Unleashing EMV Cards

For Security Research

Tomáš Rosa

crypto.hyperlink.cz

Remember…

- The one and only purpose of this lecture is to promote rigorous academic research of payment cards security.
  - *Any presentation of possible results shall obey all the rules of academic ethics as well as of responsible vulnerability disclosure paradigm…*

Agenda

- EMV card transaction process essentials – contact interface
- Certain immediate issues
- CAP/DPA overview
- Contactless cards – RF interface
- Certain immediate issues
- NFC and payment cards

Foreword

- EMV is a Europay-MasterCard-VISA general chip payment cards application framework.
  - It is publicly available at www.emvco.org as EMV Book 1-4.
  - This presentation cannot substitute the Books. It shall rather serve as a quick reference guide for security researchers.
- Card associations, however, define their own non-public extensions of EMV.
  - Whenever possible, we are basing on the pure EMV.
  - If a particular out-of-EMV topic is presented, we are basing on publicly reachable sources only.
  - Publicly leaked documents [15] are used for examples only without being included into the rigorous citations.

Part ONE
EMV Card Transaction Process Essentials

Foreword

- We describe the whole transaction flow solely from the chip card interaction viewpoint.
  - Since we are focused on APDUs only.
- Between the steps mentioned hereafter, several decision procedures usually occur.
  - For instance – terminal/card risk management, online authorization, etc.
  - EMV book 3 gives a concise overview of them.

TLV Everywhere & Anywhere

- The data model of the whole payment card application relies on ASN.1/BER tag-length-value encoding really heavily.
  - List of general tags can be found in EMV book 3 and [5].
  - If a template is used, tag-length fields can be omitted.
- TLVs can be spread out anywhere around the application, e.g.:
  - ATR history bytes (even so…)
  - SELECT response template
  - Elementary data files (of course)
- Getting a picture of the whole card basically means catching various TLVs whenever you see them.
  - So, BE PREPARED!

Notation Regarding TLVs

- We use *(tag) to denote the Value from the particular TLV record.
  - E.g. *(9F36) is the value of ATC.
  - If the tag is not present in the particular card setup, we assume it takes its default value instead.

#1: Application Selection

- Described in EMV book 1.
- Either direct approach based on a predefined AIDs list,
- or an indirect one based on the "1PAY.SYS.DDF01" PSE redirector.
  - This is a DDF providing just one EF with several records listing available AIDs.
  - PSE stands for Payment System Environment.

Certain AIDs

VISA Electron	A0 00 00 00 03 20 10
VISA debit/credit	A0 00 00 00 03 10 10
VISA DPA	A0 00 00 00 03 80 02
MasterCard	A0 00 00 00 04 10 10
Maestro	A0 00 00 00 04 30 60
MasterCard CAP	A0 00 00 00 04 80 02

#2: Get Processing Options

- CLA=8x (80), INS=A8 (GET PROCESSING OPTIONS)
- Starts the payment transaction.
  - Besides the others, Application Transaction Counter (ATC, tag 9F36) is incremented.
- Expects variable list of initial data (PDOL, tag 9F38).
  - The list is either default, or specified in application selection response template.
- Response includes Application File Locator (AFL, tag 94).
  - List of short elementary files identifiers and record numbers.

#3: Read Application Data

- CLA=0x (00), INS=B2 (READ RECORD)
- Reads the files and records listed in AFL obtained in step 2.
  - Data structure obeys ASN.1 based TLV syntax.
  - Recall, it is not so important which file the data comes from, it is the **tag** that decides.
  - So, you have to obediently read all those records listed in AFL while collecting the TLVs you get for their later processing.

#4: Data Authentication

- Static Data Authentication (SDA)
  - Simple digital signature verification (message recovery scheme).
  - AFL indicates which records are signed.
  - No APDU activity here.
- Dynamic Data Authentication (DDA)
  - Implicit static data signature verification (via public key certificate attribute) together with a challenge-response chip authentication.
  - INTERNAL AUTHENTICATE (CLA=0x (00), INS=88).
- Combined DDA/Application Cryptogram Generation (CDA)
  - Extended form of DDA.
- Potentially interesting for side channel attacks on asymmetric cryptography (DDA and CDA employ RSA computation).
  - Further details are described in EMV books 2 and 3.

#5: Get Data

- CLA=8x (80), INS=CA
- Allows retrieving certain specific data which are not obtained during step 3.
  - ATC (tag 9F36)
  - Last Online ATC Register (tag 9F13)
  - PIN Try Counter (tag 9F17)
  - Log Format (tag 9F4F)

#6: Offline PIN Verification

- CLA=0x (00), INS=20 (VERIFY)
- Optional, execution depends on the Cardholder Verification Method chosen.
- Expects PIN blob (possibly encrypted).
- Returns OK/FAIL (unprotected).
  - Successful attack presented in [11].

#7: 1st Application Cryptogram

- CLA=8x (80), INS=AE (GENERATE AC)
- Authenticates certain transaction processing data with $\boldsymbol{MK}_{AC}$ or its derivative.
- Input data are described in CDOL1 (tag 8C) field obtained during step 3.
- Response includes CBC-MAC together with some application specific data.
  - Needs to be profiled card-by-card.

AC Types

Type	Abbreviation	Meaning
Application Authentication Cryptogram	AAC	Transaction declined
Application Authorization Referral	AAR	Referral requested by the card
Authorization Request Cryptogram	ARQC	Online authorization requested
Transaction Certificate	TC	Transaction approved

Encoded in Cryptogram Information Data (CID, tag 9F27).

#8: Issuer Authentication

- CLA=0x (00), INS=82 (EXTERNAL AUTHENTICATE)
  - Can be also part of 2nd GENERATE AC command processing.
- Occurs in transactions authorized online.
  - Processes the Authorization Response Cryptogram (ARPC, proprietary tag).
- Uses symmetric key $\boldsymbol{MK}_{AC}$ or its derivative.
  - The eventual derivation has been usually made before (e.g. in step 7).

#9: Issuer Script Processing

- Various APDUs belonging to the issuer script batch.
  - Used for card (re)personalizations, counters update, PIN unblock/change, etc.
  - Security relies on a variant of Secure Message scheme according to ISO 7816.
- Pretending the ISP activity, the attacker could also gain useful side channel data here.
  - This approach is, however, considerably more complicated and beyond the scope of this introductory lecture.

#10: 2nd App. Cryptogram

- CLA=8x (80), INS=AE (GENERATE AC)
- Completes the whole transaction.
- The same computation as in step 7, the input data, however, are described in CDOL2 (tag 8D).
  - Allows the card to reflect results from online authorization procedure.
  - Finally allows or declines the whole transaction.
  - Should be performed even if we do not plan side channel measurement for it – just to calm down the card risk mgmt.
- No more GENERATE AC commands allowed for the particular transaction.
  - Another transaction must be started (causing ++(***9F36**))…

Part TWO
Certain Immediate Issues (contact if.)

PIN-less Computation

- It is still common belief that EMV cards allow cryptographic computations only after a valid (client) PIN is presented.
- This assumption is, however, FALSE.
  - PIN (offline) verification is just a part of EMV application service (cardholder verification).
  - It is not linked to any authorization for the APDU processing itself.
  - *If the card was requiring to always perform offline PIN verification, it would be merely useless for any real life payment application.*

Prime Target

- Regardless the PIN is entered or not, the GENERATE AC command is accessible.
  - Assuming the whole application is not blocked.
- This APDU forces certain CBC-MAC computation using the card master key $\boldsymbol{MK}_{AC}$ or its ephemeral derivative.
  - $\boldsymbol{MK}_{AC}$ is a highly secure value protecting the online card authentication procedure.
- This is the very natural place where to start with e.g. side channel experiments.

Risk of $\boldsymbol{MK}_{AC}$ Disclosure

- The attacker could freely forge EMV card responses during transaction authorization.
  - For SDA-only cards, the complete duplicate of the card can be made.
  - Even for DDA or CDA cards, the attacker could still succeed with Man-In-The-Middle attack.
- In CAP/DPA application, the attacker could issue a valid transaction over the client banking account.

Notes on AC Computation

- Sometimes, there is no $\boldsymbol{MK}_{AC}$ derivation applied, the master key itself is used again and again…
  - This property is highly welcome from the side channel attacks exploration viewpoint.
- Sometimes, the $\boldsymbol{MK}_{AC}$ is shared with the contactless part of the application.
  - This allows extension of possible RF side channel attack on the whole card.

Cautionary Note on APDU Integrity Checks

- There is a weak protection of the ISO 7816 interface in between the payment card and the terminal (e.g. the POS).
  - Only certain parts of certain APDU messages are cryptographically protected.
  - The attacker can spy/modify/insert messages in this channel relatively easily, provided she has a suitable HW equipment allowing her to play the role of MITM.
  - Rather classical attack was presented in [11].

Certain Extension of [11]

- During practical verification of [11], we have met a payment cards with PIN Try Counter set to 0.
  - This actually means, that offline PIN verification was blocked. Note it seems to be the only “legal” way on how to block offline PIN, since for a majority of cards the associations require offline PIN to be in the CVM list.
  - We have been informed, that these cards:
    - support the PIN-change functionality,
    - are working correctly in POS transactions.
- Direct mounting of the “Chip&PIN Broken” attack was obviously impossible.

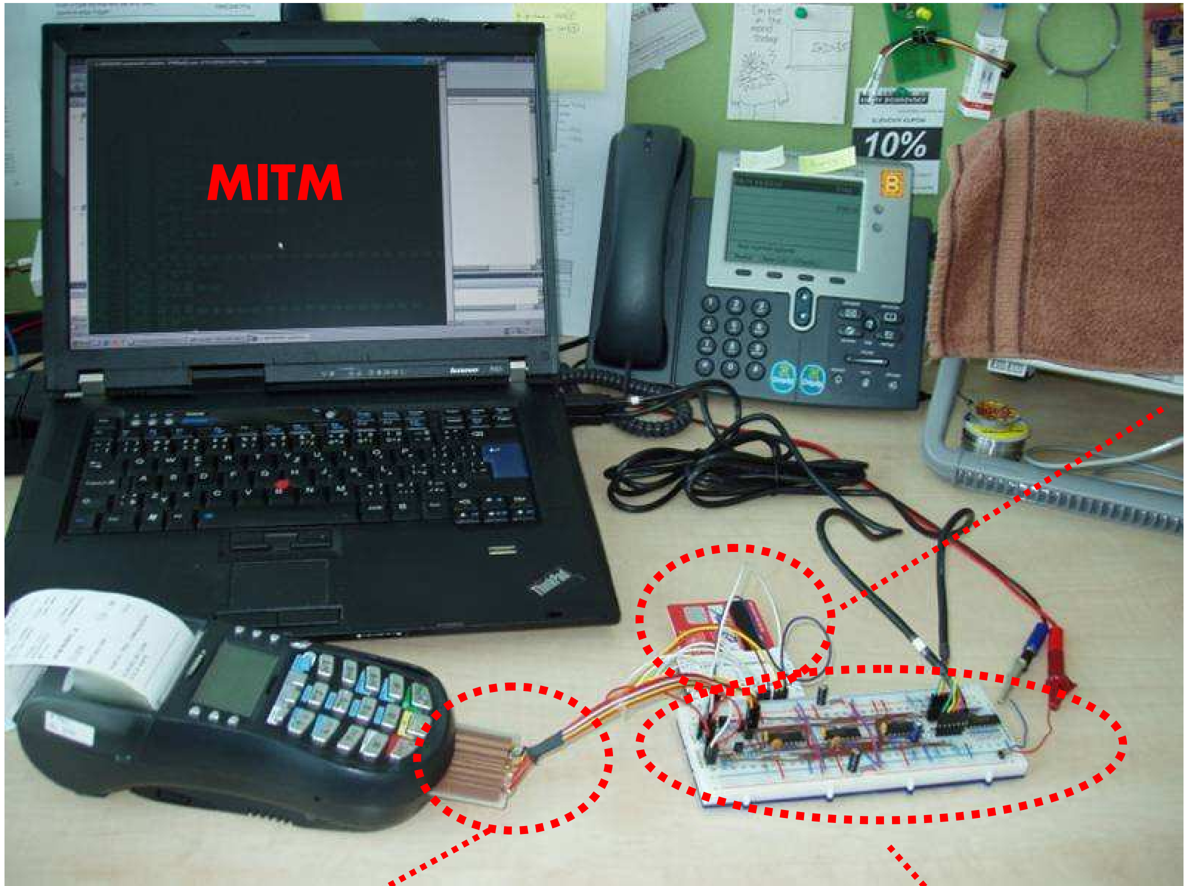
GET DATA Integrity Failure

- The PIN Try Counter is to be read by the GET DATA(9F17) command.
  - Recall there is no cryptographic integrity check for its response.
  - Extending the MITM scenario to also spoof the GET DATA response, the whole attack started working again…
  - Therefore, setting PIN Try Counter = 0 is not a countermeasure against [11].
  - Furthermore, all the data accessible through GET DATA must be considered as potential subjects to forge!

Velocity Checking Spoofing

- Another example of GET DATA integrity failure.
  - Now, we focus on Last Online ATC Register (9F13).
  - Assuming the MITM attack, it is possible to force *(9F13) = *(9F36) – 1 = ATC – 1; we further assume ATC > 1.
  - Doing so, the (offline spending) velocity checking done by a **terminal** is minimized.
  - Furthermore, the „new card“ terminal check is bypassed as well.
  - Finally, the attacker could continue spending money offline without being forced to undergo online authorization.
    - *Spending limits check done by the card is not affected this way. On the other hand, the attacker does not care for SDA/DDA cards. The attacker simply spoofs the TC response as well, since the terminal cannot check application cryptogram when working offline.*

Modest MITM Experiments



Frequently Rumored Question

- Is it possible to create working magnetic-stripe card basing on the data stored on the EMV chip?

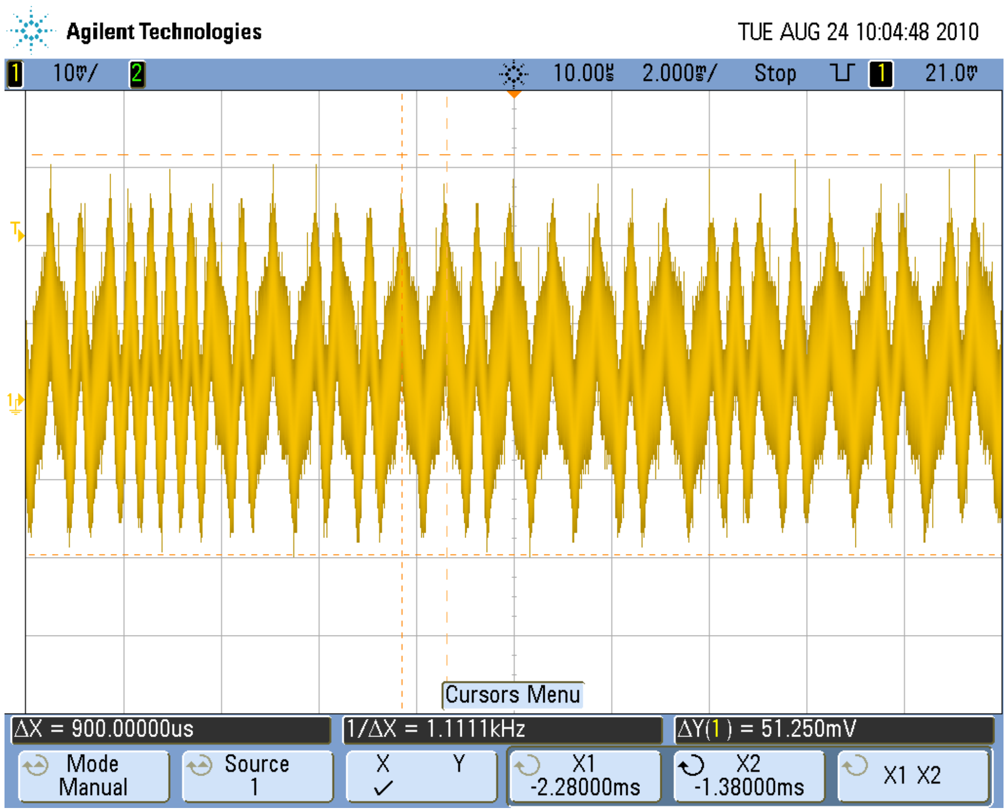
Magnetic Stripe Recalled

- Up to three data tracks.
  - Track 1 (RO), F2F modulation, 210 bits/in
    - PAN, cardholder name, expiration, service code, discretionary data incl. cryptographic checksum, etc.
  - Track 2 (RO), F2F modulation, 75 bits/in
    - PAN, expiration, service code, discretionary data incl. cryptographic checksum, etc.
  - Track 3 (RW), F2F modulation, 210 bits/in
    - Data for offline transaction processing.
    - Using track 3 is obsolete, now.

Public Standards Apply

- Following standards create general magnetic stripe framework for payment cards.
  - Particular details (cryptographic checksums, discretionary processing data, etc.) are subjects to particular proprietary extensions described by the respective association.
  - Anyway, it definitely pays off to look at those public sources.
- ISO 7811-2, ISO 7811-4, ISO 7811-5
  - recording techniques, data encoding
  - location of tracks
- ISO 7813
  - data format of track 1 and 2
- ISO 4909
  - data format of track 3

F2F Modulated Data Example



- Peeks correspond to magnetic flux changes as observed by a reading head (track 1).
- Physical fingerprinting based on magnetic noise is a possible countermeasure against skimming attacks. It is, however, really seldom used in practice.

Cross-channel Attack

- Re-creation of data tracks based on EMV chip data, contactless chip data or even data printed on the card itself.
  - Theoretically possible.
  - Since there is often no physical fingerprinting used, we can take any data we have and put them on arbitrary magnetic stripe.
  - **However**, nowadays it shall be regarded as a <u>configuration failure</u>, since mechanisms already exist to prevent this attack.

Countermeasure no. 1

- Cryptographic checksum values used to protect tracks data are (computationally) independent for each potential data storage.
  - So, there is e.g. a different code required for the magnetic stripe and the particular track data stored in EMV chip.
  - In particular, it is a shortened 3DES CBC-MAC computed over PAN, expiration, and service code.
  - This prevents re-creation of original magnetic stripe from data obtained “elsewhere”.
  - It also prevents forced fall-back from EMV card to a stripe-only card by altering the service code value.

Countermeasure no. 2

- There is a mandatory processing data element (DE 22) indicating which interface was used to enter transaction PAN, etc.
  - It distinguishes data entered through magnetic stripe, chip card reader, RF interface, keyboard, etc.
  - It prevents e.g. entering contactless chip data through magnetic stripe reader while still regarding them as a kind of legacy contactless transaction (and hence use different rules for card and cardholder verification).

Note on Shimming

- Instead of magnetic stripe, the chip and its communication is the prime target, now.
  - Attacker uses a very thin PCB plate inserted and fixed in the contact area of the EMV terminal.
  - The PCB also bears a miniature low-power microcontroller.
  - The whole device is referred to as a *shim*.
  - It works as MITM in the ISO 7816 channel.
- Particular details of these attacks are not publicly known, yet.
  - Despite not being theoretically surprising, these attacks are rather new in the criminal area.
  - Apparently, EMV protocol security research starts to be especially important, since it is desirable to know how far these shimming attacks can ever go…

Part THREE
CAP/DPA Overview

CAP/DPA Technology

- Allows using an existing payment cards infrastructure for authentication of clients and their payment orders in e.g. internet banking applications.
  - MasterCard – Chip Authentication Program (CAP)
  - VISA – Dynamic Passcode Authentication (DPA)

Based on EMV Framework

- For CAP/DPA, we use mainly:
  - offline PIN verification via VERIFY cmd.,
  - online card authentication via GENERATE AC cmd.
- Other services play more or less insignificant roles here.
  - SDA, DDA, CDA, etc.

Application Topology

- CAP/DPA allows
  - either sharing exactly the same application for payment transactions as well as for client authentication,
  - or installing a separate application (stub) that shares only a certain data objects.
- Usually, the concept of two separate applications is applied.
  - Shared: offline PIN, PAN (tag 5A), etc.
  - Independent: ATC (tag 9F36), AIP (tag 82), $\boldsymbol{MK}_{AC}$, file locators, etc.

Security Cornerstone

- The CBC-MAC computed by GENERATE AC is transformed (decimated) using the Issuer Proprietary Bitmap (IPB, tag 9F56) vector.
  - The result is displayed to the client using a numerical (or some more general) alphabet. It is then used as a kind of one-time password at the bank.
  - The Card Verification Result (CVR, proprietary tag) flags (part of CBC-MAC input data) must indicate a successful offline PIN verification. This is an implicit countermeasure against [11].
- Recall that the CBC-MAC is computed using $\boldsymbol{MK}_{AC}$ or its derivative.
  - $\boldsymbol{MK}_{AC}$ is therefore the cornerstone of the CAP/DPA security.

Public Information

- Further public information on CAP/DPA can be found in [1].
  - Presents certain reverse engineering of CPA/DPA protocols together with some comments on how (not) to design real life applications.

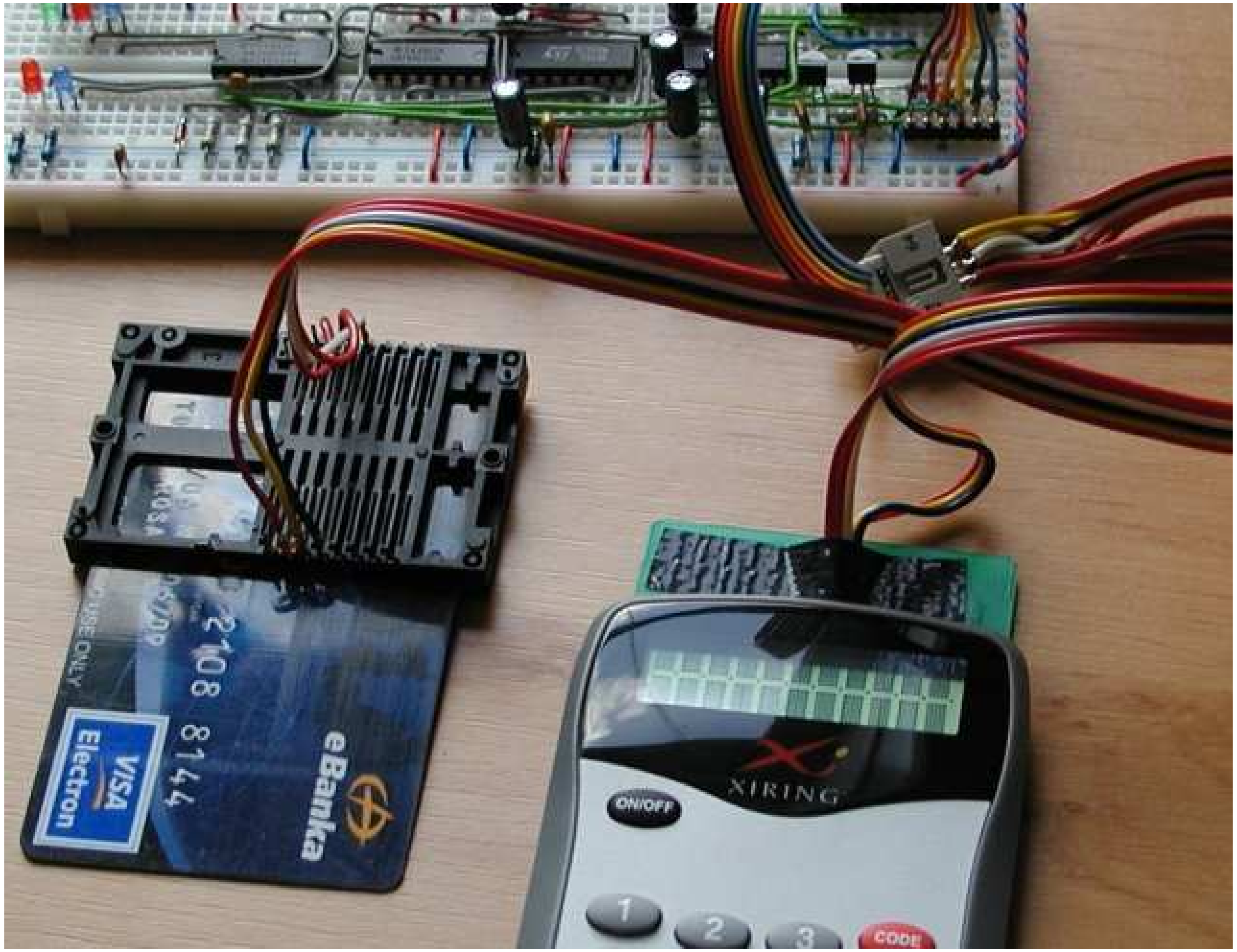
CAP/DPA Readers

- Besides their original purpose, these device can also serve the role of EMV etalons.
  - Spying the reader action helps a lot to understand all those practical aspects of EMV.
  - If necessary, a MITM technique can be used to force the reader to work with the real payment application instead of the CAP/DPA stub.
    - Simply say “not present” for the CAP/DPA AID.

CAP/DPA *Teachers*

- Confused about the new card?
  - Just take the CAP/DPA reader and let it show you the way…
- Especially, the CDOL1/2 filling for the $1^{st}/2^{nd}$ GENERATE AC commands deserves certain attention.
  - Details are elaborated in [13].

Learning the Lessons…



Part FOUR
Contactless (CL) Payment Cards

Design Objectives

- Despite not being explicitly declared, we can see the following objectives are obeyed:
  - standard-based RF interface,
  - simplified data exchange to improve communication reliability and speed,
  - certain backward compatibility with mag. stripe,
  - offering higher security standard if possible,
  - compatibility with EMV framework if possible,
  - offline transaction authorization is preferred.

Standard Interface

- The RF interface is based on widespread ISO 14443 A/B.
  - Terminal must support both A and B variants, the card may choose one.
- At this moment, this is the only part which is covered by EMV.
  - Covers card detection, singulation (anticollison), and activation [7].
  - Anything else at EMV is just a stub, now [8].

Application Selection

- PPSE method returns AIDs directly in FCI template of “2PAY.SYS.DDF01”
  - Subsequent record reading is omitted.
  - PPSE stands for Proximity-PSE and is <u>mandatory</u> for VISA and MC CL cards.
    - contrary to the PSE for contact cards

MagStripe Compatibility API

- Originally developed (perhaps) mainly for USA markets.
  - Allows CL cards acceptance with minimum existing infrastructure changes.
  - We call them "1st generation" cards, now.
  - Their security was – to say – not surprising [9].
  - Today, we see them as a separate application besides the "2nd generation" card profile.
  - Not surprisingly, there is certain suasion to remove this profile at all.

VISA’s PW-qVSDC

- This is an obvious refinement, in fact also replacement, of VISA Low-Value Payment (VLP) mechanism as it was specified for VISA chip cards version 1.4.
  - PW stands for Pay Wave.
  - qVSDC stands for quick-VSDC
    - VSDC (VISA Smart Debit/Credit) is the name of the EMV contact application of VISA.
  - The new protocol is even more atomic and faster than VLP.
  - On the other hand, the integration with the contact (VSDC) application is nearly the same as for VLP.
    - Mainly with respect to offline spending counters reset.

MasterCard's PP-M/Chip

- Very similar to the M/Chip application available through the contact interface.
  - PP stands for Pay Pass
- Changes or refinements often due to a reflection of RF communication.
  - VERIFY(PIN) not available in PP-M/Chip
  - Static data shall not contain personal data.
  - Strong push towards CDA method to enhance security of transactions authorized offline.
  - Etc…

How to Approach CL Cards

- At this moment, the application interfaces are proprietary, covered by confidential materials.
- On the other hand, the RF communication is publicly known thanks to the EMV standard.
  - We can silently assume the application interface is *somehow similar* to that one for contact cards.
  - We shall look, listen, and experiment…

Dual Cards

- Dual interface smartcards are often used for payment cards supporting both contact and contactless applications.
  - Instead of producing hybrid cards with two independent chips.
  - Furthermore, there is a certain visible interconnection in between these two applications.
    - E.g. offline counters reset, application blocking, etc.

Part FIVE
Certain Immediate Issues (RF if.)

APDU Protection

- Similarly to EMV contact interface, there is often no cryptographic APDU protection.
  - Regarding the nature of RF interface, this can be potentially dangerous.
  - We can see some tries to cope with this on the application layer.
    - Personal data shall not be accessible.
    - VERIFY(PIN) is not accessible.
    - …
  - On the other hand, systematic treatment on the transport layer would be more appropriate.

Key Management

- Sometimes, keys can be shared in between contact and contactless application parts.
  - Potential side-channel attack targeted at the RF interface can threat the contact application security as well.
  - It is definitely recommended to keep all the keys separate whenever possible.

UID

- Probably, the UID of the CL interface is not involved in the upper layer protocol protection [7].
  - Obviously, there is no UID-based key diversification, etc.
- Moreover, the UID is often constant.
  - Comparing to the electronic passports case, this can be viewed as a “certification weakness”.
- This can allow or simplify certain attacks.
  - Using NFC controller as a card emulator with no special UID-treatment (cf. www.libnfc.org).
  - Active/passive radiolocation of card holders. At this moment, this is rather theoretical threat which can, however, become practical with a time.

Part SIX
NFC and Payment Cards

NFC at Glance

- Device equipped with the NFC front-end can work in the following modes:
  - Passive-mode initiator (or just a “reader”)
  - Passive-mode target (or just a “tag emulator”)
  - Active-mode initiator/target (or just “reader-to-reader”)
- Covered by the ISO 18092 standard
  - In fact, several parts duplicate the ISO 14443 A or FeliCa, but with a rather “innovative” wording.
  - Attention – the word “passive” does no longer equal to “without autonomous power source” here.
    - It is used to address those ISO 14443 A or FeliCa compatible modes in general (reader as well as tag).
  - Furthermore, ISO 21481 addresses possible RF interference issues of NFC and other standards occupying 13.56 MHz.
    - Those mainly are ISO 14443 and ISO 15693.

NFC and Payment Cards

- NFC-equipped device can address CL payment cards world in two ways
  - As a terminal
    - ISO 14443 A – passive-mode initiator
  - As a card itself
    - ISO 14443 A – passive-mode target

NFC-based Payment Card or Terminal

- The principle is easy – simply implement the particular payment card API or payment terminal functionality (e.g. POS) over the NFC front-end.
- The question is, however, which module will then:
  - hold all those sensitive data, and
  - perform all those certified code procedures.
- At present, this problem seems to be solved only for certain special devices.
  - Namely for GSM phones.

NFC in GSM Phones

- So far, this is rather a marketing stunt than anything else.
  - Some manufacturers already provide at least one NFC-equipped phone, but this is merely a testing sample.
  - We can see them as generation-zero devices.
  - Furthermore, several incompatible architectures do exist, now.
- What seems to be the future:
  - SIM card is the security cornerstone.
    - Also called *Secure Element* here.
  - The payment card (or terminal – e.g. POS) application runs on the SIM card and communicates directly with the CLF (contactless front-end).
  - Phone-side application is possibly involved only indirectly.
    - Either through separate SIM interfaces (SIM-Toolkit over ISO 7816-3 or even web services over ISO 7816-12),
    - or through a serial link to the monitor firmware running on CLF.

CLF

- Provides SWP (Single Wire Protocol) interface.
  - Described in public standards:
    - ETSI TS 102 613 (physical and data link layer),
    - ETSI TS 102 622 (host controller interface).
- At present, CLF can be bought separately.
  - Cf. e.g. www.bladox.com
  - Seldom GSM operators, however, issue SWP-capable SIMs, now.
  - SWP<->USB interface converter is one of those wanted technical projects, since CLF seems to be a valuable tool for security analysts in itself.

Hacking Into&With NFC

- When successfully mastered, the NFC is a vital tool for any security analyst.
  - Mainly the passive-mode target promises, obviously, many interesting applications.
- The whole approach has, however, two steps:
  - Hacking into NFC. While it is relatively easy to buy a device with a NFC controller, it is much harder to get full documentation for it.
    - Even the NFC devices themselves try to somehow limit their usage for this purpose – e.g. UID setting obstacles.
    - Very important and useful project is **www.libnfc.org**.
  - Hacking with NFC. The NFC devices can be used to implement e.g. relay (wormhole) or MITM attack, etc.

Hacking with GSM-NFC

- We shall start taking the relay (wormhole) attacks really seriously!
  - Their principle is very simple, but their impact can be very dangerous [2], [14].
- Once NFC in mobile phones becomes reality, we can expect enormous rise of these attacks, since GSM phone:
  - is fully programmable,
  - offers sufficient network connectivity,
  - is highly inconspicuous.
- Unfortunately, EMV standard for contactless interface data link layer [7] is such that it:
  - does not provide any explicit distance bounding protocol,
  - relies fully on ISO 14443 augmented with ISO 7816-4, which is a combination known to actually facilitate rather than prevent relay attacks [10].

Conclusion

- The area of chip payment cards attains several acmes.
  - Highly complex and mature, widespread, highly important for almost everybody, impressive financial potential, etc.
- Surprisingly, there are just a few academic papers touching the security of chip payment cards.
  - The reason is, perhaps, the horrible obscurity of this area.
- This lecture tries to clarify the most important topics.
  - It also points out several parts where to start researching.
  - It, of course, cannot substitute hundreds of pages the researchers will probably have to read.
  - It can, however, provide a tiny light and encouraging guidance during their first steps on their own way.

Thank you for attention…

Tomáš Rosa

crypto.hyperlink.cz

References

1. Drimer, S., Murdoch, S.-J., and Anderson, R.: *Optimised to Fail: Card Readers for Online Banking*, Financial Cryptography 2009, www.cl.cam.ac.uk/~sjm217/papers/fc09optimised.pdf
2. Drimer, S. and Murdoch, S.-J.: *Relay Attack on Card Payment – Vulnerabilities and Defences*, 24C3, December 2007, www.cl.cam.ac.uk/~sjm217/talks/ccc07relayattacks.pdf
3. EMV Integrated Circuit Card Specification for Payment Systems, *Book 1 – Application Independent ICC to Terminal Interface Requirements*, v. 4.2, June 2008
4. EMV Integrated Circuit Card Specification for Payment Systems, *Book 2 – Security and Key Management*, v. 4.2, June 2008
5. EMV Integrated Circuit Card Specification for Payment Systems, *Book 3 – Application Specification*, v. 4.2, June 2008
6. EMV Integrated Circuit Card Specification for Payment Systems, *Book 4 – Cardholder, Attendant, and Acquirer Interface Requirements*, v. 4.2, June 2008
7. EMV Contactless Specifications for Payment Systems, *EMV Contactless Communication Protocol Specification*, v. 2.0.1, July 2009
8. EMV Contactless Specifications for Payment Systems, *Entry Point Specification*, v. 1.0, May 2008

References

9. 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
10. Hlaváč, M. and Rosa, T.: *A Note on the Relay-Attacks on e-passports – The Case of Czech e-passports*, IACR ePrint 2007/244, June 2007
11. Murdoch S.-J., Drimer, S., Anderson, R., and Bond, M.: *Chip and PIN is Broken*, 2010 IEEE Symposium on Security and Privacy, www.cl.cam.ac.uk/~sjm217/papers/oakland10chipbroken.pdf
12. www.emvlab.org
13. Rosa, T.: *EMV Cards Trivium – Fast Way to Side Channel Experiments*, June 2010, crypto.hyperlink.cz/files/emv_side_channels_v1.pdf
14. Weiss, M.: *Performing Relay Attacks on ISO 14443 Contactless Smart Cards using NFC Mobile Equipment*, Master’s thesis in computer science, May 2010, www.sec.in.tum.de/assets/studentwork/finished/Weiss2010.pdf
15. Certain “leaked” documents available e.g. through www.google.com