


# PayPass Vulnerabilities

Balázs Bucsay – http://rycon.hu - earthquake_at_rycon_dot_hu
PR-Audit Kft. – http://www.praudit.hu/

# PayPass

“PayPass™ lets you make everyday purchases without having to swipe the magnetic strip on your MasterCard® card or provide your signature*. It's faster than fumbling with cash or waiting for change, and it makes checkout easier than ever.”
https://www.paypass.com/tap_and_go/index.html

„Hagyományos vásárlás esetén a kártyát át kell adnia a kereskedőnek, míg a MasterCard PayPass vagy Maestro PayPass kártya esetében nem kell kiadnia kezéből a kártyáját. Ez csökkenti a kártya érzékeny adatainak másolási lehetőségét.
A kártyában működő dinamikus adatvédelmi eljárásoknak és a korszerű azonosítási megoldásoknak köszönhetően a MasterCard PayPass vagy Maestro PayPass kártya használata során visszaélésre felhasználható ügyfél adatok nem „hallgathatóak le”.
http://www.paypass.hu/

# VIDEO: “Barclays contactless cards users exposed to fraud”


http://www.youtube.com/watch?v=AGWFryVh_oE

# History

- First mentioned by Edward Bellamy in a novel – 1887
- Used to buy fuel – 1920
- Western Union issued to frequent customers – 1921 (paper card stock)
- Later: Air lines, Diners Club
- BankAmericard, first modern credit card - 1958

# ISO/IEC 7810 & 7812

ISO/IEC 7810 tells about the characteristics:

- Physical dimensions
- Resistance to bending, flame, chemicals, temperature and humidity
- Toxicity

ISO/IEC 7812 is about the numbering:

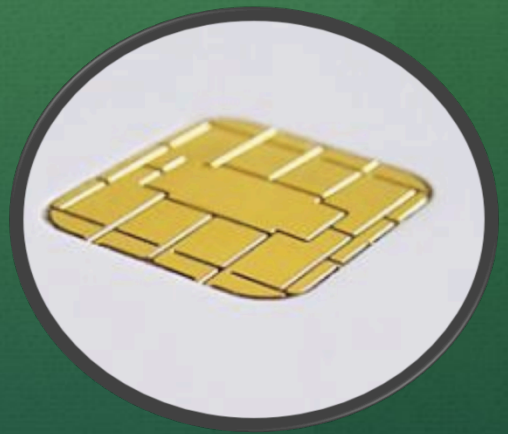
- Numbering system (MII, IIN)
- Application and registration procedures

# Magnetic Stripe Cards

- Iron based magnetic particles on a band
- Readable/rewriteable
- ISO/IEC 7811 – Recording technics
- ISO/IEC 7813 – physical characteristics & track data structures
- Track 1 & Track 2 structures
- Very easy to read and write

# Smart Cards

- ISO/IEC 7816 – All basic details about chips
- APDU – Application Protocol Data Unit
- Sending APDU, getting back error codes and/or data
- Own operating system, basically a microcomputer
- Very hard to copy



# EMV
# Europay-MasterCard-Visa

- Defines the interaction at physical, electrical, data and application level between chip and processing device
- 4 books
- Based on ISO/IEC 7816
- Well defined data structure
- EMV based cards can have different apps
- Every issuer has different applications/AIDs

# EMV Based Chip Cards

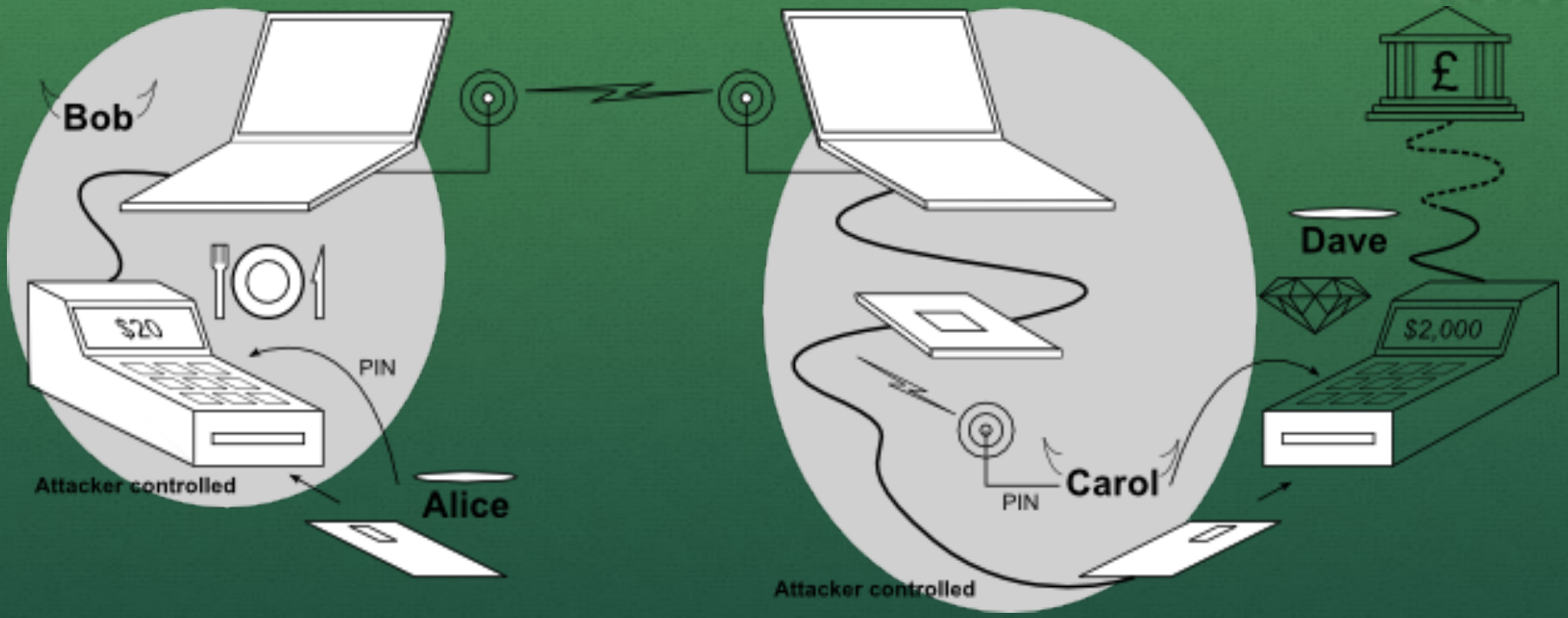
Secure because:

- Very hard to copy
- Challenge based authentication
- Signed transactions
- Risk management on both sides

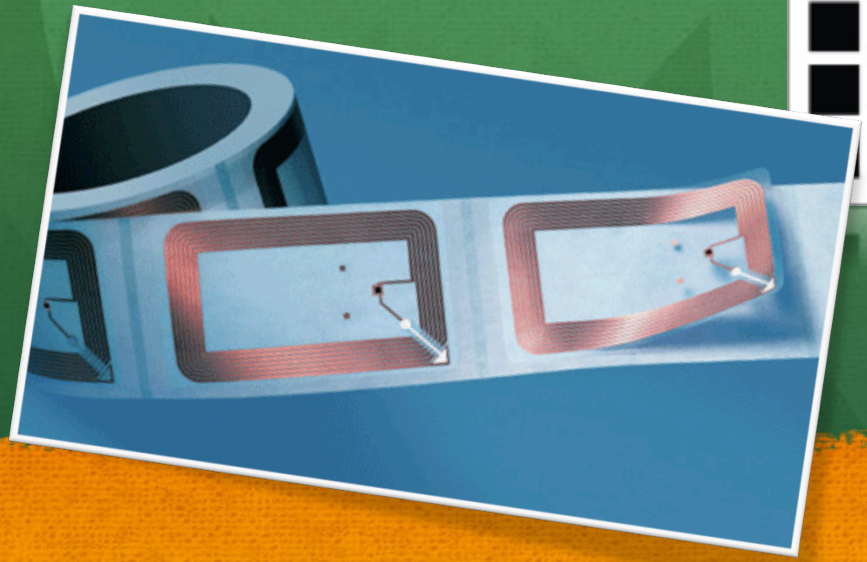
But vulnerable for some attacks!

# Chip & PIN (EMV) relay attacks

by Saar Drimer and Steven J. Murdoch


Bob
$20
PIN
Attacker controlled
Alice
£
Dave
$2,000
PIN
Carol
Attacker controlled

# Radio Frequency Identification RFID



- Wireless communication over RF
- Active, passive and battery assisted tags
- Active tag energizes the passive tag
- Many types of frequencies, standards and working distances
- Used everywhere, e.g. animals, food, entry systems

# Near Field Communication NFC


- Slice of RFID
- Based on ISO/IEC 14443
- Founded by Nokia, Philips and Sony in 2004
- NFC standard is the ISO/IEC 18092 and 21481
- Frequency is 13,56MHz (HF)
- Only 4-10cm is the working distance
- Mostly ISO/IEC 7816 is used for communication
- Mifare, Oyster, Metapay, Passports, PayPass etc…

# NFC based cards in use

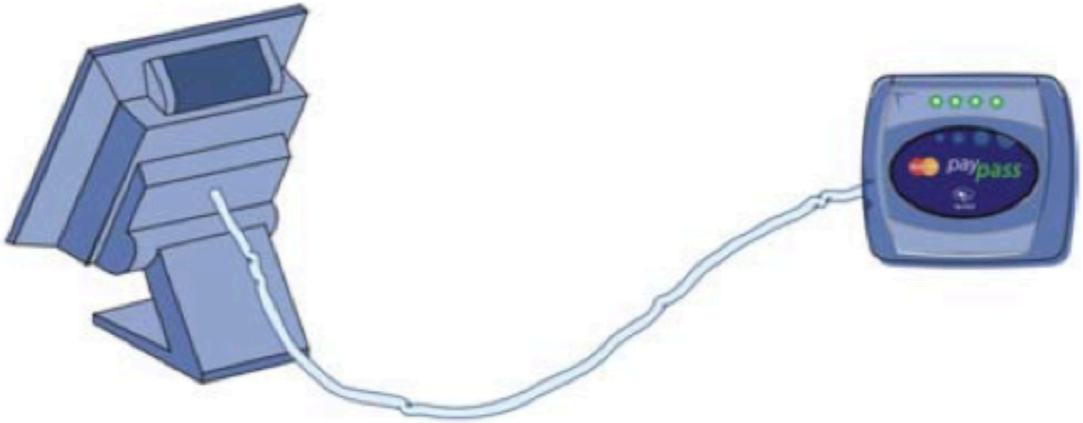
| Card | Vulnerable |
| --- | --- |
| • Mifare Classic | • Cracked in 2007 |
| • Oyster card | • Cracked in 2008 |
| • Passports | • Can be cloned (partially) 2008 |
| • Mifare Desfire | • Cracked in 2011 |
| • Metapay | • Is it vulnerable? |
| • PayPass | • Let's see and decide yourself |
| • Google Wallet | • Vulnerable for relay attack (maybe more) |

# The new generation: PayPass

# PayPass

- You can request cards at least in 6 Banks in Hungary
- Contactless payment
- Very quick
- No signature or PIN required until a certain limit
- NFC based -> ISO/IEC 14443
- EMV is here too!
- There are two types “Mag Stripe” and “M/Chip”


EMBEDDED READER




EXTERNAL READER

# Mag Stripe vs. M/Chip

"**Two generic types** of card products are part of the **PayPass** program: **PayPass—Mag Stripe and PayPass—M/Chip.**

PayPass—**Mag Stripe** was developed to allow PayPass payments using authorization networks that presently support **magnetic-stripe authorization** for credit or debit applications. Security has been enhanced with the introduction of a **new Cardholder Verification Code (CVC)** for these transactions. The new CVC is referred to as **CVC3** and may be **a Static or Dynamic** value depending on the issuer's card implementation. There is some terminal processing required to support using CVC3 which all PayPass approved terminals will have implemented. CVC3 usage does not impact acquirer host systems or networks.

PayPass—**M/Chip** was developed to allow PayPass payments in markets that support EMV. PayPass—M/Chip terminals support **EMV Chip data in authorizations and clearing**. They also **support** acceptance of PayPass—**Mag Stripe cards** and cardholder devices. PayPass—M/Chip terminals may optionally support current payment acceptance methods e.g., contact EMV and magnetic stripe."

http://www.paypass.com/pdf/public_documents/PayPass-MChip%20Acquirer%20Implementation%20Requirements.pdf

# What's on the card?

- It uses EMV
- Stores Track 1 and Track 2 data
- CVC3 – static, "dynamic" and dynamic value (depends on the issuer)
- Cardholder's first and last name, expiration date
- Transaction counter, service number, etc.

# Mag Stripe transaction

- Terminal energizes and associates with the cards
- Sends a request for details (open directories and files)
- Card sends back the requested data
- Terminal acts almost the same like it were a magnetic stripe cards

# What did I have?

- A Touchatag reader ~27€ (ACR122U)
- “Pálinka Fesztivál” payment card
- Computer with USB support e.g. Raspberry PI

# What did I know?

Nothing about the card, just an nfc-list output!

# What have I done??

- A lots of Google research about RFID, NFC, PayPass
- Struggling with PCSCD, libnfc for one or two months
- Read almost all of those ISO and other standards
- Play with the existing nfc based tools
- And finally the card answered!

# Summary of the research

- The PayPass cards are supporting the EMV standard, so we have to write a new EMV compliant reader or modify an old one.
- JavaEMVReader just fine!
- After modifying the JavaEMVReader to be compatible with the ACR122U reader and the nfc stadard, it is working like a charm, mostly
- The PayPass Mag Stripe doesn't have all the EMV standard implemented. For example: no cryptography support
- With a cheap hardware and existing tools, it is possible to read all of the containing data from a short distance

# About the finding

- PayPass Mag Stripe is weak, this is well known for a few years
- I found this vulnerability in February&March, 2012
- There were plenty prezentations, slides about this without real technical details and/or with commercial tools (external PayPass terminal)
- MasterCard knows about this for a long time
- Visa has the same technology, it's called PayWave
- Between the finding and the prezentation there are more and more ppl found/find this.
- PCI-DSS standards says: "Encrypt transmission of cardholder data across open, public networks", rly?

# Demo

# Risks & Attack Vectors

- Track 2 data can be sniffed/read from the PayPass chip and write to a magnetic stripe card
- There are merchants, whose aren't requite CVV (no need for CVV3)
- Relay attack works with PayPass too, not only Chip&PIN
- There are reports about that the 4-10cm distance can be increased to 1.5-15m!!
- It is easy to emulate a PayPass Mag Stripe card (not tested)

What do you think? Is it a safe technology in this way?

# Future and present

In 5 years time, you will have a PayPass or PayWave card

Google wallet is here, it's based on EMV too, same as PayPass Mag Stripe, but isn't readable, just if the device is on.


# Thank you for your attention

# Any Question?

PRAUDIT

http://www.praudit.hu

# References


- https://www.paypass.com/documentation.html - Everything about the PayPass standard
- http://www.rfidunplugged.com/pwnpass/pwnpass.py - A script for VivoPay terminal
- http://www.nfc.cc/2012/04/02/android-app-reads-paypass-and-paywave-creditcards/ - the same finding, from a different researcher
- http://ftpcontent.worldnow.com/wthr/PDF/statementscreditcardcompanies.pdf - statements about the vulnerability
- http://arxiv.org/pdf/1209.0875.pdf - Google Wallet Relay attack
- http://2012.hackitoergosum.org/blog/wp-content/uploads/2012/04/HES-2012-rlifchitz-contactless-payments-insecurity.pdf - Hacking the NFC credit cards for fun and debit ;)

# References


- http://www.cl.cam.ac.uk/research/security/banking/relay/ - Chip & PIN (EMV) relay attacks
- http://www.shmoocon.org/2012/videos/CreditCardFraud.m4v - Kristin Paget - Credit Card Fraud: The Contactless Generation