EMV (Chip & PIN) Protocol

Märt Bakhoff
Supervised: Arnis Paršovs
Objective

observe and describe a real world transaction
Agenda

- Tools & setup
- Quick overview of transaction processing
- High level overview of captured data
Tools & setup

- Osmocom Simtrace
- “upgraded” cardreader
- Visa Electron card
- friendly merchant
Simtrace
MITM board for SIM cards
Reading binary dumps for the win?

- EMV = Europay, Mastercard, Visa
- standardized payment cards (currently v4.3)
- released as 4 “books” with a total of 747 pages
Transaction flow

Candidate list creation

iterate applications on the card

read application ids

Candidate List Creation
Application Selection
Read Application Data
Data Authentication
Cardholder Verification
Processing Restrictions
Terminal Risk Management
Card Action Analysis
Online Processing
Final Action Analysis
Transaction flow

Application selection

select the application in the terminal
activate application in the chip

Candidate List Creation
Application Selection
Read Application Data
Data Authentication
Cardholder Verification
Processing Restrictions
Terminal Risk Management
Card Action Analysis
Online Processing
Final Action Analysis
Transaction flow

Read Application Data

expiration date
pin options
online/offline support
crypto keys

Candidate List Creation
Application Selection
Read Application Data
Data Authentication
Cardholder Verification
Processing Restrictions
Terminal Risk Management
Card Action Analysis
Online Processing
Final Action Analysis
Transaction flow

Data authentication

offline mode: verify data on the card using digital signature

online mode: challenge&response with card's private key

Candidate List Creation
Application Selection
Read Application Data
Data Authentication
Cardholder Verification
Processing Restrictions
Terminal Risk Management
Card Action Analysis
Online Processing
Final Action Analysis
Transaction flow

Cardholder verification

online pin / offline pin / handwritten signature

pinpad->icc encrypted
Transaction flow

Processing restrictions

check expiration date

check “application usage controls”
Transaction flow

Terminal risk management
decide online/offline
“floor limits”

Candidate List Creation
Application Selection
Read Application Data
Data Authentication
Cardholder Verification
Processing Restrictions
Terminal Risk Management
Card Action Analysis
Online Processing
Final Action Analysis
Transaction flow

Card action analysis

decide
online/offline/reject

can upgrade to online

can't upgrade to offline

Candidate List Creation
Application Selection
Read Application Data
Data Authentication
Cardholder Verification
Processing Restrictions
Terminal Risk Management
Card Action Analysis
Online Processing
Final Action Analysis
Transaction flow

Online processing

send ARQC to issuer
send response to chip

can downgrade to offline

Candidate List Creation
Application Selection
Read Application Data
Data Authentication
Cardholder Verification
Processing Restrictions
Terminal Risk Management
Card Action Analysis
Online Processing
Final Action Analysis
Transaction flow

Final card analysis
verify issuer online
response
decide to accept/reject
generate transaction
certificate (TC)
Captured data
(19 request/response pairs)
Request:
file '1PAY.SYS.DDF01'

Response:
ShortFileIdentifier of directory element: 1
language preference: et, en, ru, de
00 B2 READ RECORD

Request:
ShortFileIdentifier: 1; record: 1

Response:
application identifier: VISA electron
application priority: 1
Request:
ShortFileIdentifier: 1; record: 2

Response:
File not found
Request:
empty

Response:
application id: Visa Electron
application priority: 1
language preference: et,en,ru,de
issuer url: 0x9f4d020b14
Request:
empty list

Response:
dynamic data authentication (DDA) supported, cardholder verification supported, perform terminal risk mgmt supported, issuer authentication supported
locations of data records:
  SFI1, record 1-1
  SFI2, record 1-6
Request:
SFI:1, record: 1

Response:
card number: xx xx xx xx xx 37 64 61 73
expiration date: 14 12
cardholder name: BAKHOFF/MART
Request:
SFI:2, record: 1

Response:
Application Effective Date: 12 10 01
Application Expiration Date: 14 12 31
Application Usage Control: all allowed
Primary Account Number: xxxx xxxx 3764 6173
CDOL1, CDOL2, CVM
Issuer country code: 0x0233
Request:
SFI:2, record: 2

Response:
Issuer Public Key Certificate
Issuer Public Key Exponent
Issuer Public Key Key Remainder
Request:
SFI:2, record: 3

Response:
DDOL
ICC Public Key Exponent
00 B2 READ RECORD

Request:
SFI:2, record: 4

Response:
ICC Public Key Certificate
00 B2 READ RECORD

Request:
SFI:2, record: 5

Response:
ICC PIN Encipherment Public Key Certificate
ICC PIN Encipherment Public Key Exponent
00 B2 READ RECORD

Request:
SFI:2, record: 6

Response:
Application Version Number: 0x008c
Service Code: 0x0221
Application Currency Code: 0x0978
Application Currency Exponent: 2
Request:
(DDOL) 4 bytes nonce 0xd6834217

Response:
Signed Dynamic Application Data

00 88 INTERNAL AUTHENTICATE
80 CA GET DATA

Request:
pin try counter

Response:
PIN Try Counter: 3 remaining
Request:
empty

Response:
6e 46 d1 ff 7f 6e 61 30
(8-byte nonce generated by the ICC)
Request:
encrypted pin

Response:
ok

00 20 VERIFY
Request:
request ARQC (online mode)
amount: 0.99
terminal country code: 0x0233
TVR: transaction exceeds floor limit
transaction date: 14 09 25
nonce: 4 bytes

Response:
Application Transaction Counter (ATC): 0x0377
Application Cryptogram: ac 74 08 bb 16 b2 b8 6d
00 82 EXTERNAL AUTHENTICATE

Request:
Issuer Authentication Data:
83 1c 2b df 91 08 e0 70 30 30

Response:
ok
Request:
request transaction certificate
authorization response code: 0x3030
amount: 0.99
terminal country code: 0x0233
TVR: transaction exceeds floor limit
transaction date: 14 09 25
nonce: 4 bytes

Response:
Application Transaction Counter (ATC): 0x0377
Application Cryptogram: c2 f1 92 98 bd 19 a7 fe
Q/A
References

- www.emvco.com/specifications.aspx
- www.level2kernel.com/flow-chart.html
- cotignac.co.nz/emv-offline-data-authentication