

# Vybrané aspekty bezpečnosti RFID

Tomáš Rosa

[crypto.hyperlink.cz](http://crypto.hyperlink.cz)



INVESTICE DO ROZVOJE VZDĚLÁVÁNÍ

*Tento projekt je spolufinancován Evropským sociálním fondem a státním rozpočtem České republiky.*

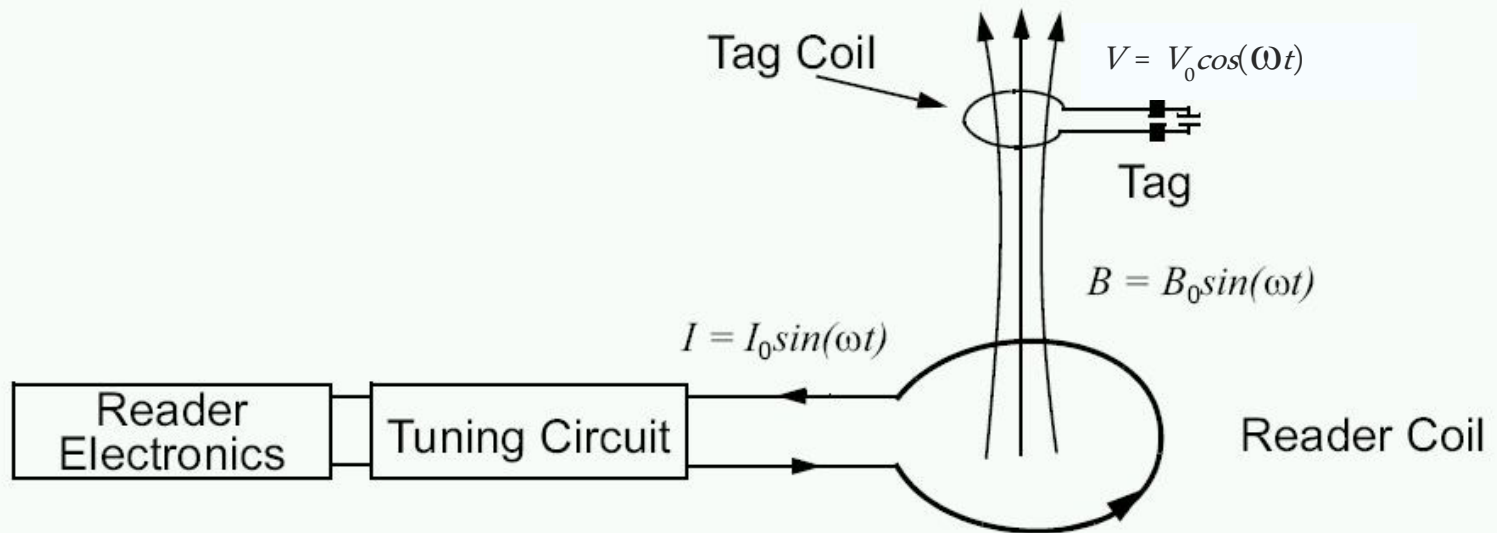
# Přehled pasivních čipů „RF“

- Radio-klasifikace bezkontaktních čipů
  - Čipy v pásmu LF (100 až 150 kHz)
  - Karty s vazbou na dálku v pásmu HF (13.56 MHz)
  - Karty s vazbou na blízko v pásmu HF (13.56 MHz)
  - Čipy v pásmu UHF (stovky MHz až jednotky GHz)
  
- Mnoho různých provedení
  - Karty, přívěsky, štítky, etikety, implantáty,...
  
- RFID – Radio Frequency Identification
  - Chápeme jako konkrétní způsob využití čipů RF.

# [ Fyzická vrstva pásem LF a HF ]

- Využívá chování tzv. blízkého magnetického pole vysílače.
  - Klasická vlna ještě není plně zformována, přenos energie vnímán přes magnetickou složku pole.
  - Na soustavu antény vysílače a přijímače je nahlíženo jako na vysokofrekvenční transformátor.
  - Principiální mez cca  $300/2\pi f$ , [m; MHz].
    - Důležité pro návrh řádných zařízení, útočník se však podle svého cíle může řídit jiným fyzikálním modelem!

# Anténní soustava

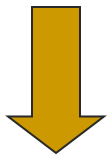


[Lee: AN710, Microchip 2003]

- Přenos energie (informace) v soustavě kruhových antén

# Ilustrace blízkého pole

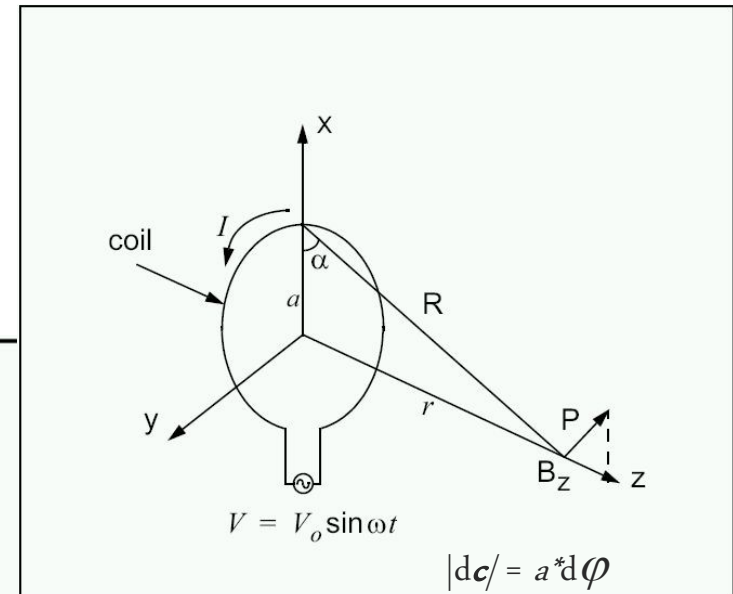
Biot-Savart:  $d\mathbf{B} = \mu_0 NI(\mathbf{R} \times d\mathbf{c}) / (4\pi |\mathbf{R}|^3)$



integrace pro ideální kruhovou  
cívku

$$B_z = \frac{\mu_0 INa^2}{2(a^2 + r^2)^{3/2}}$$

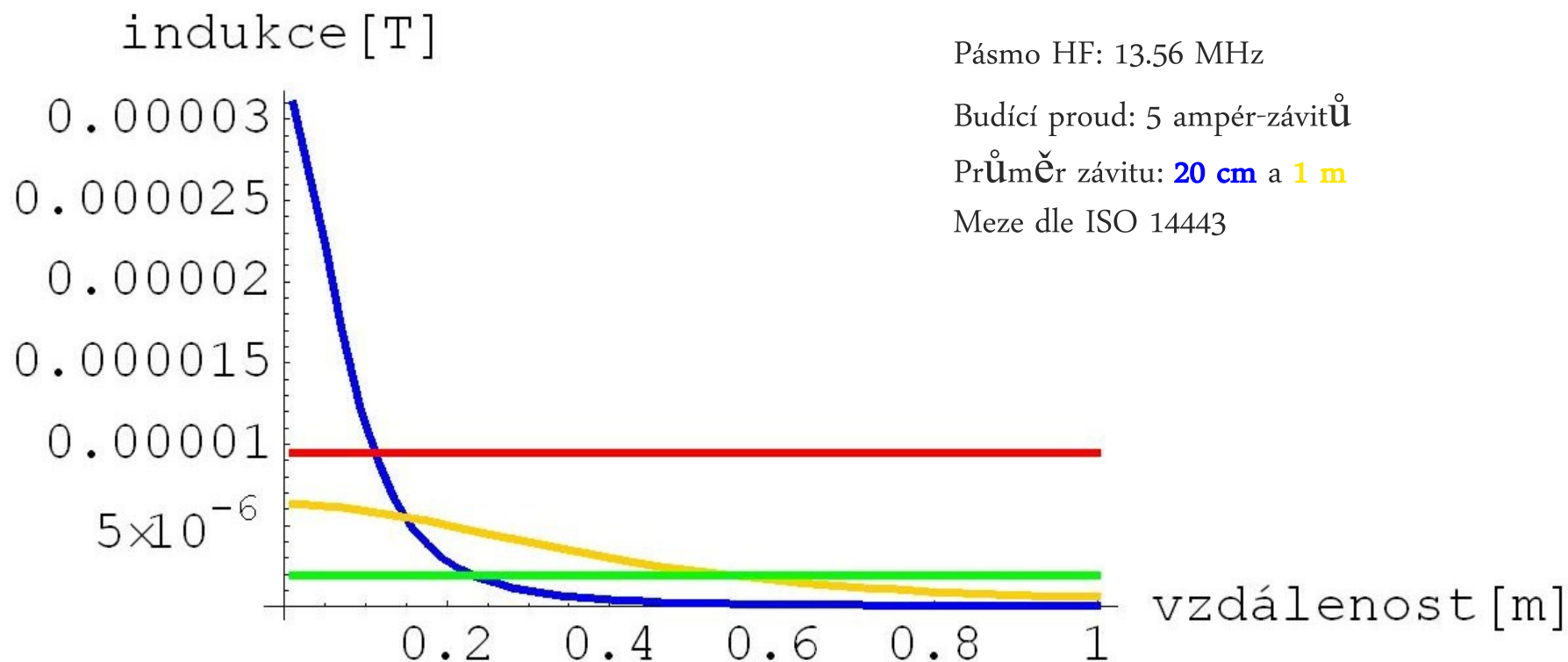
$$= \frac{\mu_0 INa^2}{2} \left( \frac{1}{r} \right) \quad \text{for } r^2 \gg a^2$$



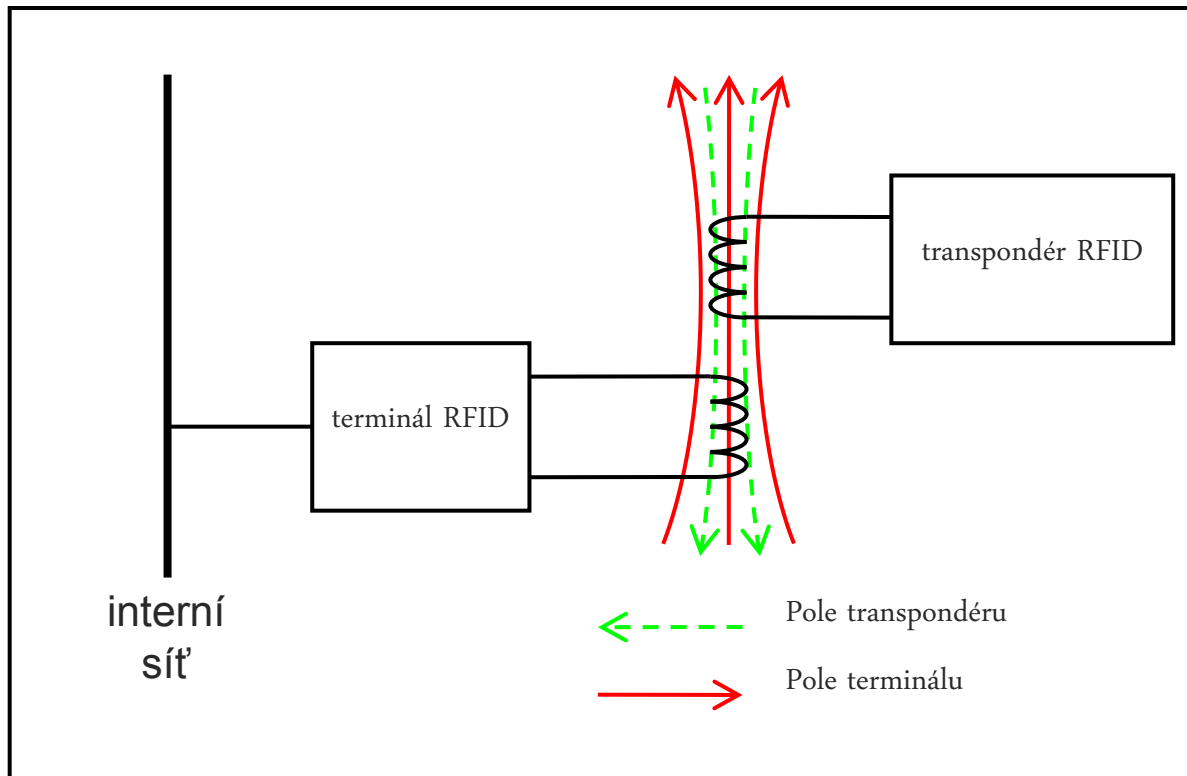
[Lee: AN710,  
Microchip 2003]

Optimálně - s ohledem na minimum budícího proudu – pak vychází  $a = r^* \sqrt{2}$ .

# [ Pole na ose kruhové antény ]



# Komunikace s transpondérem



Terminál: přímá amplitudová modulace základní nosné

Čip: zátěžová modulace vedoucí k nepřímé amplitudově/fázové modulaci základní nosné

# Odhady útočných vzdáleností pásem LF a HF

- Aktivní komunikace s čipem
  - desítky cm
  - ve variantě „write only“ až jednotky m
- Odposlech – terminál i čip
  - jednotky m
- Odposlech – pouze terminál
  - desítky m
- Aktivní komunikace s terminálem
  - desítky m

# RFID v přístupových systémech

- Pro naprostou většinu přístupových systémů v ČR v současnosti platí, že používají
  - buď tzv. transpondéry unikátního ID v pásmu LF,
  - anebo karty MIFARE (Classic) v pásmu HF.

# [ Transpondéry unikátního ID ]

- Sériová paměť naprogramovaná při výrobě či personalizaci čipu
- V poli terminálu automaticky cyklicky vysílá svůj obsah
- Přenos není nijak kryptograficky chráněn
  - Čip sdělí svůj obsah komukoliv
  - Terminál naslouchá komukoliv
- Příklady: „Unique ID“, HID Prox, INDALA

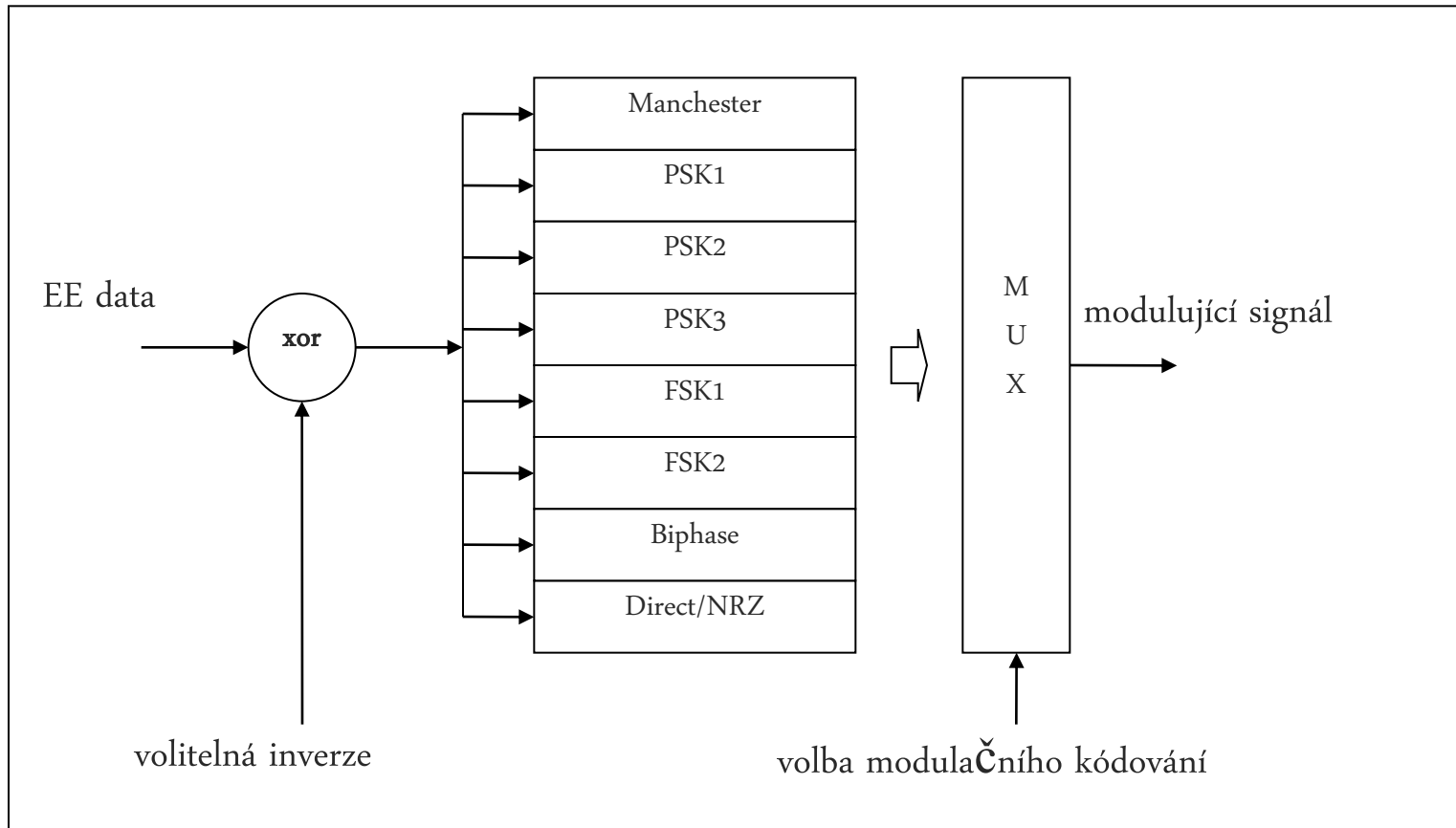
# [ Co nám vlastně brání... ]

- Je důležité uvědomit si, co útočník rozhodně nemusí:
  - Pochopit význam dat uložených v paměti transpondéru. Ta někdy bývají i šifrována.
- Nutnou a postačující podmínkou k vytvoření klonu je:
  - Efektivně popsat posloupnost řídicí zátěžovou modulaci transpondéru s cílem dokázat její projev dostatečně věrně zopakovat.

# [ Q5 – Královna pásma LF ]

- Programovatelný transpondér
  - 330 bitů EEPROM, z toho 224 bitů k libovolnému využití
  - široká podpora modulačních schémat
- Variabilita provedení – přívěsek, karta, atp.
- Zatím dokázala emulovat všechny testované transpondéry unikátního ID v pásmu LF
- Volně v prodeji 😊

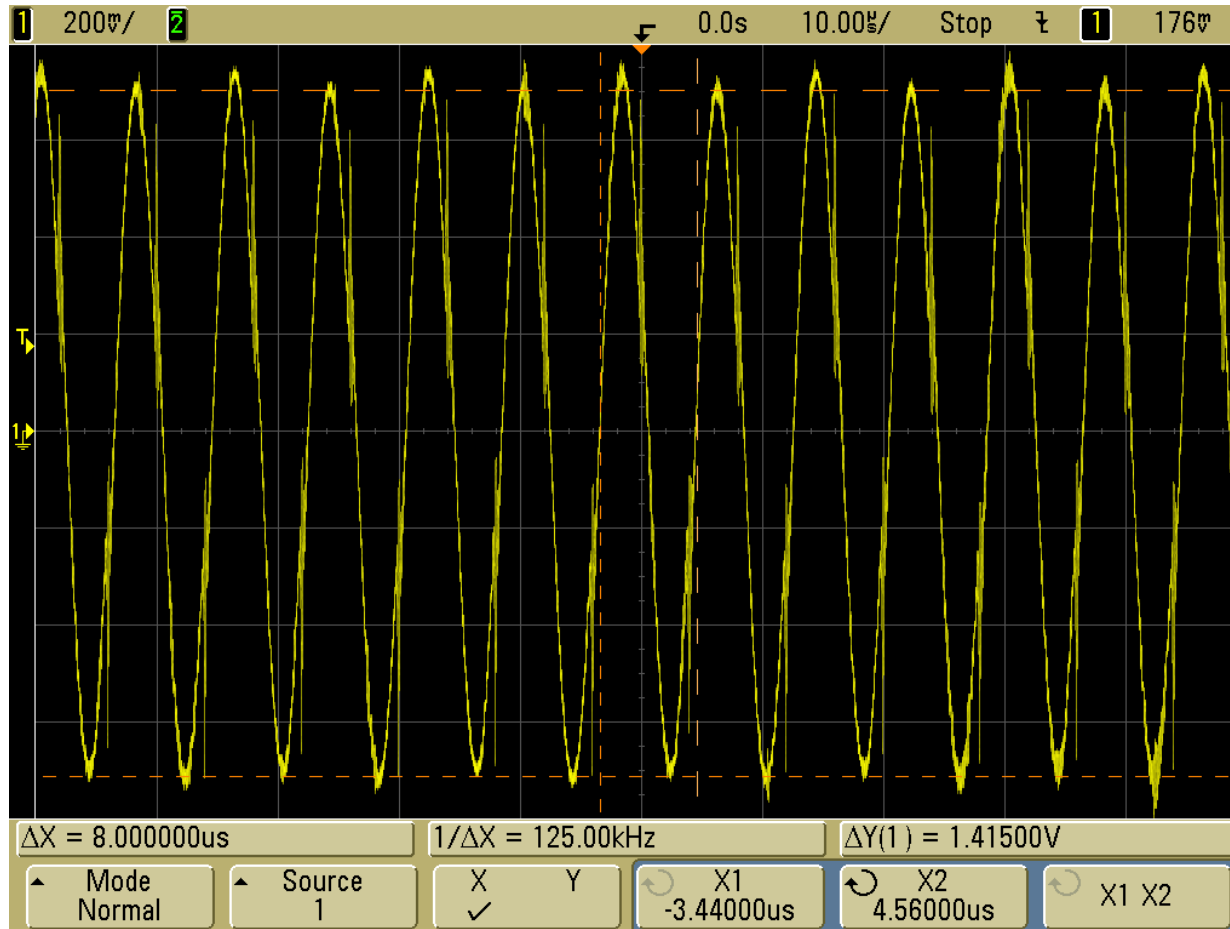
# Q5 – výstupní kodér



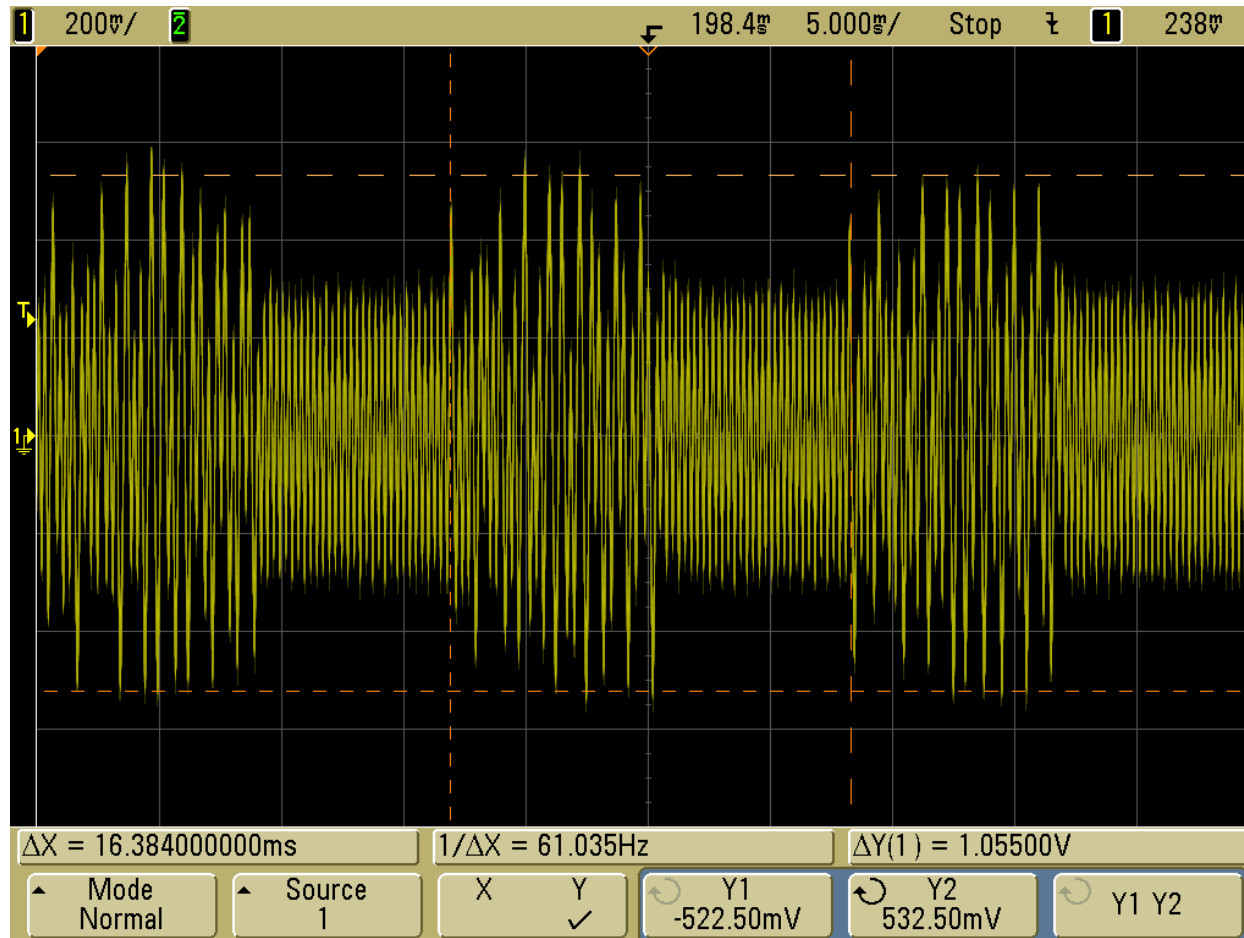
# [ Útok s využitím Q5 ]

- Fáze I – popis signálu originálního čipu
  - Teoreticky složitá úloha, ale... v technické praxi se málokdy setkáme s unikátem.
  - Nechme se vést možnostmi Q5!
  
- Fáze II – výroba duplikátu
  - Popis signálu uložíme do paměti Q5 a naprogramujeme výstupní kodér...

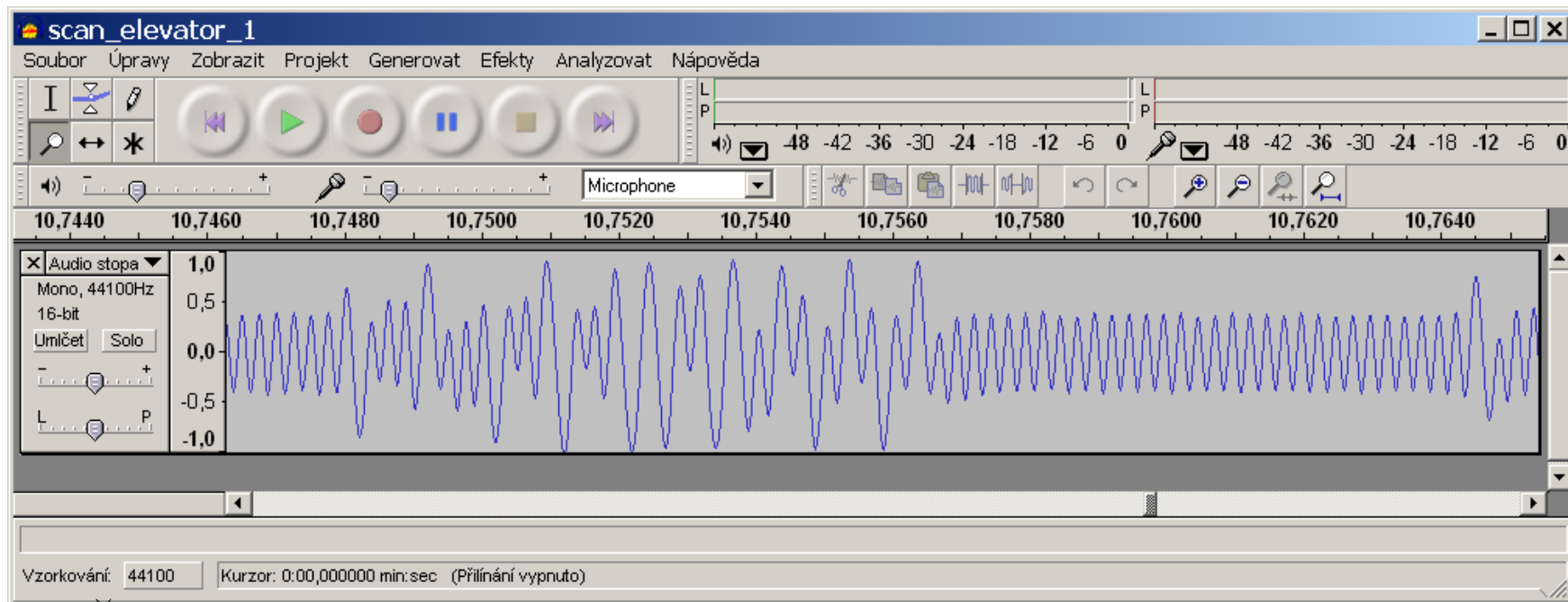
# Příklad projevu pomocné nosné na základní nosné



# Po detekci AM: Pomocná nosná s fázovou modulací



# Záchyt cestou ve výtahu



Čip v pásmu LF, vzdálenost od autentizující se osoby cca 0,5 m.

Přijímač Sangean ATS 909W.

Podrobnosti viz ST 7/2008, [crypto.hyperlink.cz/cryptoprax.htm](http://crypto.hyperlink.cz/cryptoprax.htm).

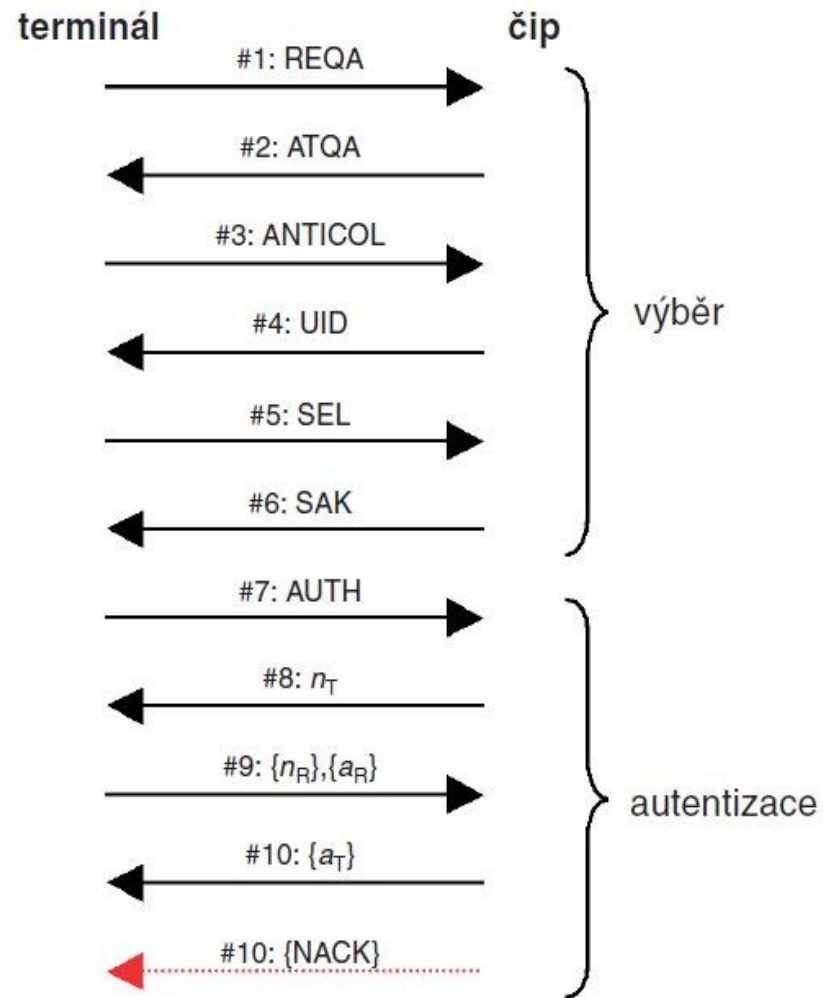
# [ Takže, tedy... ]

- Rodina „Unique ID“
  - přímý kód manchester, rychlost  $f/64$ , 64 bitů celkem
  - konfigurační slovo Q5: 60 01 F0 04
- INDALA (1 konkrétní konfigurace)
  - pomocná nosná  $f/2$  s fázovou modulací, obraz délky 64 modulačních znaků
  - konfigurační slovo Q5: 60 00 F0 A4
- HID Prox (1 konkrétní konfigurace)
  - 2 pomocné nosné  $f/8$  a  $f/10$ , frekvenční klíčování, obraz délky 96 modulační znaků
  - konfigurační slovo Q5: 60 01 80 56

# [ MIFARE Classic ]

- Existují dva základní druhy použití:
  - Režim „jen UID“, který je de facto ekvivalentní transpondérům unikátního ID.
    - Snadno prolomitelné vhodným emulátorem.
  - Režim „kryptografický“, který využívá obousměrnou autentizaci čipu a terminálu.
    - Totálně prolomeno v letech 2007-2009. V současnosti existují desítky útoků, všechny prakticky schůdné s devastujícími následky.

# [ Chybový postranní kanál ]



# [ Využití postranního kanálu ]

- Jeden úspěšný dotaz na čip poskytuje až 12 bitů informace o tajném klíči (48 b).
  - 8 platných paritních rovnic plus 4 rovnice ze známého otevřeného textu odpovědi (NACK: 0x5)
- 4 dotazy by měly stačit k útoku hrubou silou
  - Předpokládá intenzivní použití hradlových polí
    - stroj COPACOBANA na bázi Spartan3 či jiná konstrukce s Virtex5 LX50
  - Výsledek do cca hodiny
  - Samotný sběr dat ovšem trvá jen několik vteřin

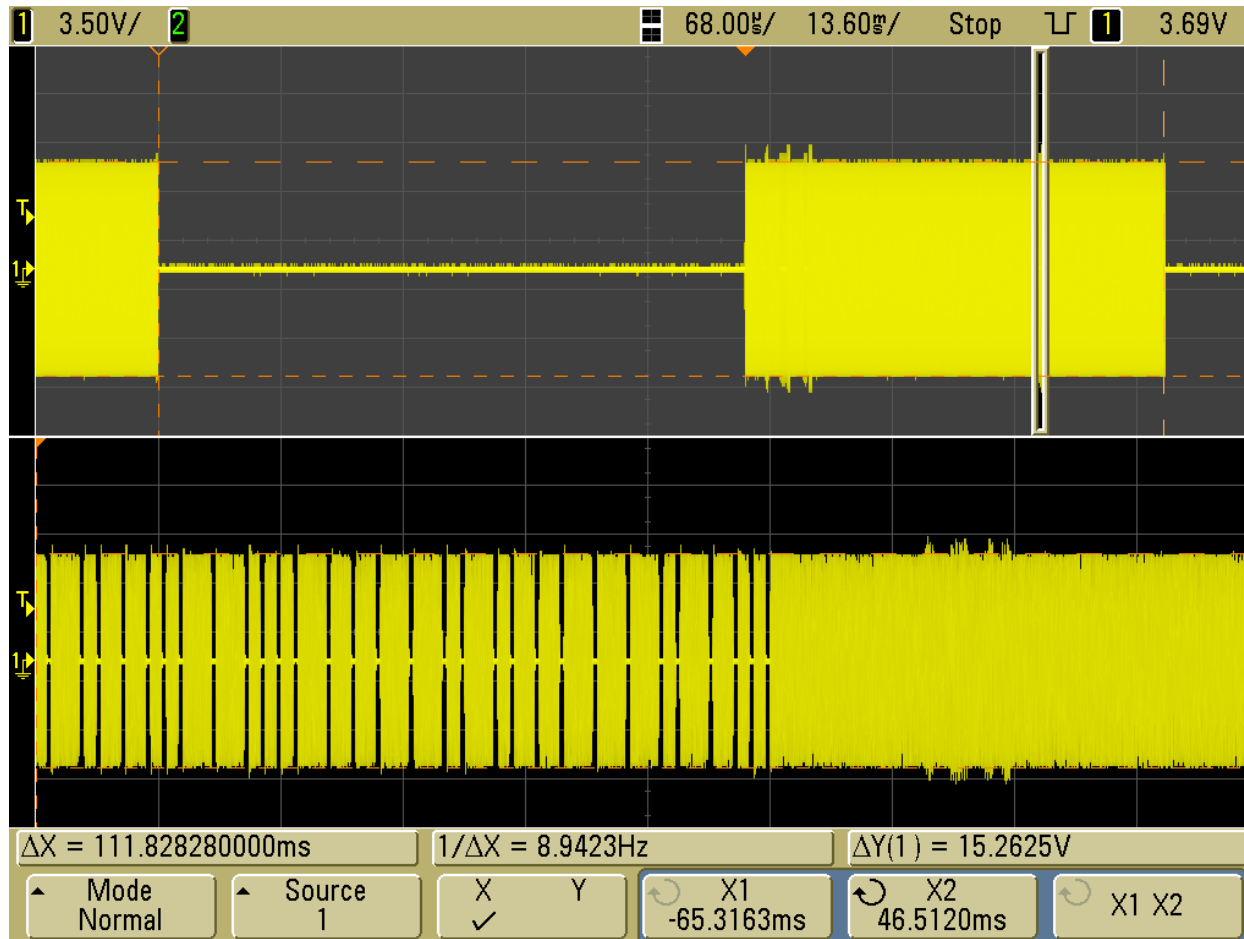
# [ Jak se obejít bez FPGA ]

- Rekapitulace známých slabin MF Classic
  - Krátká délka klíče algoritmu Crypto1 (48 bitů)
  - Kvazistabilita PRNG
  - Nevhodné napojení nelineárního filtru na LFSR
  - Podmíněné multidiferenciály nelineárního filtru
  - Chybový postranní kanál v autentizačním protokolu
  - Nevhodné pořadí aplikace šifrování a bezp. kódů
  - ...

# [ Optimalizovaný útok ]

- Lze provést na běžném PC za pomoci upravené čtečky.
  - Úprava spočívá ve specifickém časování za účelem stabilizace PRNG.
  - Při praktickém ověřování byla využita vývojová čtečka EMDB408.
    - [http://www.asicentrum.cz/cz\\_01\\_07\\_05.php](http://www.asicentrum.cz/cz_01_07_05.php)
  - Podrobnosti viz Sdělovací technika 8/2009.
    - <http://crypto.hyperlink.cz/cryptoprax.htm>

# Praktický útok - úspěšný dotaz



# [ Kryptoanalýza MF Classic ]

- Celková rekapitulace (původní i nové útoky)
  - Možnost získání tajného klíče interakcí útočníka s terminálem (čtečkou)
  - Možnost získání tajného klíče z odposlechnuté relace mezi čtečkou a čipem MF (stačí jen strana čtečky – lze na desítky metrů daleko)
  - Možnost získání tajného klíče pouhou interakcí s čipem MF
    - Zcela devastující útoky pro řadu aplikací typu elektronických peněženek a legitimací (MHD, atp.)

# [ MIFARE Classic – co dál? ]

## ■ MIFARE DESFire

- Řadu slabín odstraňuje, ale řadu nových potenciálních zranitelností zavádí!
- Evidentně nezvládnuté propojení kryptografie s aplikačním protokolem.
- Hrozí útoky těžící z nevhodných konfigurací – karta k nim sama dost navádí...

## ■ MIFARE Plus

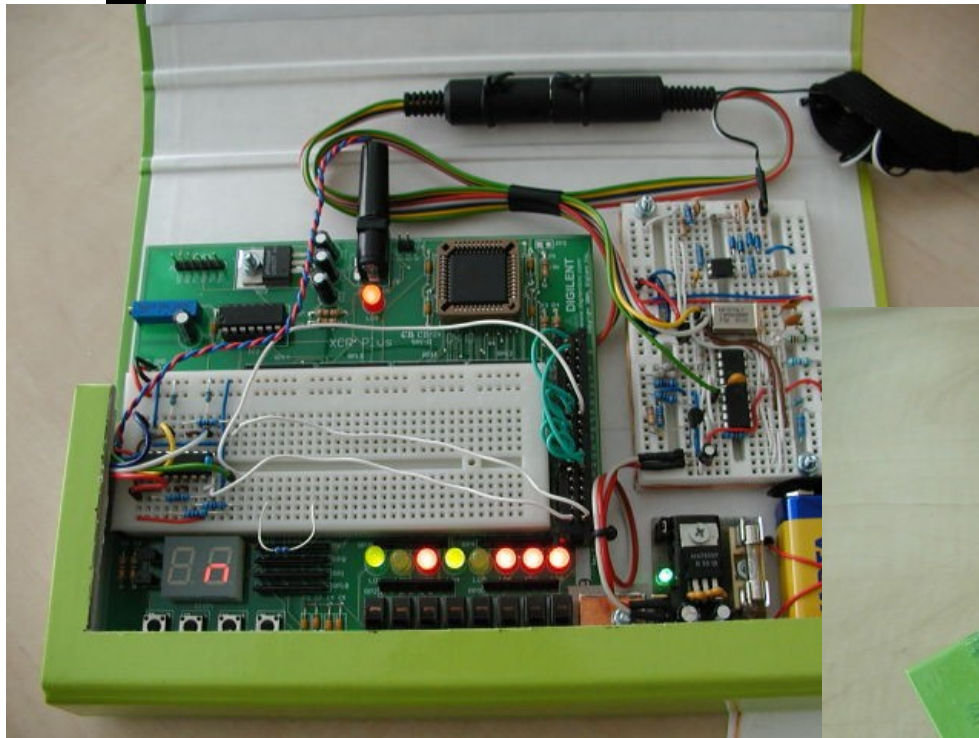
- První vzorky jsou snad již (s nejméně ročním zpožděním) k dispozici, dokumentace je neveřejná.

# [ MIFARE „jen UID“ ]

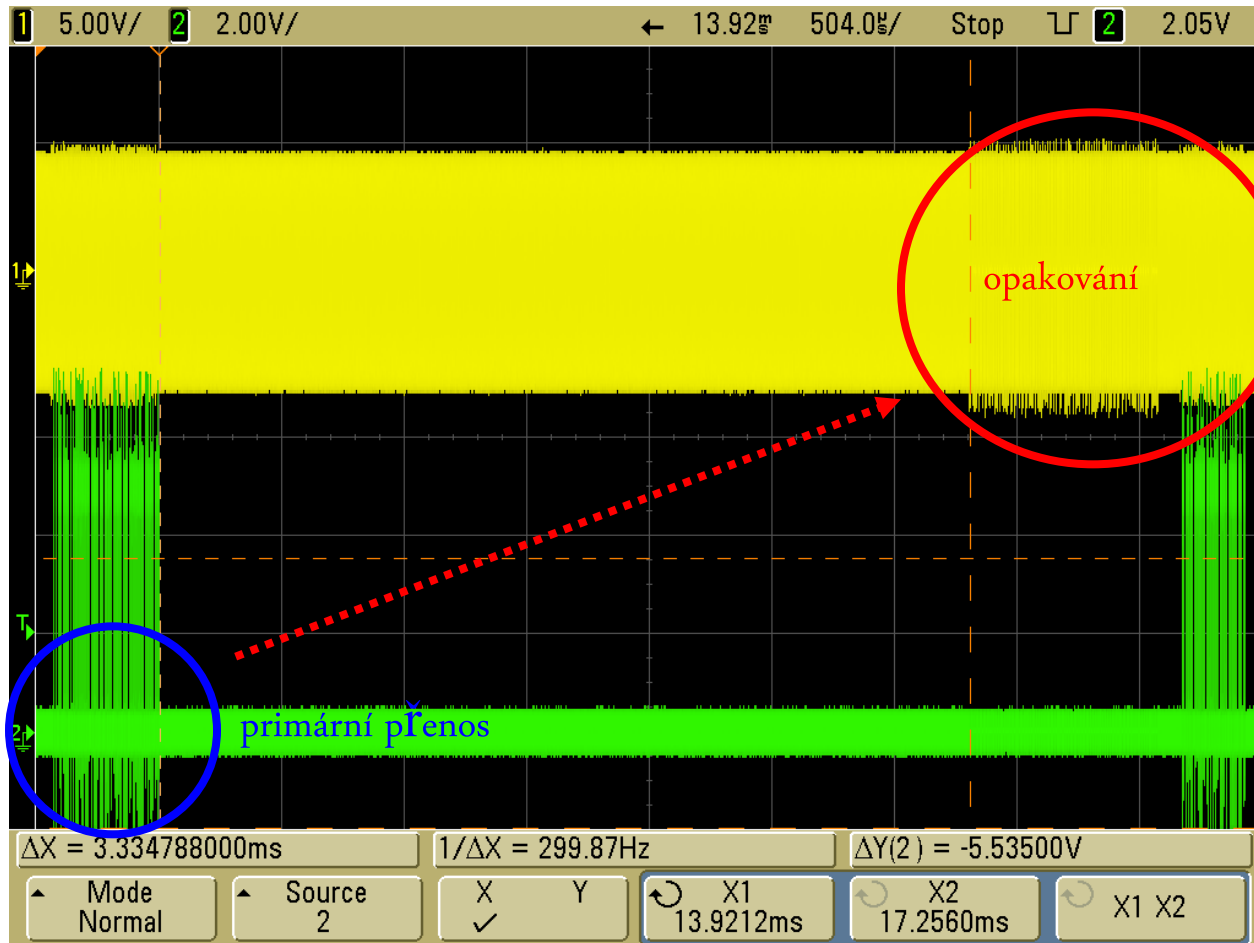
- Časté použití MIFARE **Classic** i **DESFire**.
- V řadě aspektů je výsledek horší než u transpondérů unikátního ID v pásmu LF.
  - Standardizovaný protokol (ISO14443A)
  - Odposlech UID možný na desítky metrů daleko
- Jistou překážkou je absence čipu á-la Q5 v pásmu HF.
  - Nutno použít emulátor – například PicNic.



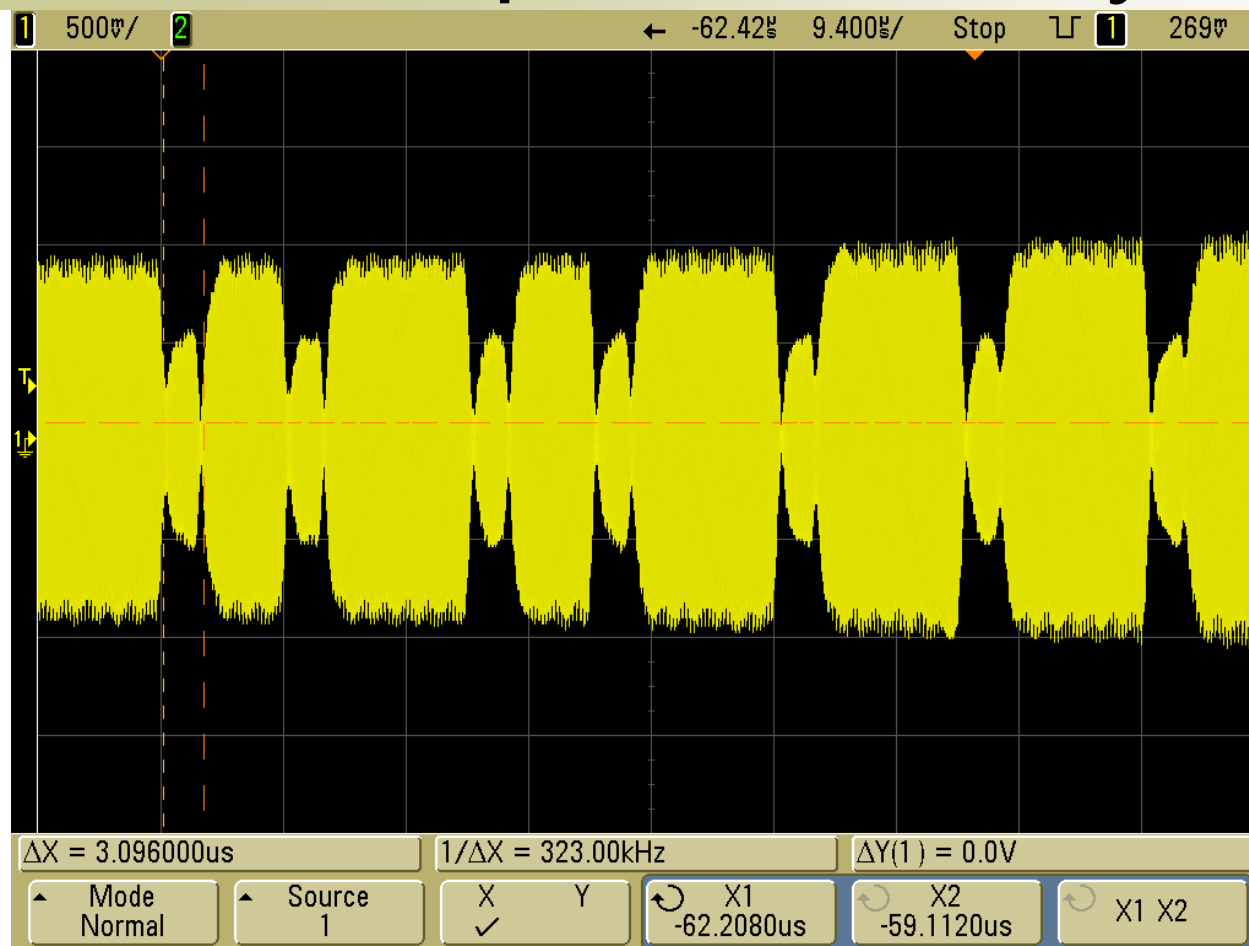
# PicNic & CPLD koprocesor in natura



# [ K odposlechu hodnoty UID ]



# Konkrétní podoba záchytu



Přijímač AOR AR8600MK2, výstup KV mf 10,7 MHz.  
Vzdálenost cca 2 m, nejméně 2 čtečky v poli.

# [ Inherentní hrozby ]

- Jakékoliv jednoznačné konstantní identifikátory v principu umožňují
  - jednak aktivní i pasivní(!) radiolokaci zájmové osoby,
  - jednak aktivní i pasivní(!) parciální rádiový skimming transpondéru.
    - Využitelnost samozřejmě dále závisí na architektuře navazující aplikace.

# UID lze často získat i jinak...

Danový doklad č.: PD-08-002-5396  
 DUZP: 1.12.08  
 \_\_\_\_\_, s.r.o.  
 PS-08-002-9080 \_\_\_\_\_ 1.12.08 11:07

1x Zampionova polevka	29,00	A
1x Cocka se sazenym vejcem	69,00	A
1x Bonaqua neperliva 0,5l	20,00	A
<b>Sleva 5%</b>	-6,00	
<b>CELKEM</b>	<b>112,00</b>	

3cf2e2da9000 15 ROSA TOMAS  
 Zam. Karta 112,00  
 9% DPH/VAT 9,30 (102,70) 112,00 A

Puvodni zustatek: **395,00**  
 Novy zustatek: **283,00**

Kromě placení  
 obědů je ta samá  
 karta využita i v  
 přístupovém  
 systému.  
 Samozřejmě...

# [ Jasně doporučení ]

- Zcela eliminovat jakékoliv jednoznačné konstantní identifikátory čipu RFID.
- Tím se předejde slabinám, které:
  - zavádí jednak jejich samotná přítomnost,
  - dále ochotně dotvářejí vývojáři navazujících aplikací – viz dále.



# Příklad

## OpenCard v Městské knihovně v Praze

- Data potřebná k emulaci lze získat:
  - Aktivním rádiovým skimmingem (na vzdálenost menší než 30 cm).
  - Možná i pasivním odposlechem při použití karty oprávněnou osobou (na vzdálenost až desítek metrů).
    - Hypotetická možnost, která nebyla testována v praxi.
    - Rovněž nebyla rozvíjena použitelnost „masových“ skimmingových, respektive emulačních nástrojů z [www.libnfc.org](http://www.libnfc.org).

# Příklad

## OpenCard v Městské knihovně v Praze

- Doporučení: Aktivovat si doplňkové (nepovinné) přihlašovací heslo.
  - Jinak hrozí krádež identity a únik veškerých osobních údajů, které knihovna o daném držiteli vede.
- Silným heslem lze riziko prakticky eliminovat, nicméně od „**multifunkční chytré čipové karty**“ bychom snad čekali trochu víc.
  - Na druhou stranu i u „tvrdé“ integrace je vhodné zavést heslo (PIN) jako ochranu proti zneužití zcizené karty.
  - Pravdou je, že v praxi se obvykle setkáme spíš s primitivními a přímočarými útoky...

# Příklad

## Osobní údaje vedené v MKP

```
<?xml version="1.0" encoding="windows-1250" ?>
- <xml>
  <Prijmeni>ROSA</Prijmeni>
  <Jmeno>Tomáš</Jmeno>
  <TitulPred />
  <TitulZa>Ph.D.</TitulZa>
  <DatumNarozeni>██████████1974</DatumNarozeni>
  <Pohlavi>muž</Pohlavi>
- <OsobniDoklad>
  <Druh>OP</Druh>
  <Cislo>██████████</Cislo>
</OsobniDoklad>
- <TrvaleBydliste>
  <Ulice>██████████</Ulice>
  <Misto>██████████</Misto>
  <Posta>Praha ██████████</Posta>
  <PSC>██████████</PSC>
  <Okres>PH ██████████</Okres>
  <Stat>CZ</Stat>
</TrvaleBydliste>
+ <KorespondencniAdresa>
  <Telefon>██████████, ██████████</Telefon>
  <Email>tomas.rosa@rb.cz</Email>
</xml>
```

**Žádnou paniku, prosím!**  
**Raději si nastavte heslo.**  
**Instrukce podá [web MKP](#)**

# Bezkontaktní platební karty

- V naprosté většině případů pracují v pásmu HF dle ISO 14443 A/B.
- První vlna byla nasazena v USA.
  - Cílem bylo co nejméně měnit stávající infrastrukturu pro online akceptaci magnetického proužku.
  - V důsledku toho trpí bezpečnost těchto karet zásadními nedostatky [7].
- Uvidíme, jak obstojí druhá, vylepšená vlna, která nyní postupuje Evropou...

# [ Hlavní zranitelnosti první vlny ]

- Možnost rádiového skimmingu [7]
  - Obraz karty byl úspěšně zneužit jednak pomocí emulátoru karty, jednak při platbě přes internet.
  - Fatální při absenci dynamicky generovaných kontrolních kódů CVV/CVC.

# [ Hlavní zranitelnosti první vlny ]

- Možnost přímého čtení osobních údajů držitele karty [7]
  - Karta terminálu útočníka bez jakékoliv autentizace ochotně „prozradila“
    - PAN (číslo karty),
    - datum expirace karty,
    - jméno držitele karty.

# Hlavní zranitelnosti první vlny

- Možnost útoku typu DoS [7]
  - Některé karty obsahují čítač, který se nevyhnutelně a nevratně inkrementuje s každou zahájenou transakcí.
  - Toto je opatření mj. proti RF-skimmingu.
  - Nepozorované zvyšování hodnoty čítače však může kartu zablokovat.

# [ NFC – věc, o které se hovoří ]

- Near Field Communication
  - Další komunikační rozhraní vedle Bluetooth, IrDA, ZigBee, atd.
- Významným atributem je cílený přesah s oblastí pasivního RFID v pásmu HF.
  - Popsáno v ISO/IEC 18092 a navazujících standardech, viz <http://www.nfc-forum.org/home/>.

# [ NFC v kostce ]

- Zařízení vybavené řadičem NFC může komunikovat v následujících modech:
  - režim terminálu (de facto čtečka),
  - režim pasivního cíle (de facto emulátor transpondéru),
  - obousměrný aktivní režim (novinka v NFC).
- Některé stávající terminály a transpondéry pro pasivní RFID lze též vnímat jako částečné(!) implementace standardu NFC.

# [ NFC coby nástroj útočníků ]

- Zajímavý je režim emulace pasivního transpondéru.
- V současnosti je běžně podporován zejména standard ISO 14443 A.
- Utajováním a naivními úpravami rozhraní se výrobci radičů NFC snaží bránit útokům na původní aplikace pasivního RFID.
  - Zejména jde aplikace typu „UID-only“.
  - Více viz projekt [www.libnfc.org](http://www.libnfc.org).

# [ NFC coby cíl útoků ]

- Nativní aplikace založené na NFC zatím v praxi chybí.
- Přirozeně lze očekávat, že se zde samo NFC stane cílem útoků.
  - Například tzv. chytré etikety se mohou pokusit injektovat škodlivý kód do mobilního telefonu, atp.

# [ NFC a marketing ]

- Rozlišujeme řadič NFC
  - obvod zajišťující komunikaci od (zhruba) transportní vrstvy dolů
  - středem zájmu je hlavně rádiová komunikace a navazující protokoly
- Versus telefon GSM s NFC
  - telefon vybavený řadičem NFC a příslušnou službou aplikační úrovně (e.g. platební kartou)
  - středem zájmu jsou tahanice o to, kde bude jaká část aplikace uložena a kdo, komu, kolik zaplatí

# [ Závěr ]

- RFID je bezesporu perspektivní technologií.
  - Skutečný rozmach technických aplikací nejspíš teprve přijde.
- Úroveň bezpečnosti však často poněkud zaostává za běžným standardem oblasti IS/IT.
  - Široký prostor pro aplikovaný výzkum v oblasti analýzy zranitelností a návrhu protiopatření.
  - Zásadní úlohou je mj. najít prakticky použitelnou ochranu proti tzv. přepojovacímu útoku.
  - I „menší“ úlohy však mají svůj smysl.
  - Mimo jiné je záhodno bránit se povinnému používání nebezpečných produktů.

[ Děkuji za pozornost... ]



Tomáš Rosa

[crypto.hyperlink.cz](http://crypto.hyperlink.cz)

# Reference

1. Courtois, N.-T.: *The Dark Side of Security by Obscurity and Cloning MiFare Classic Rail and Building Passes Anywhere, Anytime*, rev. May 2009, <http://eprint.iacr.org/2009/137>
2. EM4094 – Analog Front End Integrated Circuit for 13.56MHz RFID Base Station, EM Microelectronic-Marin SA, SWATCH Group, 2005
3. EMD408 – EM4094 RFID Reader, Support Tools, EM Microelectronic-Marin SA, SWATCH Group, 2005
4. Finkenzeller, K.: *RFID Handbook*, 2nd edition, John Wiley & Sons, 2003
5. Garcia, F.-D., et al.: *Dismantling MIFARE Classic*, ESORICS 2008, pp. 97-114, 2008
6. Garcia, F.-D., et al.: *Wirelessly Pickpocketing a Mifare Classic Card*, IEEE S&P 09, May 2009
7. Heydt-Benjamin, T.-S., Bailey, D.-V., Fu, K., Juels, A., and O'Hare, T.: *Vulnerabilities in First-Generation RFID-Enabled Credit Cards*, In Proc. of Financial Cryptography and Data Security 2007
8. Myslík, J.: *Elektromagnetické pole - základy teorie*, BEN - technická literatura, 1998
9. Nohl, K, and Plötz, H.: *MIFARE – Little Security, Despite Obscurity*, 24th Chaos Communication Congress, 2007, <http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html>
10. Nohl, K., et al.: *Reverse-Engineering a Cryptographic RFID Tag*, USENIX 2008

Viz také odkazy uváděné lokálně v průběhu přednášky.