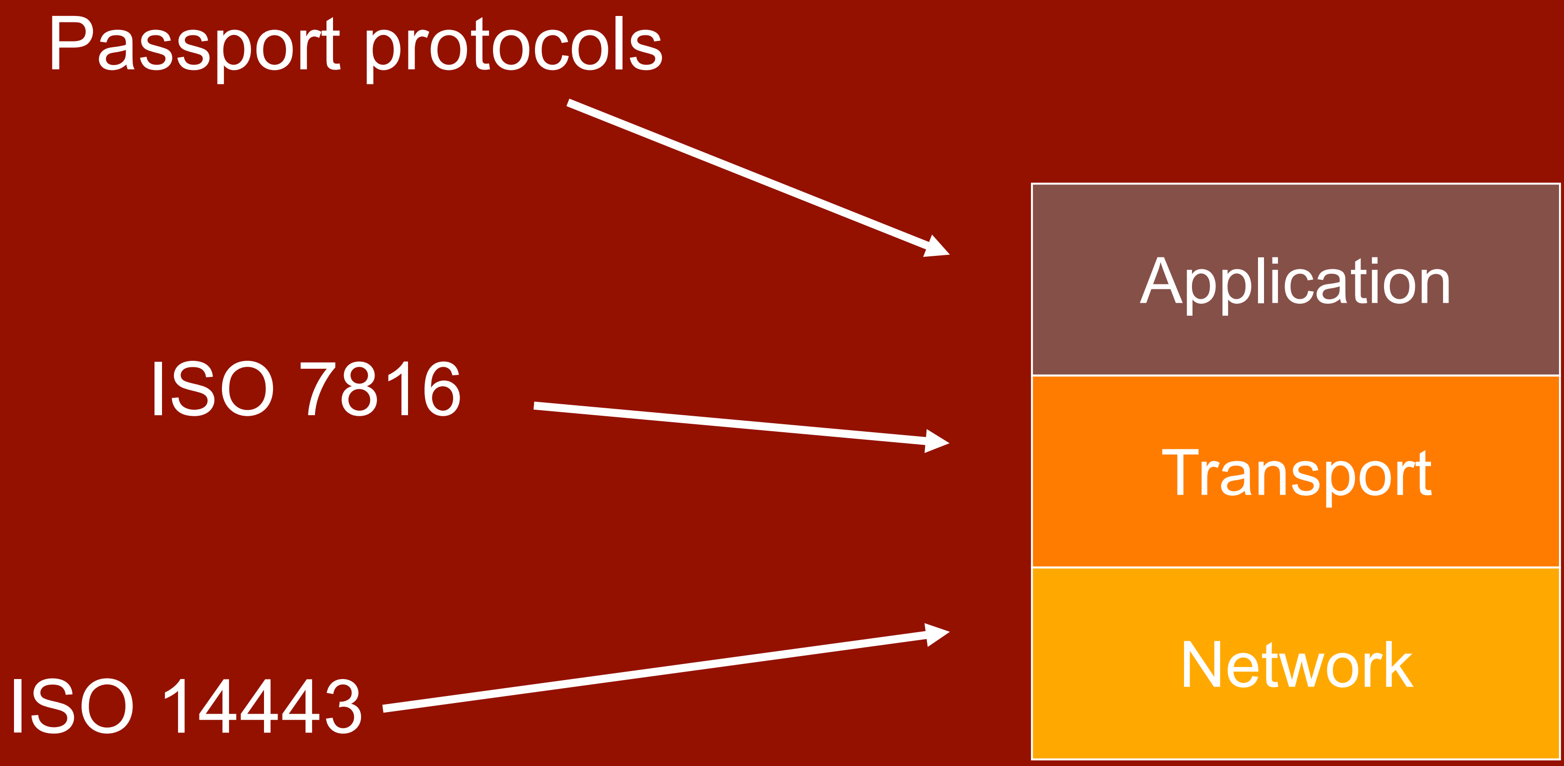
- We relate anonymity and unlinkability and show that they are unrelated. i.e., unlinkability doesn’t imply anonymity.


MM
CM
1 2 3 4 5 6 7 8


EUROPEAN UNION
UNITED KINGDOM OF
GREAT BRITAIN
AND NORTHERN IRELAND
DIEU ET MON DROIT
PASSPORT


EUROPEAN UNION
UNITED KINGDOM OF
GREAT BRITAIN
AND NORTHERN IRELAND
DIEU ET MON DROIT
PASSPORT

The RFID Passport Protocol Stack



ISO 14443

ISO 14443 handles low level communication.

The reader powers up the tag, official range 9cm, real range: 50cm+.

After power up the card broadcasts a UID.

Most passports randomise the UID,

Those that aren't random are traceable!

ISO 7816

ISO 7816 defines:

- A set of commands,
- Response format
- “Answer to Reset”

ISO 7816

ISO 7816 defines:

- A set of commands,
- Response format
- “Answer to Reset”

Commands include:

- SELECT FILE
- READ BINARY
- GET CHALLENGE
- INTERNAL AUTHENTICATE
- EXTERNAL AUTHENTICATE

RFID in Passports

Passport spec. is published as ICAO Doc 9303.

Passport stores information printed on the back page + maybe finger prints, iris...

Data is secured with a key based on the DoB,DoE and passport number.

Suite of Protocols

Passive Authentication
– *Data is signed with a key,*
– *which is signed by a “country key”.*

Basic Access Control
–*Stops skimming,*
–*Officially optional, but everyone has it.*

Active Authentication
–Stops passport being copied,
–Optional.

Enhanced Access Control

Data on the Passport

DG1: Machine readable info.
DG2: Picture
DG3: Fingerprints (seen on German)
DG4: Iris Scans (not seen)
DG7: Signature (not seen)
DG11+12: Optional (height&home address on FR)
DG14: Extended Access Control Options
DG15: Active Authentication public key
DG16: Emergency Contact

Basic Access Control

This protocol is run first and establishes a session key.

Goal: stop “skimming” and eavesdropping.

Only allows access to a reader that knows the date of birth, data of expiry and number of the passport.

Basic Access Control

DoB,DoE,# reader generates Km Ke

Basic Access Control

DoB,DoE,# reader generates Km Ke

1 Reader $\rightarrow$ Passport : GET CHALLENGE

Basic Access Control

DoB,DoE,# reader generates Km Ke

1 Reader $\rightarrow$ Passport : GET CHALLENGE

2 Passport $\rightarrow$ Reader : N_P

Basic Access Control

DoB,DoE,# reader generates Km Ke

1 Reader → Passport : GET CHALLENGE

2 Passport → Reader : N_P

3 Reader → Passport : $\{N_R, N_P, K_R\}_{Ke}$, $MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$

Basic Access Control

DoB,DoE,# reader generates Km Ke

1 Reader → Passport : GET CHALLENGE

2 Passport → Reader : N_P

3 Reader → Passport : $\{N_R, N_P, K_R\}_{Ke}$, $MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$

4 Passport → Reader : $\{N_P, N_R, K_P\}_{Ke}$, $MAC_{Km}(\{N_P, N_R, K_P\}_{Ke})$

Session key based on K_P xor K_R

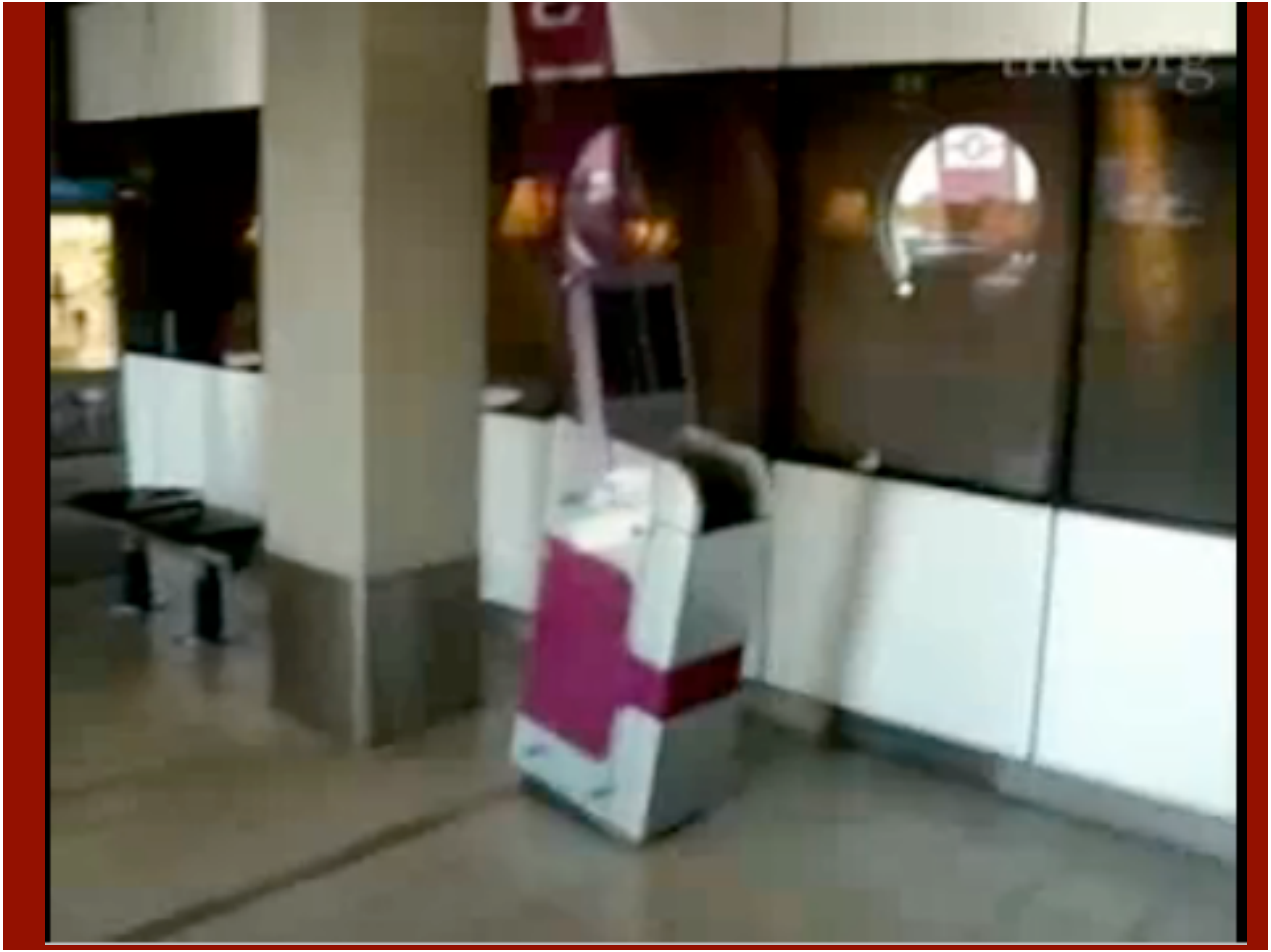
Reading a Passport

Knowing BAC lets us read passports

Hardware: any cheap RFID reader

Software: Adam Laurie's RFID tools:

http://rfidiot.org/




thc.org


Paspoort
thc.org
PRESLEY
ELVIS AARON
USA
M
08-01-35
USA
The fake passport chip is accepted by
the terminal; no error or alert is raised

Simple Attacks on Passports

- Some machines don't check the signature.
- You can detect the presence of a passport.
- Access cannot be revoked.
- If you know someone's DoB,DoE and passport number, you can check for their passport.

Guessing the number

- Guest the DoB, DoE and # and break the passport.
- Some countries e.g. Belgian have easy to guess passport numbers.
- In response some countries (e.g. DK) have switched to alpha-numeric passport #.
- Alpha-numeric key entropy can be > 69 bits.

Country Finger Printing

	Commands						
	44	**82**	**84**	**88**	**A4**	**B0**	**B1**
	Rehab. CHV	Ext. Auth.	Get Chall.	Int. Auth.	Select File	Read Binary	Read Binary
Australian	6982	6985	6700	6700	9000	6700	6700
Belgian	—	6E00	—	6700	6A86	6986	6700
Dutch	—	6700	6700	6982	6A86	6982	6982
French	6982	6F00	6F00	6F00	6F00	6F00	6F00
German	—	6700	6700	—	6700	6700	—
Greek	6982	63C0	6700	6982	9000	6986	6700
Italian	—	6700	—	—	—	—	—
Polish	6982	6700	6700	6700	9000	6700	—
Swedish	6982	6700	6700	—	9000	6700	—
Spanish	—	6700	6700	—	6700	6700	—

Answer to Reset

Answer to Reset responses from

UK passports:
3B898001097877D4020000900048

French passports:
3B8E80011177B3A7028091E16577010103FF61

German passports:
3B898001097877C4020000900058

Basic Access Control

Reader

Passport

Basic Access Control

Reader Passport

— GET CHALLENGE ⟶

Basic Access Control

Reader Passport

— GET CHALLENGE ⟶

Pick random N_P

Basic Access Control

Reader Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_P ———

Basic Access Control

Reader | Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$ N_P ——

Pick random N_R, K_R

Basic Access Control

Reader | Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_P ——

Pick random N_R, K_R

— $\{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Basic Access Control

Reader | Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$ N_P ———

Pick random N_R, K_R

— $\{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Check MAC,
Decrypt, Check N_P
Pick random K_P

Basic Access Control

Reader   Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_P ———

Pick random N_R, K_R

— $\{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Check MAC,
Decrypt, Check N_P
Pick random K_P

$\longleftarrow$ $\{N_P, N_R, K_P\}_{Ke}, MAC_{Km}(\{N_P, N_R, K_P\}_{Ke})$ —

Basic Access Control

Reader Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_P ———

Pick random N_R, K_R

— $\{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Check MAC,
Decrypt, Check N_P
Pick random K_P

$\longleftarrow$ $\{N_P, N_R, K_P\}_{Ke}, MAC_{Km}(\{N_P, N_R, K_P\}_{Ke})$ —

Check MAC,
Decrypt, Check N_R

Error Messages: French Passport

Error Messages: French Passport

Reader Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_P ——

Pick random N_R,K_R

— $\{N_R,N_P,K_R\}_{Ke}$,$MAC_{Km}(\{N_R,N_P,K_R\}_{Ke})$ $\longrightarrow$

Error Messages: French Passport

Reader Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_P ——

Pick random N_R,K_R

— $\{N_R,N_P,K_R\}_{Ke}$,$MAC_{Km}(\{N_R,N_P,K_R\}_{Ke})$ $\longrightarrow$

Check MAC Fails

Error Messages: French Passport

Reader Passport

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_P ——

Pick random N_R, K_R

— $\{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ ⟶

Check MAC Fails

⟵ 6300 no info. –

MAC fail equals with error 6300: “no info”

Error Messages: French Passport

Reader   Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_P ——

Pick random N_R, K_R

— $\{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Error Messages: French Passport

Reader | Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$——— N_P ———

Pick random N_R, K_R

— $\{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Check MAC, Decrypt

Check N_P Fails

Error Messages: French Passport

Reader Passport

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_P ———

Pick random N_R,K_R

— $\{N_R,N_P,K_R\}_{Ke}$,$MAC_{Km}(\{N_R,N_P,K_R\}_{Ke})$ ⟶

Check MAC, Decrypt

Check N_P Fails

⟵ 6A80 Incorrect params –

Nonce fail equals error 6A80 “Incorrect params”

Attack Part 1

Attack Part 1

Attacker eavesdrops on Alice using her passport

Reader Passport

Attack Part 1

Attacker eavesdrops on Alice using her passport

Reader Passport

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_P ———

Attack Part 1

Attacker eavesdrops on Alice using her passport

Reader Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_P ———

Pick random N_R, K_R

— $M = \{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Attack Part 1

Attacker eavesdrops on Alice using her passport

Reader Passport

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_P ———

Pick random N_R, K_R

— $M = \{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ ⟶

Attack records message M.

Attack Part 2

Attacker

????

Attack Part 2

Attacker ????

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_{P2} ——

Attack Part 2

Attacker ????

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$—— N_{P2} ———

— $M = \{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Attack Part 2

Attacker ????

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_{P2} ———

— $M = \{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ ⟶

⟵ 6300 no info. –

Attack Part 2

Attacker ????

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$ N_{P2} ——

— $M = \{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

$\longleftarrow$ 6300 no info. –

Mac check failed.

Attack Part 2

Attacker ????

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_{P2} ———

— $M = \{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ ⟶

⟵ 6300 no info. –

Mac check failed.
???? is not Alice

Attack Part 2

Attacker ????

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_{P2} ——

— $M = \{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ ⟶

Attack Part 2

Attacker ????

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_{P2} ———

— $M = \{N_R,N_P,K_R\}_{Ke},MAC_{Km}(\{N_R,N_P,K_R\}_{Ke})$ ⟶

⟵ 6A80 incorrect params. –

Attack Part 2

Attacker ????

— GET CHALLENGE ⟶

Pick random N_P

⟵—— N_{P2} ———

— $M = \{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ ⟶

⟵ 6A80 incorrect params. –

Mac check passed,

Attack Part 2

Attacker ????

— GET CHALLENGE $\longrightarrow$

Pick random N_P

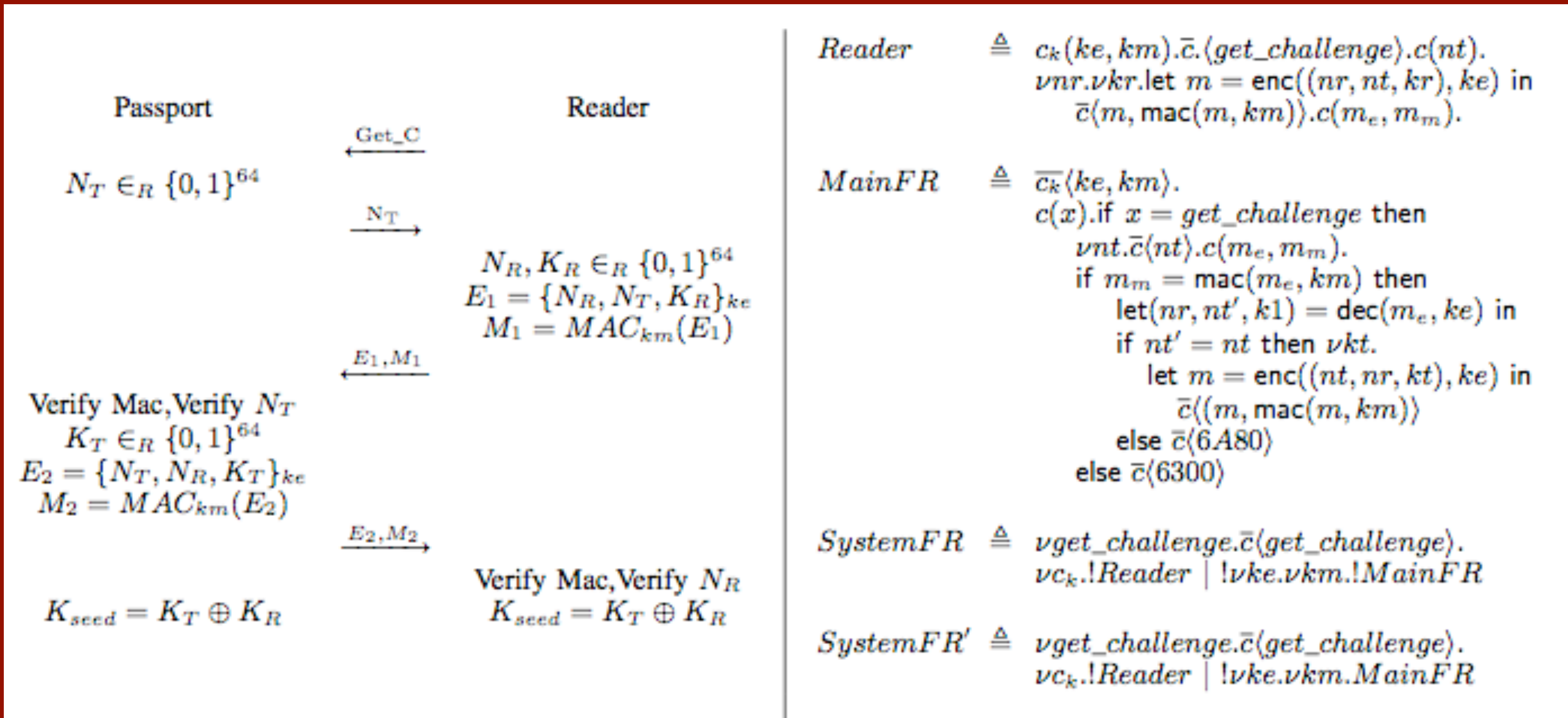
$\longleftarrow$—— N_{P2} ———

— $M = \{N_R,N_P,K_R\}_{Ke},MAC_{Km}(\{N_R,N_P,K_R\}_{Ke}) \longrightarrow$

$\longleftarrow$ 6A80 incorrect params. –

Mac check passed,
???? must have used Alice's Mac key
therefore ???? is Alice.

French Passport Attack in the Applied pi-calculus



a) In Alice & Bob notation

b) In applied pi calculus

Guilty Confession Time

We did not find this attack using our formal analysis methods.

We spotted the attack while read the specification.

20 or so other papers about e-passports missed this attack,

- maybe we spotted because we had our formal methods in mind, when reading the specification?

Other Passports

- UK, German, Russian, Irish passport return same error messages both situation.

Other Passports

- UK, German, Russian, Irish passport return same error messages both situation.

- But what about a timing attack?

Basic Access Control

Reader Passport

— GET CHALLENGE $\longrightarrow$

Pick random N_P

$\longleftarrow$ N_P ———

Pick random N_R, K_R

— $\{N_R, N_P, K_R\}_{Ke}, MAC_{Km}(\{N_R, N_P, K_R\}_{Ke})$ $\longrightarrow$

Check MAC,

Decrypt, Check N_P

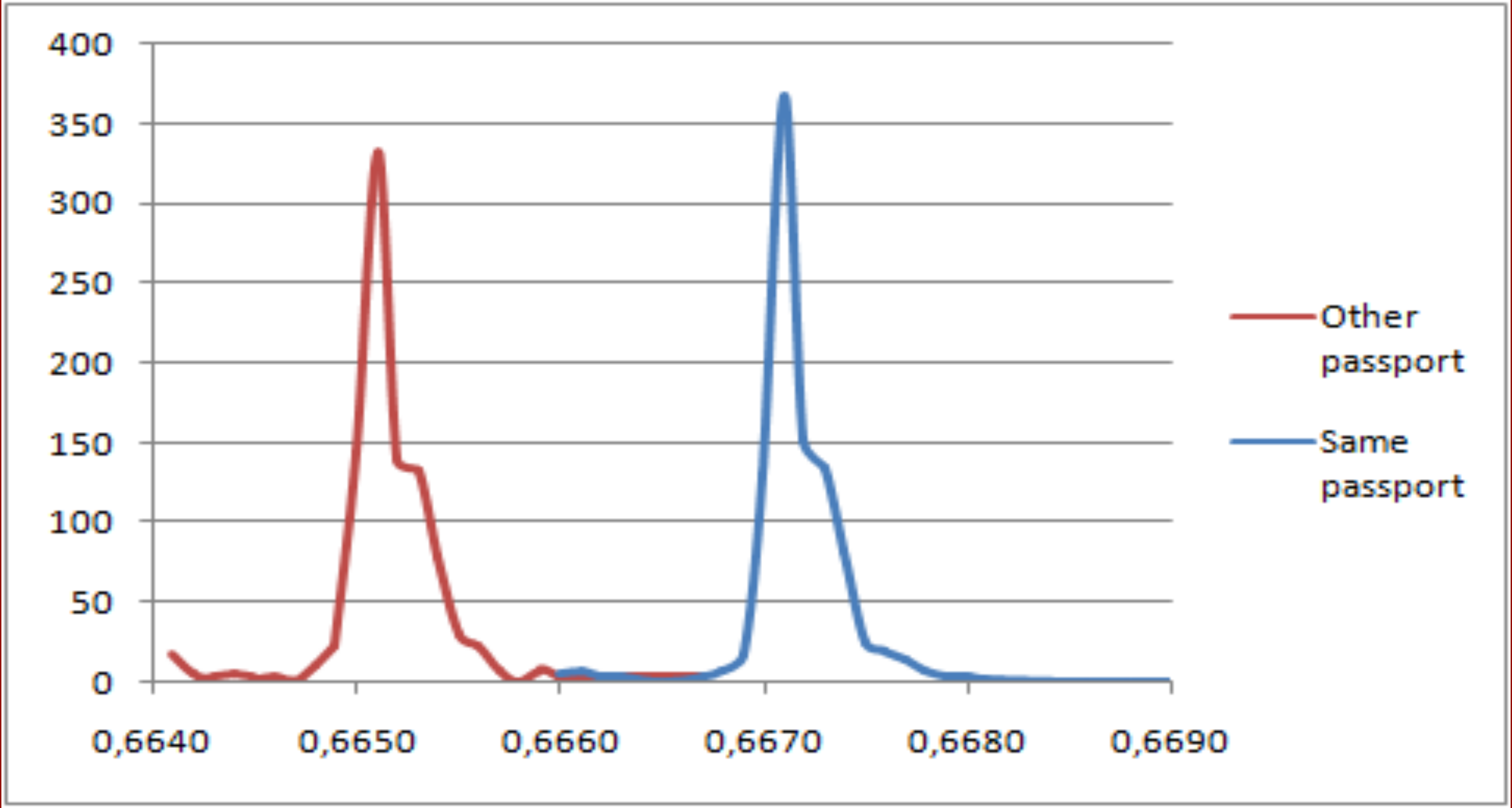
Pick random K_P

$\longleftarrow$ $\{N_P, N_R, K_P\}_{Ke}, MAC_{Km}(\{N_P, N_R, K_P\}_{Ke})$ —

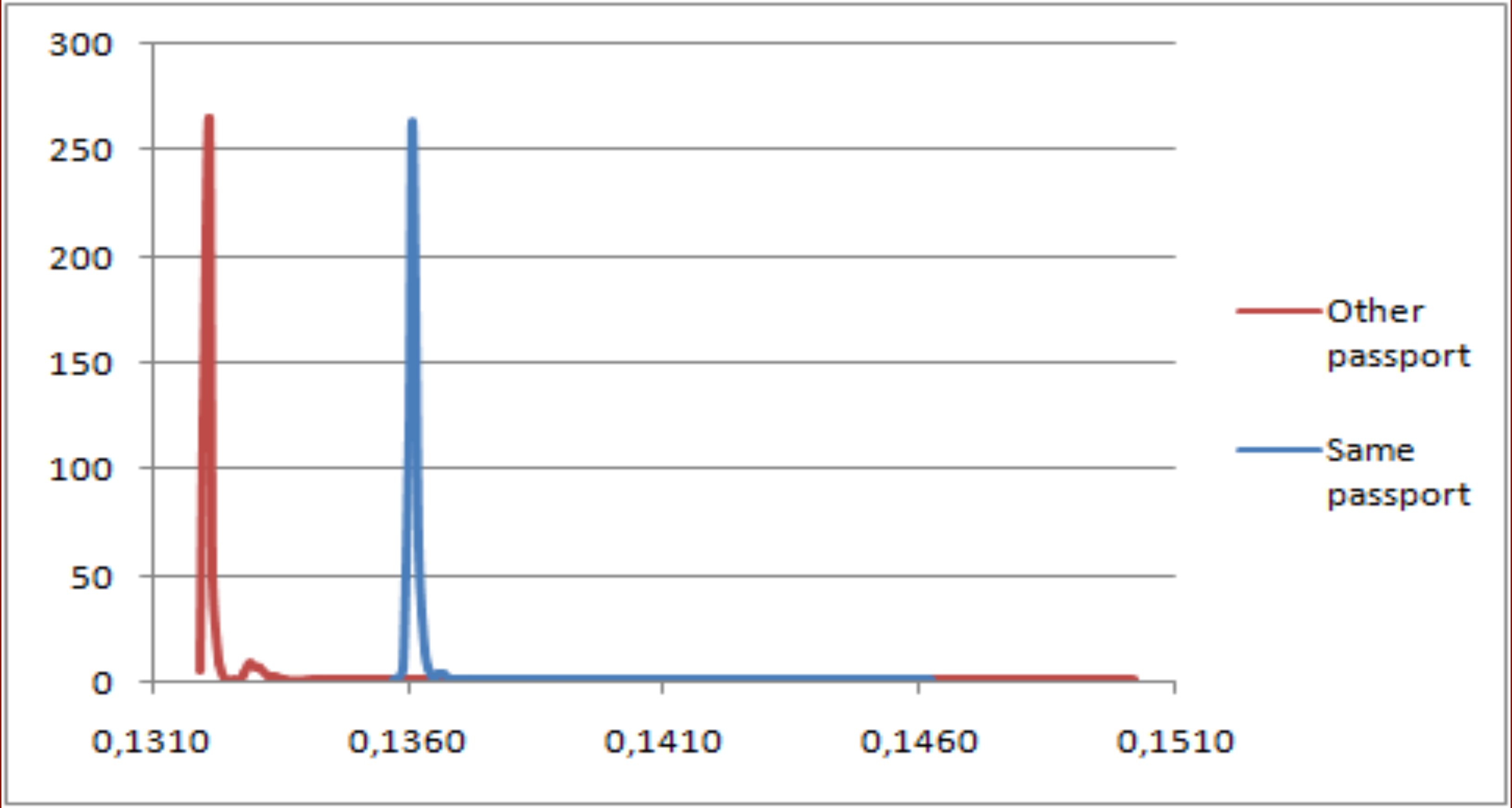
Check MAC,

Decrypt, Check N_R

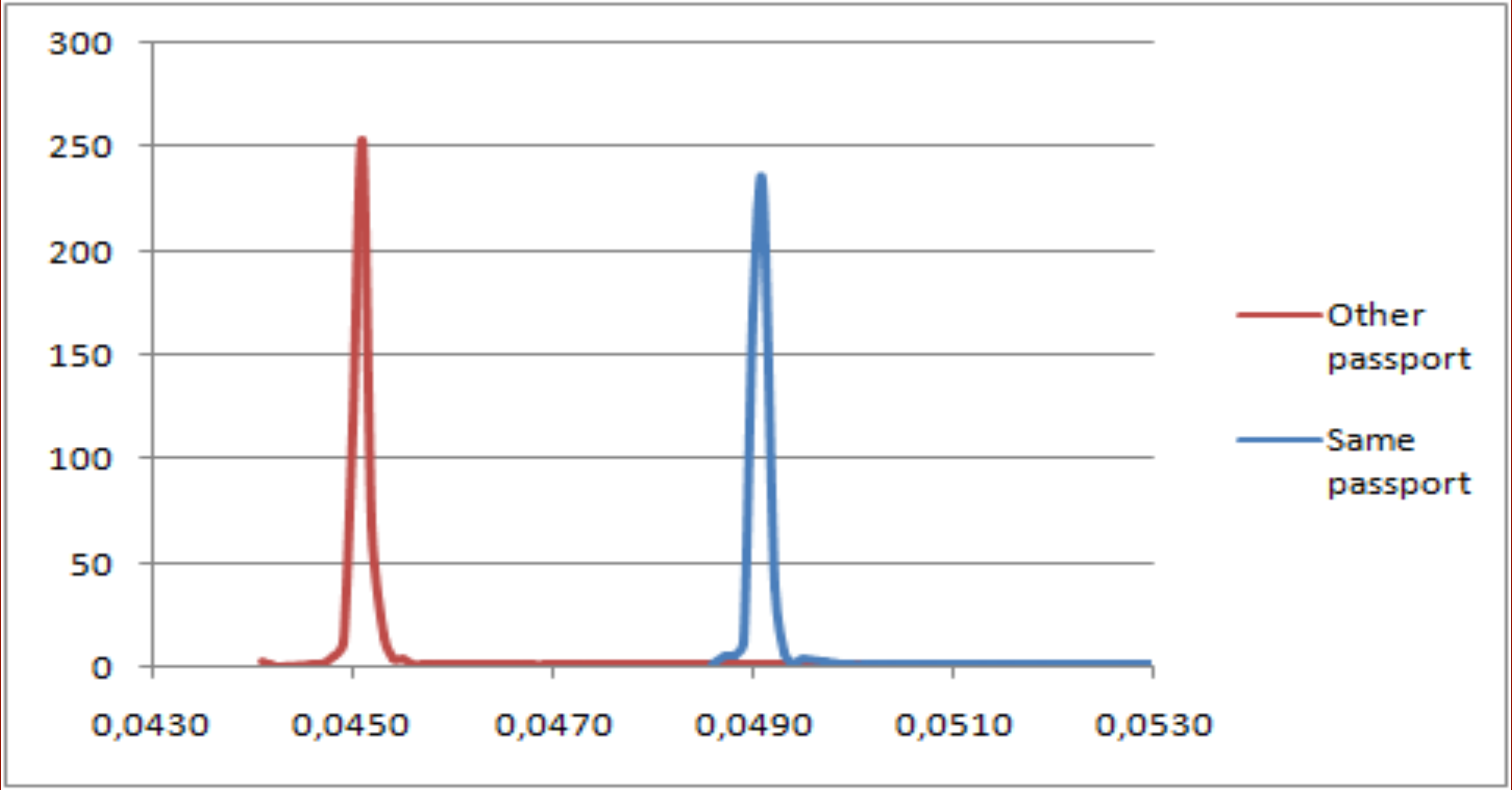
The failed MAC is rejected sooner, UK passport



German Passports:

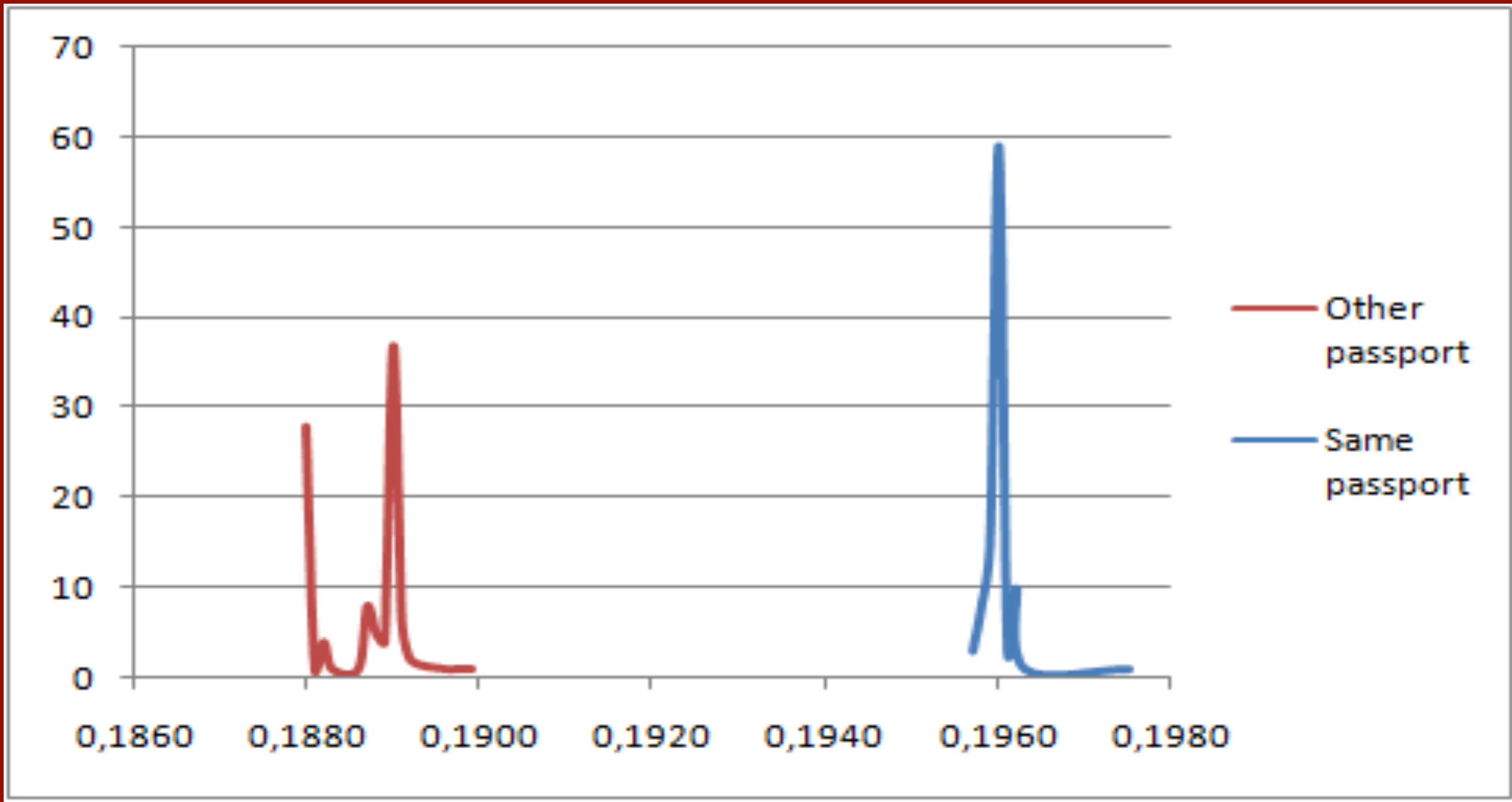


Greek



300
250
200
150
100
50
0
0,0430
0,0450
0,0470
0,0490
0,0510
0,0530
Other passport
Same passport

Russian



70
60
50
40
30
20
10
0
0,1860
0,1880
0,1900
0,1920
0,1940
0,1960
0,1980
Other passport
Same passport

The Timed Attack

Our tests show that its possible to identity a passport with a high degree of reliability in a few seconds.

Passports can be used for targeted surveillance, but not mass surveillance.

Defects in e-passports allow real-time tracking

This threat brought to you by RFID

By **Dan Goodin in San Francisco** • **Get more from this author**

Posted in Security, 26th January 2010 22:07 GMT

Computer scientists in Britain have uncovered weaknesses in electronic passports issued by the US, UK, and some 50 other countries that allow attackers to trace the movements of individuals as they enter or exit buildings.

The Register®

Hardware Software Music & Media Ne

Crime Malware Enterprise Security S

Defects in e-passports allow real

This threat brought to you by RFID

By Dan Goodin in San Francisco • Get

Posted in Security, 26th January 2010 22:07

Computer scientists in Britain have uncov
by the US, UK, and some 50 other countr
individuals as they enter or exit buildings.

Times Higher Education

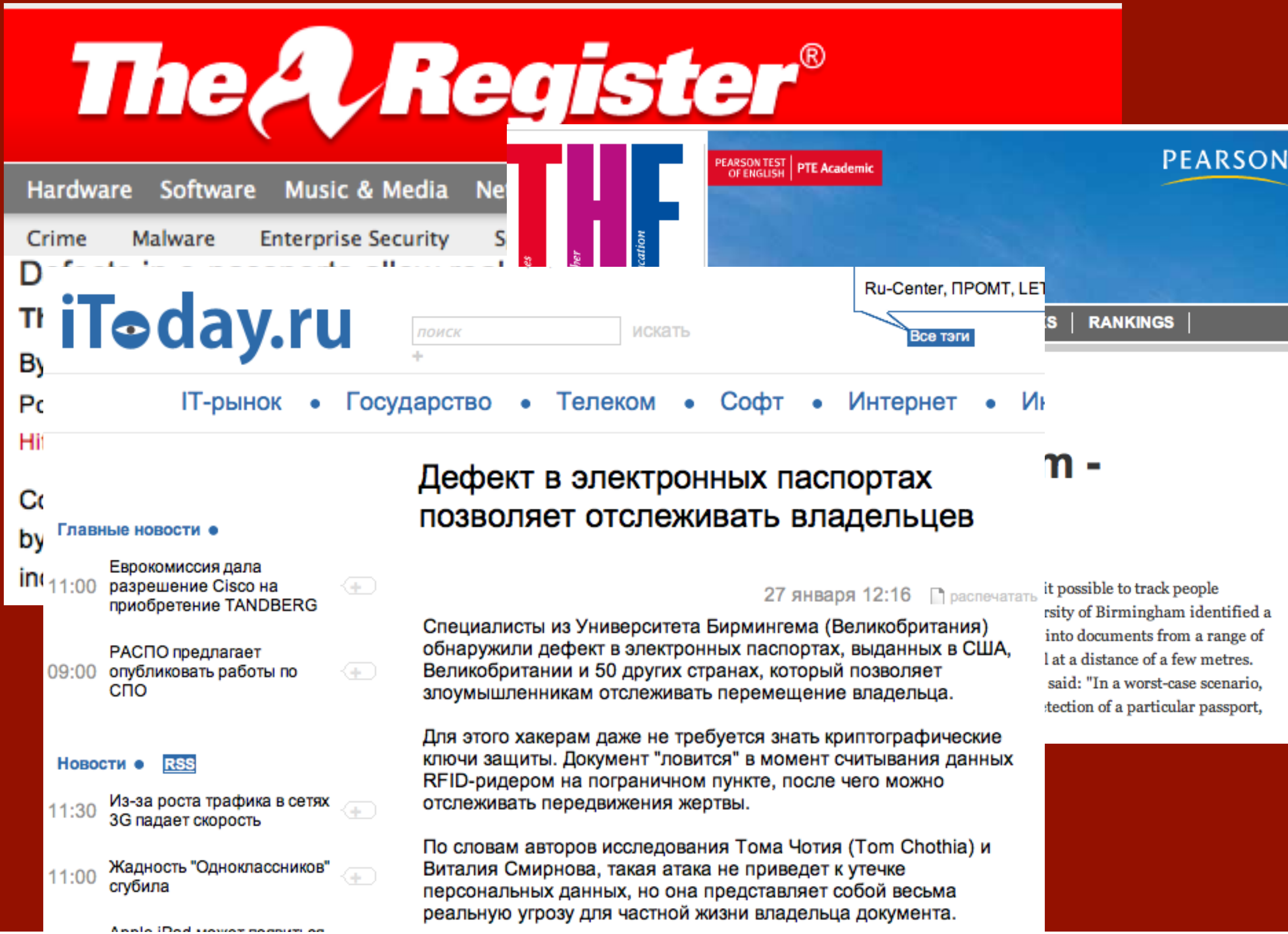
HOME | CONTACT | COMMENT | CAREER | NEWS | BOOKS | RANKINGS |

ADVERTISE

University of Birmingham - Passport to oblivion

28 January 2010

Computer scientists claim to have found a flaw in e-passports that makes it possible to track people carrying them - potentially assisting murderers. Researchers at the University of Birmingham identified a fault in the design of the radio-frequency identification tags incorporated into documents from a range of countries. The scientists could detect the passport carried by an individual at a distance of a few metres. Tom Chothia, researcher at the Birmingham School of Computer Science, said: "In a worst-case scenario, this flaw would make it possible to build a bomb that would explode on detection of a particular passport, killing the bearer."



Дефект в электронных паспортах позволяет отслеживать владельцев

27 января 12:16 распечатать

Специалисты из Университета Бирмингема (Великобритания) обнаружили дефект в электронных паспортах, выданных в США, Великобритании и 50 других странах, который позволяет злоумышленникам отслеживать перемещение владельца.

Для этого хакерам даже не требуется знать криптографические ключи защиты. Документ "ловится" в момент считывания данных RFID-ридером на пограничном пункте, после чего можно отслеживать передвижения жертвы.

По словам авторов исследования Тома Чотия (Tom Chothia) и Виталия Смирнова, такая атака не приведет к утечке персональных данных, но она представляет собой весьма реальную угрозу для частной жизни владельца документа.


EUROPEAN UNION
UNITED KINGDOM OF
GREAT BRITAIN
AND NORTHERN IRELAND
PASSPORT


National Identity Card
Johnson
Alan Arthur
Specimen
British Citizen
17-05-1950
London
27-07-2009
31-07-2009
© PA

123456789
UNITED KINGDOM
National Identity Card
Surname/Nom
Johnson
Alan Arthur
Specimen
Sex/Sexe
M
British Citizen
Date of birth/Date de naissance
17-05-1950
London
Date of issue/Date de délivrance
27-07-2009
Date of expiry/Date d'expiration
31-07-2009
© Getty Images


123456789
National Identity Card
Johnson
Alan Arthur
Specimen
Sex/Sexe
M
British Citizen
Date of birth/Date de naissance
17-05-1950
London
27-07-2009
31-07-2009
© Getty Images

RFID in UK ID cards?

UK has been issuing “ID cards for foreigners”

Adam Lauire and NO2ID have both tested cards and found that they use RFID.

I’ve tested four cards issued in the last 6 months and not found RFID tags.

Government official on record as saying they will have RFID.

Must have RFID if they are to be used to travel.

How do I say this without sounding like a crazy conspiracy theorist?

How do I say this without sounding like a crazy conspiracy theorist?

- Proposed ID cards may contain a RFID tags.

How do I say this without sounding like a crazy conspiracy theorist?

- Proposed ID cards may contain a RFID tags.
- The RFID protocol allows your movements to be traced.

How do I say this without sounding like a crazy conspiracy theorist?

- Proposed ID cards may contain a RFID tags.
- The RFID protocol allows your movements to be traced.
- It may become a legal requirement to carry such a broken card.

How do I say this without sounding like a crazy conspiracy theorist?

- Proposed ID cards may contain a RFID tags.
- The RFID protocol allows your movements to be traced.
- It may become a legal requirement to carry such a broken card.
- Wrapping your card/passport in lots of tin foils might help

Conclusion

RFID tags in identification documents really aren’t a good idea.