

Płatności NFC: fakty i mity

Łukasz Siewierski



XVII Konferencja na temat bezpieczeństwa teleinformatycznego
SECURE 2013

Warszawa, 9 – 10 października 2013

1 Historia

- 1 Wypukłe karty / MOTO
- 2 Pasek magnetyczny
- 3 EMV: chip + PIN

2 Płatności zbliżeniowe: prawie-EMV/MagStripe-over-NFC

3 Ataki



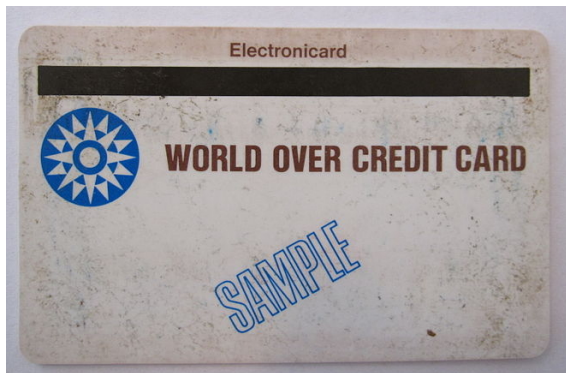







- card security code (CSC)
- card verification data (CVD)
- card verification number (CVN)
- card verification value (CVV2)
- card verification value code (CVVC)
- card verification code (CVC2)
- verification code (V-code or V code)
- card code verification (CCV)
- signature panel code (SPC)



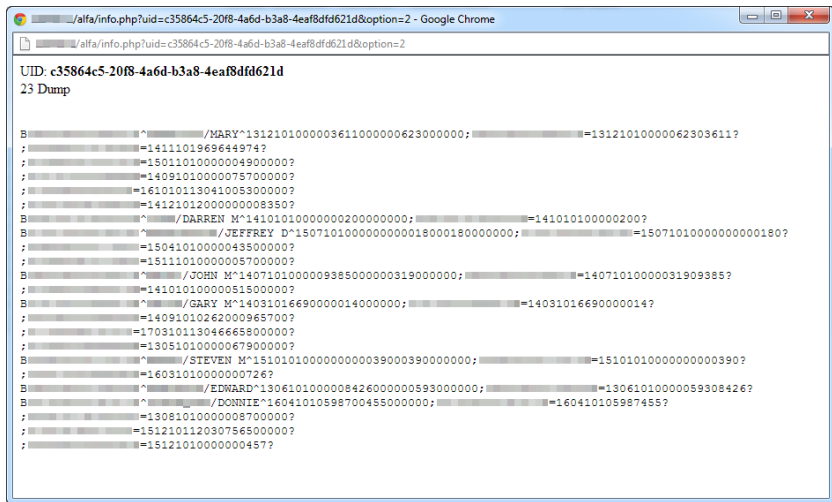
Pasek Magnetyczny (MagStripe)



1 B  ^  /MARY^131210100000361100000062300000

2 ;  =13121010000062303611?

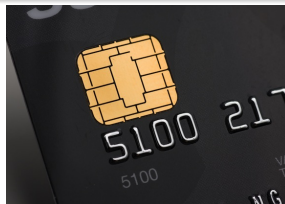
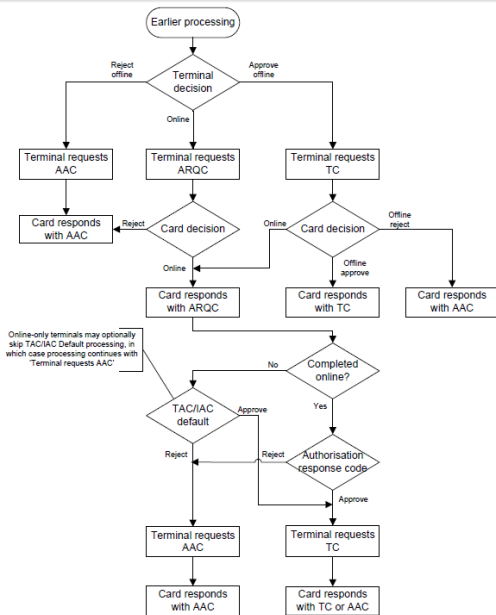
Pasek Magnetyczny (MagStripe)



The screenshot shows a web browser window with the address bar containing the URL: `/alfa/info.php?uid=c35864c5-20f8-4a6d-b3a8-4eaf8dfd621d&option=2`. The page content displays the following information:

```
UID: c35864c5-20f8-4a6d-b3a8-4eaf8dfd621d
23 Dump

B [redacted]^ [redacted]/MARY^13121010000003611000000623000000; [redacted]=13121010000062303611?
; [redacted]=1411101969644974?
; [redacted]=15011010000004900000?
; [redacted]=14091010000075700000?
; [redacted]=1610101130410053000000?
; [redacted]=14121012000000008350?
B [redacted]^ [redacted]/DARREN M^1410101000000020000000; [redacted]=141010100000200?
B [redacted]^ [redacted]/JEFFREY D^150710100000000018000180000000; [redacted]=15071010000000000180?
; [redacted]=15041010000043500000?
; [redacted]=151110100000005700000?
B [redacted]^ [redacted]/JOHN M^14071010000009385000000319000000; [redacted]=14071010000031909385?
; [redacted]=14101010000051500000?
B [redacted]^ [redacted]/GARY M^140310166900000014000000; [redacted]=140310166900000014?
; [redacted]=14091010262000965700?
; [redacted]=170310113046665800000?
; [redacted]=13051010000067900000?
B [redacted]^ [redacted]/STEVEN M^151010100000000003900039000000; [redacted]=15101010000000000390?
; [redacted]=160310100000000726?
B [redacted]^ [redacted]/EDWARD^130610100000842600000059300000; [redacted]=13061010000059308426?
B [redacted]^ [redacted]/DONNIE^1604101059870045500000; [redacted]=160410105987455?
; [redacted]=13081010000008700000?
; [redacted]=151210112030756500000?
; [redacted]=15121010000000457?
```





- Kompatybilność wsteczna z EMV,
- Kompatybilność wsteczna z paskiem magnetycznym (MagStripe – MasterCard)
- Standardy: NFC (13.56 MHz), ISO/IEC 14443 Type A,
- Szybciej niż EMV (bez PIN, zgoda przez zbliżenie),
- Karta nie jest podawana sprzedawcy (choć...)

Zagrożenia

- Płatność nie tylko kartą,
- Możliwość podsłuchania i zainicjowania komunikacji,
- Zbliżenie karty != zgoda na jej odczytanie.

Zagrożenia

- Płatność nie tylko kartą,
- Możliwość podsłuchania i zainicjowania komunikacji,
- Zbliżenie karty != zgoda na jej odczytanie.

Zabezpieczenia

- CVV3,
- Brak imienia i nazwiska (MasterCard),
- Niemożliwa weryfikacja PIN offline.

- *wedge vulnerability / no-PIN attack* (Murdoch, Drimer, Anderson et al., 2010),

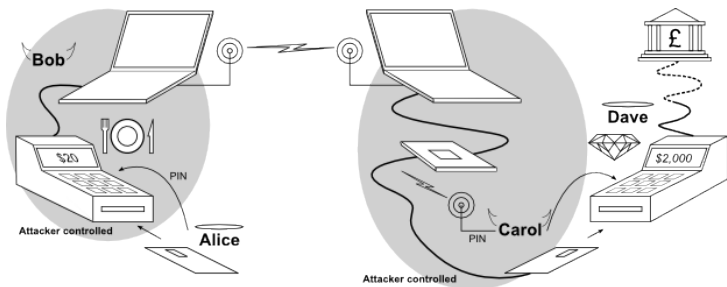
- *wedge vulnerability / no-PIN attack* (Murdoch, Drimer, Anderson et al., 2010),
- *pre-play attack* (Bond, Choudary, Murdoch et al., 2012),

- *wedge vulnerability / no-PIN attack* (Murdoch, Drimer, Anderson et al., 2010),
- *pre-play attack* (Bond, Choudary, Murdoch et al., 2012),
- klonowanie paska magnetycznego,

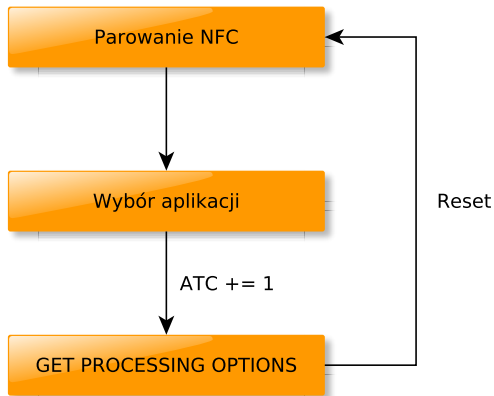
- *wedge vulnerability / no-PIN attack* (Murdoch, Drimer, Anderson et al., 2010),
- *pre-play attack* (Bond, Choudary, Murdoch et al., 2012),
- klonowanie paska magnetycznego,
- klonowanie wypukłych kart.

Ataki: relay attack

Drimer, Murdoch, 2007



Application Transaction Counter (ATC) – 2 bajty (0 – 65535)



Czas trwania: ok. 100 minut

Dziękuję za uwagę

Ta prezentacja nie byłaby taka atrakcyjna graficznie, gdyby nie:

- \LaTeX oraz klasa beamer (jak i wiele innych paczek),
- Wikimedia Commons i obrazki, które udostępnia na licencji GPL oraz Creative Commons,
- film pt. *Ile waży koń trojański?*, z którego pochodzi kadr zaprezentowany na jednym ze slajdów,
- Blog <http://www.xylibox.com/>, z którego pochodzi zrzut ekranu z danymi pasków magnetycznych,
- techvibes.com, shoreline-solutions.com, z których pochodziły niektóre zdjęcia.