Black-Box Assessment of Smart Cards

Daniel Crowley
Head of Research, X-Force Red

X-Force Red

IBM

Why Smart Cards?

Pervasive

Credit / debit cards

Physical access cards

SIM cards

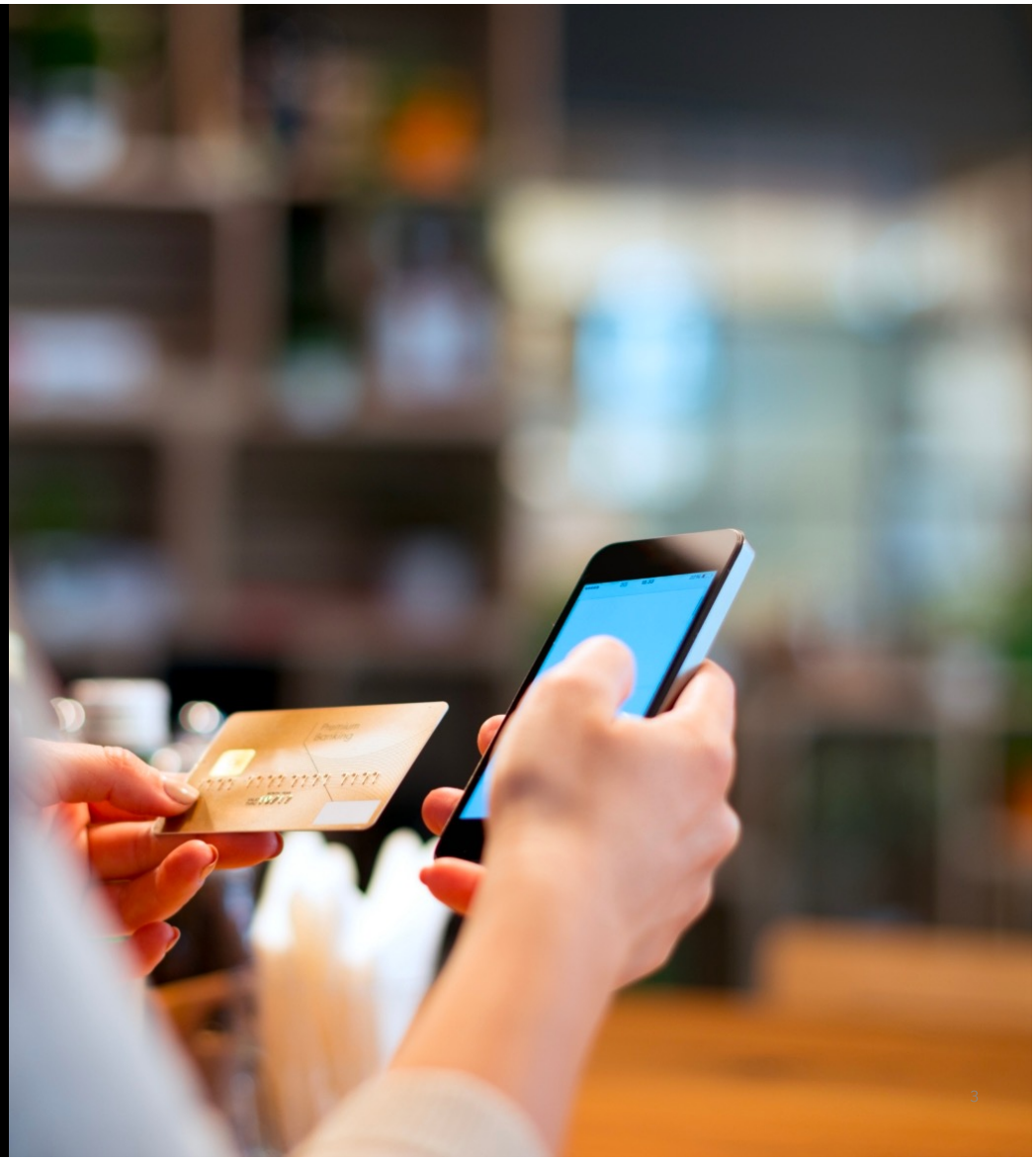
2FA cards

Cryptographic co-processor cards

Transit fare cards

Passports

Amiibos



Handles important things

Money

Physical access

Digital access

Cryptographic key material

Communications

Standards

ISO7816 standard – What does it define?

Contact cards

Physical format of connector

Pinout of connector

Command format – APDU

Certain commands

ISO7816 standard – What does it NOT define?

Which commands must be implemented

Particulars of implementation

- Challenge / response mechanism

ISO14443

Contactless cards

Uses APDUs, same as ISO7816

How well do cards follow standards?

Size / shape of connector

Almost all implement SELECT FILE

VERIFY also common

GET CHALLENGE / GENERAL AUTHENTICATE

Error codes all over the map

APDU

APDU command format

Select file by DF name, first occurrence, named "ABC"

CLA	INS	P1	P2	Lc	Data	...	...
00	A4	04	00	03	41	42	43

APDU command format

Select file by DF name, first occurrence, named "ABC"

CLA	INS	P1	P2	Lc	Data	...	...
00	A4	04	00	03	41	42	43

- CLA is short for Class
- Defines what category of instruction to execute
- First bit 0 is interindustry
- First bit 1 is proprietary
- FF is invalid (but used in related PCSC standard)
- Various bitflags define connection properties

APDU command format

Select file by DF name, first occurrence, named "ABC"

CLA	INS	P1	P2	Lc	Data	...	...
00	A4	04	00	03	41	42	43

- INS is short for Instruction
- Defines which command to execute
- A4 is SELECT FILE

APDU command format

Select file ***by DF name, first occurrence***, named "ABC"

CLA	INS	P1	P2	Lc	Data	...	...
00	A4	04	00	03	41	42	43

- P1 and P2 are Parameters 1 and 2
- Like command line switches
- Value depends on instruction
- P1 == 04 means select by DF name
- P2 == 00 means first occurrence

APDU command format

Select file by DF name, first occurrence, ***named "ABC"***

CLA	INS	P1	P2	Lc	Data	...	...
00	A4	04	00	03	41	42	43

- Lc is Length of Command in bytes
- Data following Lc must be Lc bytes long
- Can be omitted if length is zero

APDU command format

Select file by DF name, first occurrence, named "ABC"

CLA	INS	P1	P2	Lc	Data	...	...
00	A4	04	00	03	41	42	43

- Le byte can follow Lc + data
- Defines maximum response Length Expected
- Omitted here, no specific response length expected

APDU response format

Command executed without error – response "ABC"

SW1	SW2	Data	...	...
90	00	41	42	43

- SW1 is type of response
  - 0x90 is success
- SW2 is subtype
  - 0x00 is only subtype of 0x90
- Response also includes data field

APDU response format

Le field incorrect, correct value in SW2

SW1	SW2	~~Data~~	~~...~~	~~...~~
6c	10			

- This SW1 means expected response length is wrong
- This SW2 is the correct length value
- No data sent with response

APDU response code samples

6e 00 – Invalid CLA

6d 00 – Invalid INS

6b 00 – Invalid P1/P2

6a 86 – Incorrect P1/P2

6a 00 – Bytes P1 and/or P2 are incorrect

6a 82 – File not found

69 82 – Access conditions not fulfilled

61 xx – xx response bytes still available

Feasibility of brute forcing CLA / INS / P1 / P2

- CLA
  - if interindustry, no brute needed
  - if proprietary, 7 bits = 128 possible values
- INS
  - ISO7816 forbids 6x and 9x INS codes
  - 256-16-16 = 224 possible values
  - 51 command values defined by ISO7816
- P1 / P2
  - 65536 possible values

Feasibility of brute forcing CLA / INS / P1 / P2

- Could parallelize with multiple cards of the same type
- Some commands should be avoided
  - TERMINATE CARD USAGE / BLOW FUSE
  - DELETE FILE

Feasibility of brute forcing CLA / INS / P1 / P2

Worst case scenario

- Generic error messages
  - Unlikely given wide support for SELECT FILE
- Slow card, 10 tries / sec
- ~ Six years for all combinations

Best case scenario

- Specific error messages
- Fast card, 30 tries / sec
- ~ 30 minutes

Feasibility of brute forcing DF name

- Right-truncation
  - "abc" is acceptable for file "abcdefgh"
- Registered IDs
  - 5 bytes
  - International starts with quartet (aka nibble) A
  - Next nine quartets can only be 0-9
  - RIDs are registered and public knowledge
  - 652 from public list
  - Works VERY well

Self-describing card features

Answer-to-Reset (ATR)

Transaction begins with reset

Card sends information on reset (answer to reset)

- OR makes data available in known file EF.ATR

Historical Bytes

Optional card info sent with ATR

- Alternatively, as part of retrievable card data

Country / issuer code

AID of implicitly selected application

Card support for

– Application select by
  - Full / partial DF name?
– EF.ATR / EF.DIR and how to access

Historical Bytes

Initial access data

– Expected first APDU command

Card issuer data

- Whatever the issuer wants; contents not standardized

Support for file select by

- Full/partial DF name
- Path
- ID

EF.DIR

Directory file

Provides directory of available files

File system structure and access

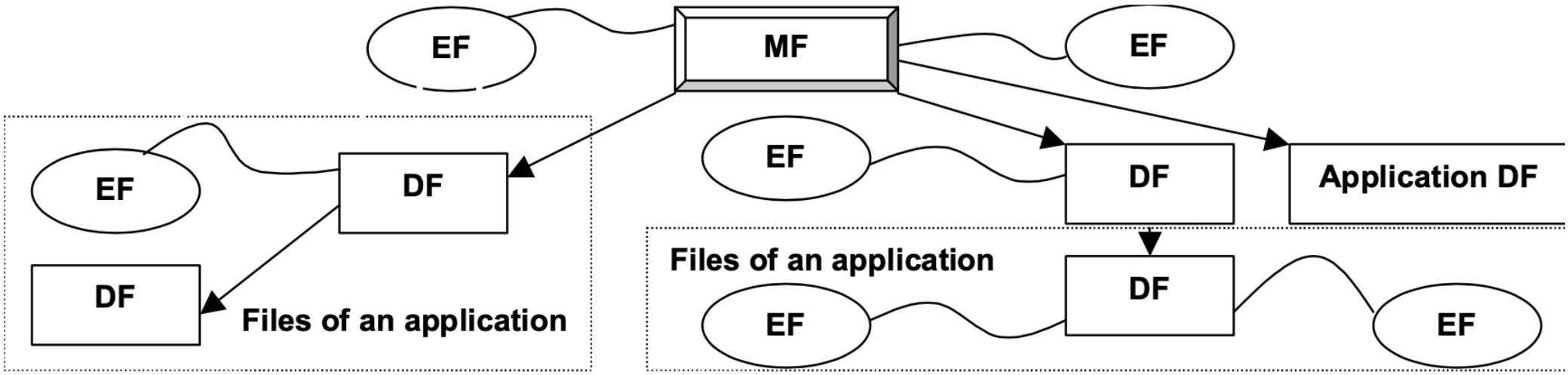


Figure 2 — Example of hierarchy of DFs

MF

Master File

Root node

DF

Dedicated File

Can be dir/app/file

Application DF

DF hosting an application

EF

Elementary File

Data store

Files aren't just files

Files are also contexts

Working directory context

Command set context

SELECT FILE by DF name

Comparable to filenames in desktop / server file systems

Can allow for right truncation

e.g. "foo" will return results if "foobar" or "foodang" exist

Minimum length may be enforced

Standard defines National ID

Alternatives to DF name

Implicit file selection

- After card reset, a file is selected

Two-byte identifier

- Two bytes that uniquely identify files relative to current selected file

Path

- Series of two-byte identifiers

- Like a file path with no delimiters

Records and binary data

Elementary files with data

READ RECORD

READ BINARY

GET DATA

Sensitive data exposure?

Authentication

VERIFY

Provide PIN or password

Direct comparison

Sent along data channel

If transmission is unencrypted, authenticator is too

Timing attacks?

Eavesdropping?

Unlimited retries?

Unauthenticated RESET RETRY COUNTER?

Challenge / Response

Ask for random data from card

Quality of randomness source?

Enforced minimum challenge length?

Broken cryptography?

SCQL: Smart Card Query Language

SCQL

Same INS for everything

P2 values correspond to common SQL commands

I have still never seen this on any card

SCQL

Same INS for everything

P2 values correspond to common SQL commands

~~**I have still never seen this on any card**~~

ZOMG I FOUND ONE YESTERDAY AT DEFCON

Bug hunting

Unauthenticated Sensitive Commands

RESET RETRY COUNTER

Load Applet

DISABLE VERIFICATION REQUIREMENT

Undocumented Applications / Instructions

Leftovers from debugging

Backdoor?

Default Keys / Passwords

Classic MIFARE bug

VERIFY code 0000

APDU data field fuzzing

Opportunities for many generic application bugs

Nested TLV

Cryptographic flaws

One-byte or zero-byte challenge

Unpadded RSA

Results from real smart cards

Self-description

Historical bytes common

Often contains single application ID

Often describes file select support

Have not seen EF.DIR yet

SELECT FILE support

DF name incredibly common

– Right truncation common

– Often a minimum of five bytes

One card supporting select by ID

Vulnerabilities

One-byte challenge

- Replay attacks

Tool drop

Wubblegum

Enumerates / Dumps

- CLA
- Files
- INS
- Records / Data

Demo

Future work

Additional enumeration support

READ BINARY

VERIFY check

SCQL

EF.DIR / Historical bytes parsing

Dir / Read info command support

Common vuln checks

Unauthenticated sensitive functions

Default PIN / pw

One-byte / zero-byte challenge

Card to terminal fuzzing

Phones

ATMs

Passport readers

Electronic locks

POS systems

Greetz

Ludovic Rousseau

foundation

Jean-Daniel Aussel

Kristopher Beauchemin

Cheef

Alaska and the HTS crew

X-Force