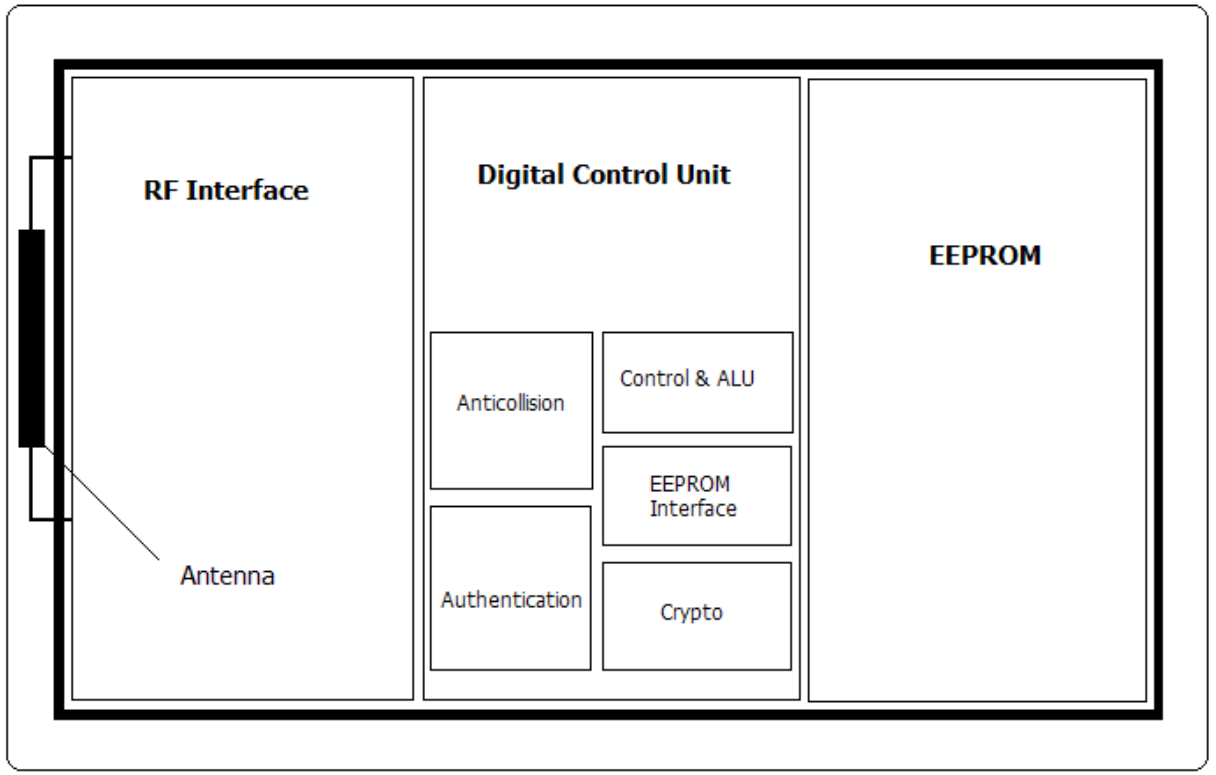
Podatności kart Mifare

URSZULA STACHOWIAK – INTERNET PRZEDMIOTÓW

Plan prezentacji

1. Czym są karty Mifare?
2. Rodzaje kart Mifare
3. Przegląd podatności kart Mifare
4. Omówienie wybranej podatności
5. Sposoby ochrony przed podatnościami

Czym są karty Mifare?



Rodzaje kart Mifare

- MIFARE Classic
- MIFARE Plus
- MIFARE Ultralight
- MIFARE DESFire

Przegląd podatności kart Mifare

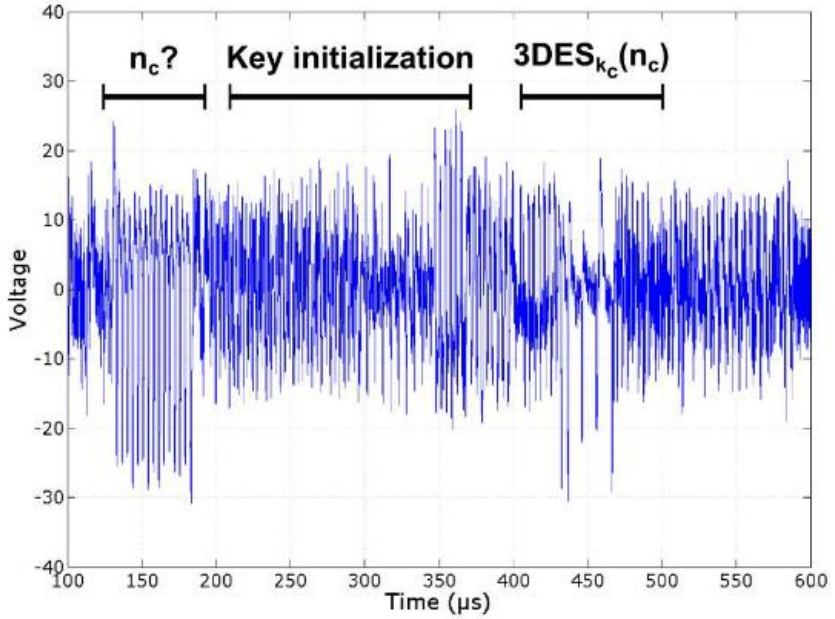
Ataki na Mifare Classic

- 2007 – Henryk Plötza i Karsten Nohl – Chaos Communication Congress – częściowa inżynieria wsteczna
- 2008 - Radboud University Nijmegen - Digital Security Group – kompletna inżynieria wsteczna – możliwość sklonowania i manipulowania zawartością chipa OV-Chipaart
- 2009 - Eurocrypt – sklonowanie dowolnej karty Mifare Classic w niecałe 10 sekund
- 2011 – wydanie edycji kart MIFARE Classic EV1- edycja niewrażliwa na znane wówczas ataki i wstecznie kompatybilna z dotychczasowymi systemami
- 2015 – odkrycie ataku pozwalającego na odzyskanie kluczy z wzmocnionej wersji i ostateczna decyzja o migracji systemów opartych na Mifare Classic do produktów o wyższym poziomie bezpieczeństwa

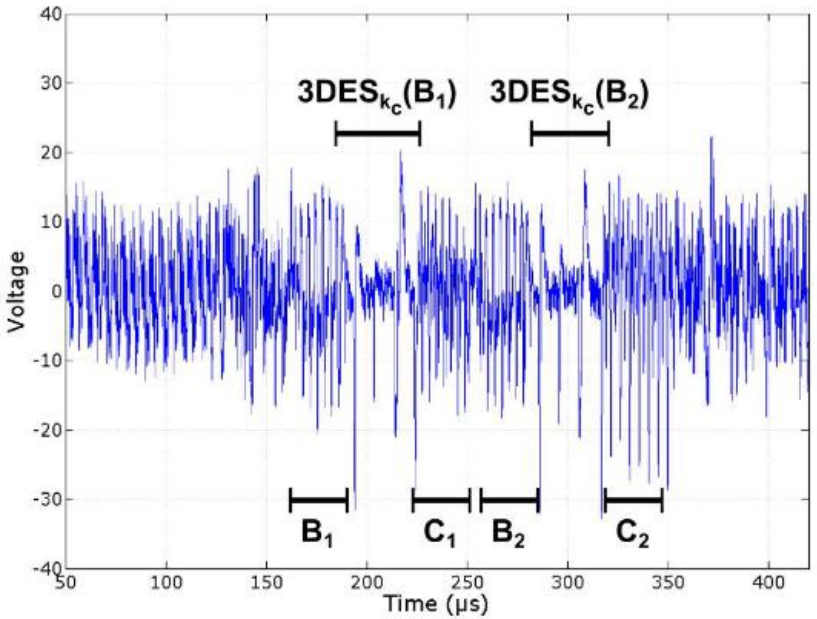
Ataki na Mifare Ultralight i Mifare DESFire

- 2010/11 – David Oswald and Christof Paar of Ruhr-University in Bochum
- 2012 – EU SecWest Amsterdam – Interpidus – manipulacja kartą przy pomocy aplikacji dostępnej w systemie Android

Analiza sygnału podczas uwierzytelnienia – inżynieria wsteczna



(a) Step 1



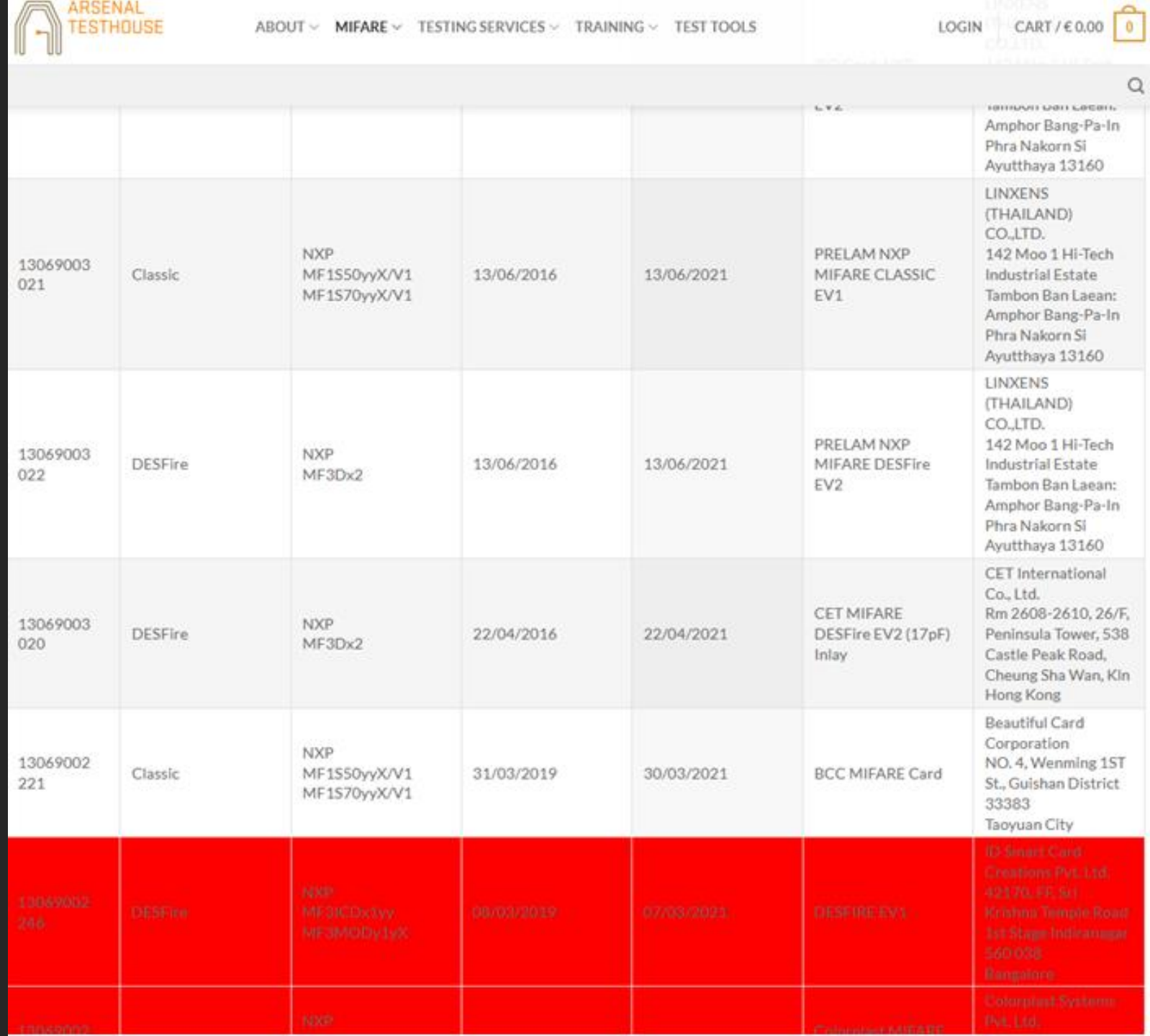
(b) Step 2

Sposoby ochrony przed podatnościami

W celu uniknięcia manipulacji i klonowania kart chipowych należy podjąć odpowiednie działania:

- Korzystanie z zróżnicowanych kluczy zalecanych przez NPX
- Wielopoziomowe środki zaradcze – bezpieczeństwo systemu końcowego dla indywidualnej infrastruktury
- Blokowanie skradzionych i zgubionych kart przez operatora – konieczność implementacji mechanizmów, które to umożliwiają po stronie właściciela systemu
- Implementacja mechanizmów detekcji manipulacji
- Korzystanie z usług firm zajmujących się certyfikacją np. Arsenal Testhouse

Przykładowa lista certyfikowanych produktów Mirfare za strony firmy Arsenal Testhouse



ARSENAL TESTHOUSE

ABOUT MIFARE TESTING SERVICES TRAINING TEST TOOLS LOGIN CART / € 0.00 0

						Amphor Bang-Pa-In Phra Nakorn Si Ayutthaya 13160
13069003 021	Classic	NXP MF1S50yyX/V1 MF1S70yyX/V1	13/06/2016	13/06/2021	PRELAM NXP MIFARE CLASSIC EV1	LINXENS (THAILAND) CO.,LTD. 142 Moo 1 Hi-Tech Industrial Estate Tambon Ban Laean: Amphor Bang-Pa-In Phra Nakorn Si Ayutthaya 13160
13069003 022	DESFire	NXP MF3Dx2	13/06/2016	13/06/2021	PRELAM NXP MIFARE DESFire EV2	LINXENS (THAILAND) CO.,LTD. 142 Moo 1 Hi-Tech Industrial Estate Tambon Ban Laean: Amphor Bang-Pa-In Phra Nakorn Si Ayutthaya 13160
13069003 020	DESFire	NXP MF3Dx2	22/04/2016	22/04/2021	CET MIFARE DESFire EV2 (17pF) Inlay	CET International Co., Ltd. Rm 2608-2610, 26/F, Peninsula Tower, 538 Castle Peak Road, Cheung Sha Wan, Kln Hong Kong
13069002 221	Classic	NXP MF1S50yyX/V1 MF1S70yyX/V1	31/03/2019	30/03/2021	BCC MIFARE Card	Beautiful Card Corporation NO. 4, Wenming 1ST St., Guishan District 33383 Taoyuan City
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]
[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]

Źródła

1. https://pl.wikipedia.org/wiki/Mifare

2. https://en.wikipedia.org/wiki/MIFARE

2. https://www.mifare.net/en/about-mifare/

3. https://www.emsec.ruhr-uni-bochum.de/media/crypto/veroeffentlichungen/2011/10/10/desfire_2011_extended_1.pdf

4. https://www.theregister.com/2011/10/10/mifare_desfire_smartcard_broken/

5. https://www.trojmiasto.pl/wiadomosci/Luka-w-systemie-pozwala-ladowac-karty-miejskie-biletami-na-wiele-lat-i-za-darmo-n65714.html

6. https://uitspraken.rechtspraak.nl/#zoekverfijn/ljn=BD7578&so=Relevance

7. http://arsenal-testhouse.com/certified-mifare-products/

8. https://blog.cryptographyengineering.com/2011/10/11/desfire/

9. http://www.cryptotech.com.pl/Produkty/karty_Mifare,content.html