Men who stare at bits

Security of RFID studentcards in Germany

@nv1t, Rena Tangens

29c3 Hamburg

Who we are

Rena Tangens

Art d'Ameublement

FoeBuD e.V. (jetzt: digitalcourage)

BigBrotherAwards

foebud.org
bigbrotherawards.de
rena@digitalcourage.de

digitalcourage e.V.

Who we are

Jan Hoersch, nuit

Member of IT Security
TMT GmbH & Co. KG

TMT
Technik. Medien. Telekommunikation.

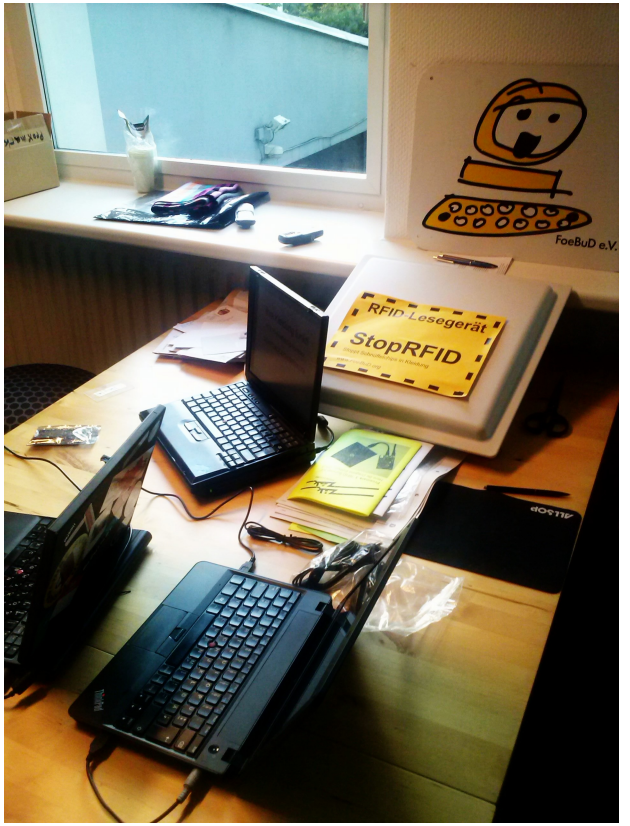
This research is not work related

From one card to many

23.03.2012 Presenting “encryption” of one card at the b4ckspace takeoff
18.05.2012 SIGINT 2012 – Men who stare at bits

Brainstorm with FoeBuD:

… double the target size, double the fun.



Cards, please!

RFID-Forschungsprojekt: Wer hat Mensa- oder Studikarten für uns?

Der FoeBuD braucht Ihre und Eure Mithilfe für ein Forschungsprojekt. In vielen Mensa- und Studikarten sind nämlich RFID-Chips vorhanden, zum Bezahlen und zum Ausweisen. Wir wollen diese Chips einmal genauer analysieren und auf Datensicherheit prüfen – und dabei die Karten von möglichst vielen verschiedenen Hochschulen vergleichen.

So sehen sie zum Beispiel aus - ganz harmlos - und drinnen schläft der Chip, bis er einen Einsatzbefehl erhält ... ;-)

Die meisten Hochschulen verwenden übrigens nicht den Begriff "RFID", sondern sprechen von einem "Mifare-Chip" – aus Angst vor Protesten.
Klar ist: Wenn der Ausweis kontaktlos funktioniert, dann ist auch ein RFID-Chip drin!

Wir freuen uns über alle Einsendungen. Schreibt bitte die Hochschule dazu und welche Funktionen mit der Karte genutzt werden können. Auch wer seine Karte nur für ein, zwei Wochen entbehren kann, kann sie uns schicken. Die Karten werden nicht verändert oder beschädigt und wir senden sie hinterher natürlich zurück. Die Aktion läuft bis Ende
Oktober 2012.

Die Adresse zum Einsenden der Karten ist:
FoeBuD e.V., RFID-Forschungsprojekt, Marktstraße 18, 33602 Bielefeld

(Source: http://www.foebud.org/rfid/rfid-mensa/)

Universities are not amused

- Student union Berlin demands removal of their card as illustration for our appeal.
- Warning message in the mailing list of the data protection officers and legal departments of North Rhine-Westphalia.
- FH Bielefeld demands removal of appeal because of security reasons.

Still not amused...

Quote letter FH Bielefeld:
“Eine Weitergabe von Schlüsseln an unbefugte Dritte würde zu Sicherheitslücken im Sicherheitssystem der Hochschule führen.”

Reply Rena Tangens:
“Wir versichern Ihnen, dass wir keineswegs vorhaben, uns mit den zur Verfügung gestellten Karten Zugang zu irgendeiner Hochschule zu verschaffen. […] Dass man mit der Karte eines anderen - ebenso wie mit einem geliehenen Schlüssel - sich Zugang verschaffen kann, ist auch keine überraschende Erkenntnis, die noch einer forschenden Untersuchung bedürfte.”

We come in peace...

Die Karten werden an einem separaten Laptop ausgelesen, der **physikalisch vom Internet getrennt** ist. Der Rechner selbst besitzt eine **verschlüsselte LVM**, wobei das "Archiv" auf dem Rechner nochmal in einem verschlüsselten Container liegt. Der Zugriff vom Internet ist vollkommen ausgeschlossen. Es wird **keine Veröffentlichung des Archivs** geben, da dies extrem fahrlässig wäre und wir Datenschutz bekanntermaßen wichtig finden.
Es werden die direkten **Payloads** der Karten gespeichert, wobei diese natürlich **anonymisiert** sind, soweit es möglich ist. D.h. bei Studiausweisen sind die erkennbaren Teile (wie Name, Nummern, die der Person zugeordnet werden können) herausgelöscht. Lediglich der Ort und **welche Universität / Fachhochschule, ist abgespeichert,** da wir ja genau dies untersuchen wollen. Wir können also im Nachhinein **keine Aussage treffen, wem eine bestimmte Karte gehört.**

(Source: http://www.foebud.org/rfid/rfid-mensa/)

Best practice

Ruhr University Bochum

The only university who offered testcards!

Put up or shut up...

... dataformats and results in detail

Naming-convention-fu...

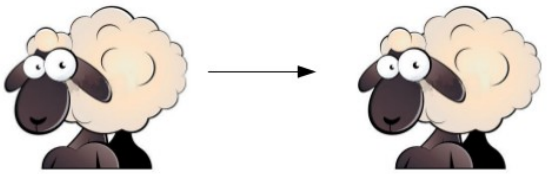
Sector																	Block
	0	000	92	18	a7	10	3d	88	04	00	46	7a	a8	05	32	31	3a	31	0
		010	32	02	00	00	01	38	01	38	01	38	00	00	00	00	00	00	1
		020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	2
		030	a0	a1	a2	a3	a4	a5	78	77	88	c1	2a	0d	4b	ad	81	92	3
	1	040	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
		050	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
		060	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
		070	ff	ff	ff	ff	ff	ff	ff	07	80	69	ff	ff	ff	ff	ff	ff	
	2	080	04	50	00	ff	00	dc	99	00	00	00	00	00	00	00	00	00	
		090	00	03	03	00	00	00	00	00	00	00	00	00	00	00	c0	3a	
		0a0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
		0b0	a0	a1	a2	a3	a4	a5	78	77	88	69	ea	ed	bb	d5	97	84	
	3	0c0	ff	98	f7	1d	ee	06	73	83	bd	47	d5	45	51	e7	fd	dd	
		0d0	2d	cf	92	67	5b	1d	03	75	00	00	00	00	00	00	00	00	
		0e0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	
		0f0	12	b8	77	14	a3	b2	7f	07	88	69	5e	a9	6b	ad	1a	c6	
	4	100	c5	f7	1d	ec	bb	ae	b0	42	14	a0	4e	8e	e0	32	6b	47	
		110	f7	4d	a3	0c	98	58	17	8c	26	0b	79	be	29	72	37	c7	
		120	c6	49	ed	85	f4	fc	c1	30	00	00	00	00	00	00	00	00	
		130	61	51	e0	71	3c	82	7f	07	88	69	48	3c	53	21	e6	f5	

What's the problem again?

Mifare Classic … do we have to say more?

We know the format, therefore we know everything

Cloning



Be locker...

nächsten Terminal aktiviert werden!

Verschließen

- Schranktür schließen
- Karte leicht gegen Schließknopf drücken
  - grünes Licht und ein Klicken bestätigen die Aktivierung des Schließknopfs
- Knopf drehen (wie einen Schlüssel)
- Prüfen, ob Schrank verschlossen ist!

Öffnen

- Karte leicht gegen Schließknopf drücken
  - grünes Licht und ein Klicken bestätigen die Aktivierung des Schließknopfs
- Schloss öffnet automatisch

DESfire secure?!

Aachener Nachrichten

LOKALES | NACHRICHTEN | SPORT | VIDEOS | FOTOS | MEINUNG | DOSSIER | RATGEBE

POLITIK | AUS ALLER WELT | WIRTSCHAFT | KULTUR | KINO | DIGITAL | WISSENSCHAFT | HOC

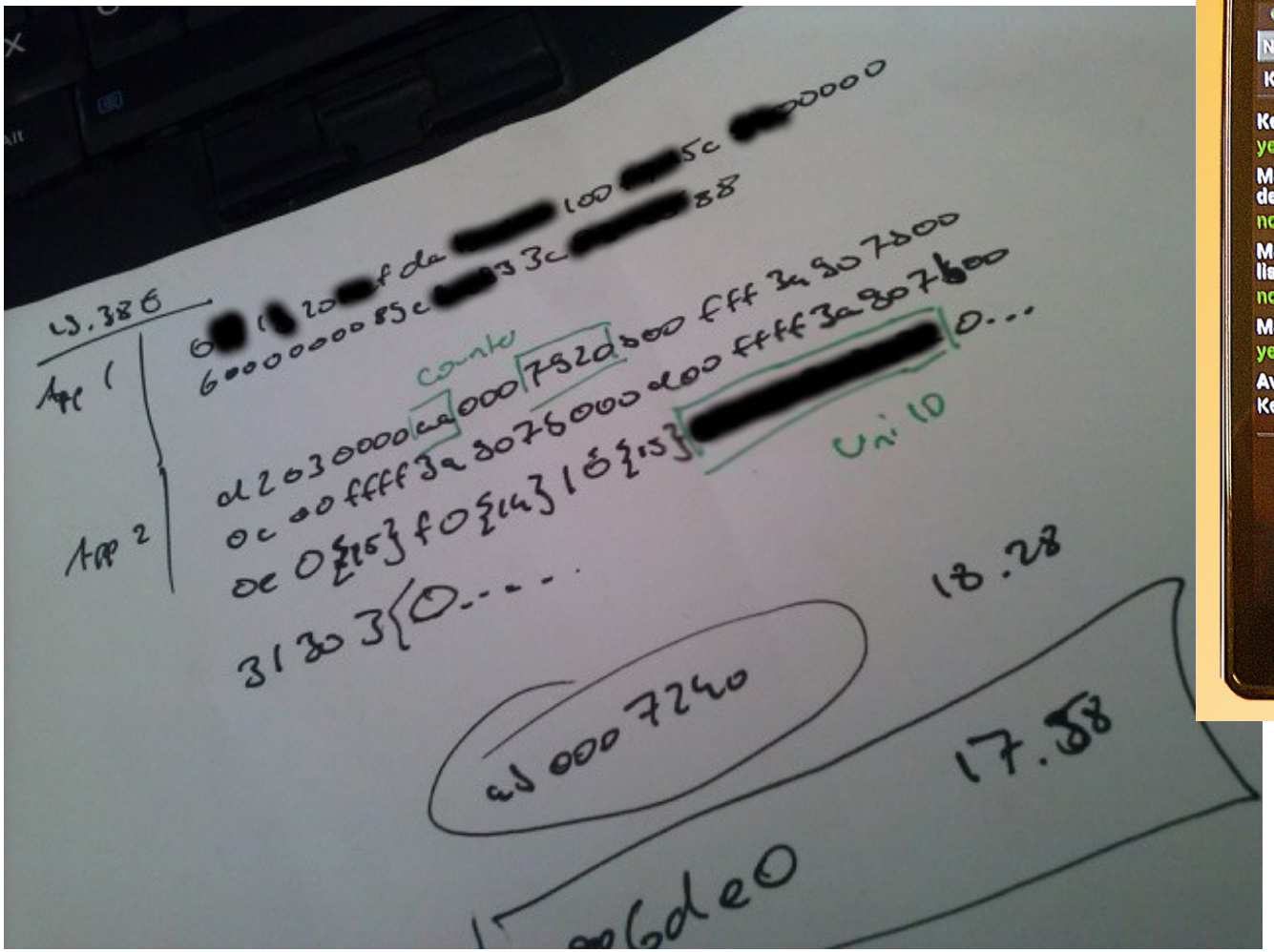
RWTH muss 30.000 Karten austauschen

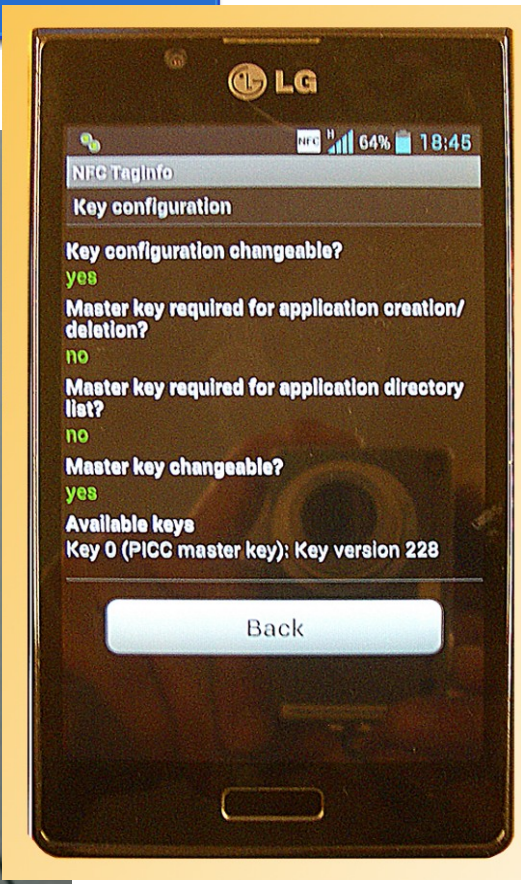
Von: Achim Kaiser
Letzte Aktualisierung: 19. April 2011, 18:34 Uhr

Einführung misslungen: Der neue Plastikausweis für Studierende weist Sicherheitslücken auf und muss erneuert werden. Foto: Harald Krömer

Fact: Just stating the card can crypt with triple DES does not make it encrypted!

Another cleartext DESfire





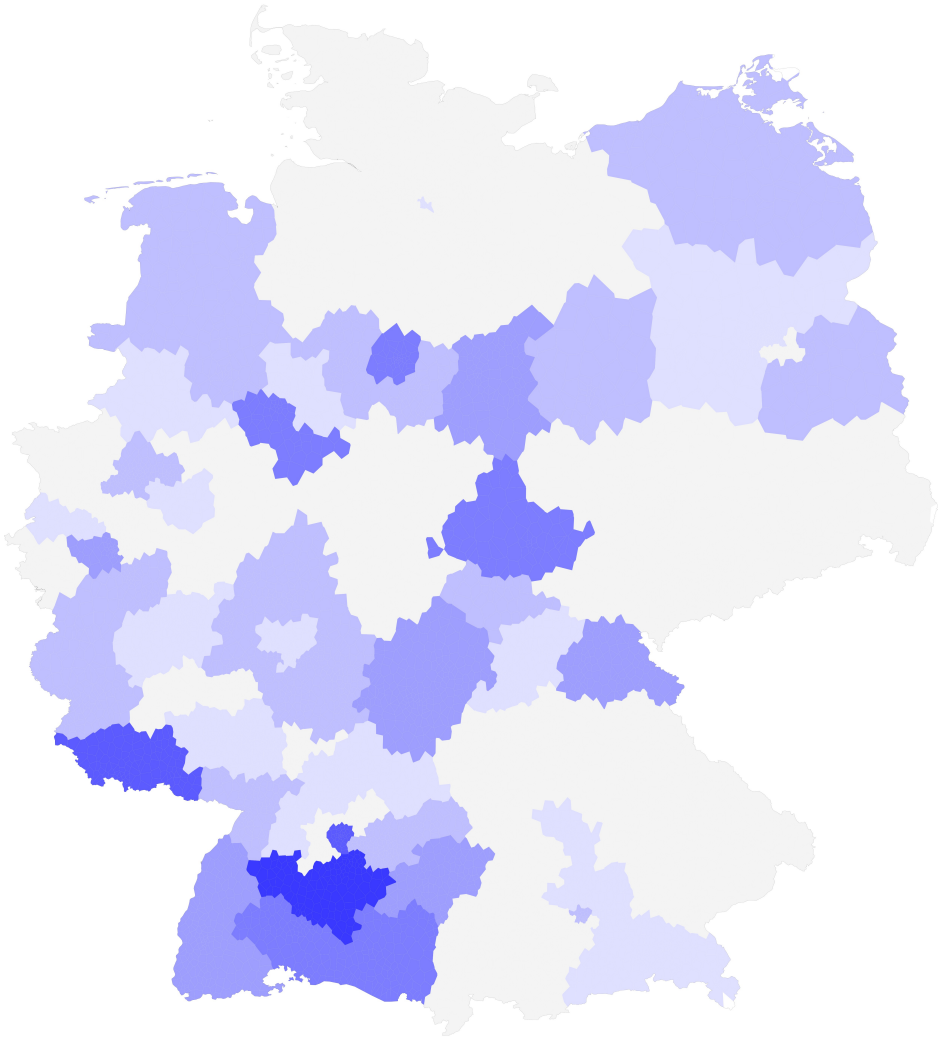
Some weeks of research

Hs-Nr.	Hochschulkurzname	Bundesland	Anzahl Studierende	Kartentyp / Hersteller	Durch Analyse	Recherchiert
128	Hildesh./ Holzm./ Göttingen H	Niedersachsen	5147	DESfire / InterCard		X
287	Hof H	Bayern	2985	InterCard		X
129	Hohenheim U	Baden-Württemberg	8626	InterCard		X
271	Idstein HFresen	Hessen	1462			
130	Ilmenau TU	Thüringen	6763	DESfire / InterCard		X
288	Ingolstadt H	Bayern	3549			
335	Iserlohn BiTS	Nordrhein-Westfalen	1180			
132	Isny H	Baden-Württemberg	216			
134	Jena FH	Thüringen	4802	Mifare Classic / InterCard		X
133	Jena U	Thüringen	20417	Mifare Classic / InterCard	X	
306	Kaiserslautern FH	Rheinland-Pfalz	5571	DESfire / Professional Services		X
135	Kaiserslautern TU	Rheinland-Pfalz	13388	DESfire / Professional Services		X
139	Karlsruhe AkdBK	Baden-Württemberg	309			
138	Karlsruhe H	Baden-Württemberg	6972	Mifare Classic / InterCard	X	
140	Karlsruhe HfGest	Baden-Württemberg	438			
141	Karlsruhe HfM	Baden-Württemberg	567			
359	Karlsruhe IKH	Baden-Württemberg	576			
137	Karlsruhe PH	Baden-Württemberg	3433			
136	Karlsruhe U KIT	Baden-Württemberg	22546	Mifare Classic / InterCard	X	
418	Kassel CVJM	Hessen	196			
142	Kassel U	Hessen	21361			
143	Kempten H	Bayern	4521			
145	Kiel FH	Schleswig-Holstein	6451			

Thanks to Thorben, digitalcourage

One vendor to rule them all...

(..nearly)



One card vendor

115 from **392** colleges
1.087.778 from **2.342.621** students

No Information about cards
~ 260 colleges

We are not alone

Credit to all individuals and teams
who have done their own research
and shared them with us.

Thank you!

Contact

Rena Tangens

mail@digitalcourage.de
0521/16391639

digitalcourage e.V
Marktstrasse 18
33602 Bielefeld

Jan Hoersch

nuit@hoeja.de
0x6F2172E7

@nv1t