

A recent open source embedded implementation of the DESFire specification designed for on-the-fly logging with NFC based systems

Maxie Dion Schmidt

Georgia Institute of Technology
School of Mathematics
Atlanta, GA 30318, USA

mschmidt34@gatech.edu

<http://people.math.gatech.edu/~mschmidt34>

<https://github.com/maxieds>

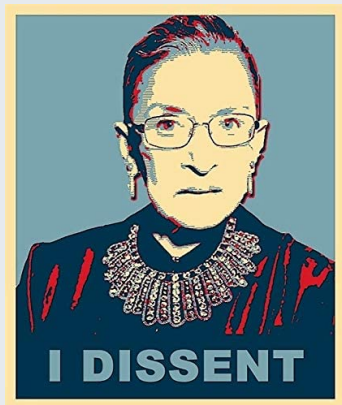
Future Technologies Conference
October 2021

High-level overview

- ▶ Near Field Communication (NFC) protocol over short-distance RFID @ 13.56MHz
- ▶ Enables contactless data exchanges between passive tags (PICC) and active hosts (PCD)
- ▶ DESFire type cards provide modern cryptographic algorithms and more sophisticated feature set
- ▶ Chameleon Mini (RevG) devices used for pentesting and security applications as tag emulators and data loggers

High-level overview (cont'd)

- ▶ DESFire emulation support for the Chameleon Mini has been a frequently requested, however complicated to deliver, feature for years
- ▶ How the first testing releases came together in the Fall of 2020
- ▶ <https://github.com/emsec/ChameleonMini/pull/287>



High-level overview (cont'd)

- ▶ Significance: First of its kind functional embedded proof-of-concept DESFire stack that is freely available as OSS to researchers, security experts and end users alike
- ▶ Limitations: Small R&D budget for testing and lack of standardized default data transfer modes to ensure interoperability amongst door readers in applications

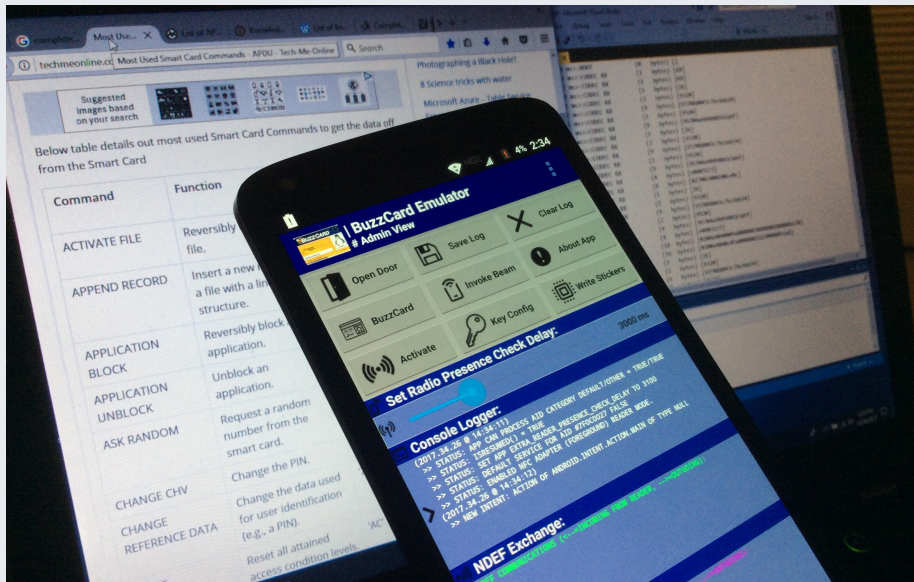
Outline of topics

Presentation outline

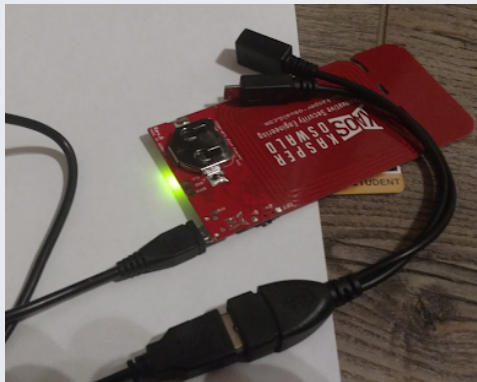
- ▶ The Chameleon Mini device hardware profile and embedded software features
- ▶ Overview of key features of the proprietary DESFire command set
- ▶ Key features and challenges in writing the embedded DESFire implementation (with examples)

Chameleon Mini Hardware

Origins of the project I



Origins of the project II



Chameleon Mini Live Debugger
Portable logging interface v0.1.1

MF_CLASSIC_4K MEM-4K/LOG-2K/DIP#1
AB:CD:EF:01 RW/FLD-0/NO-CHRG
THRS-400 mv/TMF-5000 ms

Log Tools Menu Log Tools Export

000006 LOG_CODE_DNE 4B +0ms
00 00 00 00
... ISO_STD_APOU

000007 LOG_CODE_DNE 4B +0ms
00 00 00 00
... ISO_STD_APOU

000008 LOG_CODE_DNE 4B +0ms
00 00 00 00
... ISO_STD_APOU

000009 CONFIG_SET 24B ~5656ms
49 53 4f 31 34 34 34 33 41 5f 52 45 41 44 45 52 31 30 30 3a 4f 4b 0d 0a
ISO14443A_READER100-OK...

000010 CONFIG_SET 21B +24946ms
4d 46 5f 43 4a 41 53 53 49 43 5f 34 4b 31 30 30 3a 4f 4b 0d 0a
MF_CLASSIC_4K100-OK
GENERATE_PUBLIC_KEY_PAIR (ISO 7816-8)

INFO: SHELL COMMAND of UID=ABCDEF01
RETURNED STATUS **K** 100:OK --
2018-01-11-20:30:14

The Chameleon Mini device profile (hardware)

- ▶ On-board integration of a modern AVR chip (ATxmega128A4U)
- ▶ Memory: 128Kb of FLASH, 8Kb of SRAM, and 2Kb of EEPROM spaces and support for faster FRAM-based memory access
- ▶ Accelerated hardware support for AES and DES cryptographic engines
- ▶ Embedded firmware and flashable bootloader support to memory map the integrated RF hardware on the PCB
- ▶ Serial data transfer over wired micro-USB

The Chameleon Mini device profile (software)

- ▶ Embedded OSS firmware and bootloader sources in C and ASM compiled with `avr-gcc` that are flashed to the device over USB
- ▶ Convenient serial terminal that has a human-readable command set for easy on-the-fly configuration of emulated tags
- ▶ Ability to act as a PICC, PCD or bidirectional NFC packet sniffer depending on the active configuration set in one of the eight 8Kb sized partitions of the onboard memory
- ▶ Logging of time-stamped communication details and status events to internal FRAM memory or LIVE mode printed to the serial USB

DESFire tags

Key Features

- ▶ Multiple nested and semi-interoperable generations of DESFire tags: Legacy Mifare DESFire, EV1, EV2, EV3 and Light variants
- ▶ Larger scale integrated memory storage sizes than most contactless NFC tags (usually 2Kb, 4Kb or 8Kb)
- ▶ Standard use of modern cryptographic algorithms for secure data exchange (legacy DES/3DES/AES-128/AES-256)
- ▶ Data messages optionally padded with cryptographically hashed bytes to ensure data integrity over the physical interface using 2-byte CRC checksums or 4-byte MAC trailers
- ▶ Implementations are complicated by proprietary handling of most DESFire tag specs by the manufacturers

Filesystem: Organization and internal storage types

- ▶ Files grouped by allocations of the physical IC memory into top-level subdirectories called applications indexed by unique application identifier (AID)
- ▶ Native file types: Standard data files (type 0), backup data files (type 1), value files (type 2), linear record files (type 3), and cyclic record files (type 4)
- ▶ Each file has 2-bytes of associated access rights to indicate one of read/write/read and write/change.
- ▶ Access permissions on the files provide more secure protections for storage of secret binary key data

Commands and native instruction support

- ▶ Formats to communicate instructions is performed by sending unpadded native commands or by communicating ISO standardized wrapped APDU messages

PICC-to-PCD wrapped APDU data exchange format:

CLA	INS	P ₁	P ₂	L _c	Data Bytes	L _e
0x90	command code	0x00	0x00	variable length of data	command data	0x00

PCD-to-PICC format:

Data Bytes	SW1	SW2 (Status)
DESFire command response data	0x91	0xYY

Supported command codes

Command Long Name	INS	Description
AUTHENTICATE	0x0A	Legacy mode authentication
AUTHENTICATE_ISO	0x1A	ISO authentication with 3DES
AUTHENTICATE_AES	0xAA	Standard AES authentication
AUTHENTICATE_EV2_FIRST	0x71	More recent EV2 authentication mode
AUTHENTICATE_EV2_NONFIRST	0x77	More recent EV2 authentication mode
CHANGE_KEY_SETTINGS	0x54	Modify PICC master key properties
SET_CONFIGURATION	0x5C	Used to configure DESFire card or application specific attributes
CHANGE_KEY	0xC4	Changes the key data stored on the PICC
GET_KEY_VERSION	0x64	Returns the active key version stored on the PICC
CREATE_APPLICATION	0xCA	Creates new applications by unique AID
DELETE_APPLICATION	0xDA	Non-restorable deletion operation
GET_APPLICATION_IDS	0x6A	Returns a list of all AID codes stored on the PICC
FREE_MEMORY	0x6E	Returns the total free memory on the tag in bytes
GET_DF_NAMES	0x6D	Obtain the ISO7816-4 DF names associated with the tag
GET_KEY_SETTINGS	0x45	Get permissions data and format for PICC and application master keys
SELECT_APPLICATION	0x5A	Select a specific application by AID for further access

Supported command codes

Command Long Name	INS	Description
FORMAT_PICC	0xFC	Releases the previously stored user memory (not reversible)
GET_VERSION	0x60	Returns manufacturing header data stored in the PICC
GET_CARD_UID	0x51	Returns the 7-byte card UID assigned by the manufacturer
GET_FILE_IDS	0x6F	Get a list of the file identifiers (by index) within the selected AID
GET_FILE_SETTINGS	0xF5	Obtain properties and permissions about a file
CHANGE_FILE_SETTINGS	0x5F	Modify access permissions of an existing file
CREATE_STDDATA_FILE	0xCD	Add new unformatted binary data storage file type
CREATE_BACKUPDATA_FILE	0xCB	Create unformatted binary file with a shadow backup mechanism
CREATE_VALUE_FILE	0xCC	Create new 32-bit integer storage file
CREATE_LINEAR_RECORD_FILE	0xC1	Create new fixed size file for sequential storage of structurally similar record data structures
CREATE_CYCLIC_RECORD_FILE	0xC0	Similar to the linear record case except that there is a wrap-around storage functionality when the file size limit is exceeded

Supported command codes

Command Long Name	INS	Description
DELETE_FILE	0xDF	Non-restorable deactivation of a file within the active AID
GET_ISO_FILE_IDS	0x61	Returns a list of the 2-byte file identifiers of all files within the active AID
READ_DATA	0xBD	Read byte-wise contents of standard or backup file types
WRITE_DATA	0x3D	Write data at an offset to standard or backup file types
GET_VALUE	0x6C	Reads the last permanently stored integer from value records
CREDIT	0x0C	Increase the integer value type in the value type
DEBIT	0xDC	Decrease the integer value type in the value type
LIMITED_CREDIT	0x1C	Increase by a preset limited amount the integer in a value record (must commit the transaction changes at a later time)
WRITE_RECORD	0x3B	Write data to a linear or cyclic record file type
READ_RECORDS	0xBB	List the set of complete records in the associated file type
CLEAR_RECORD_FILE	0xEB	Reset a linear or cyclic record type to an empty state
COMMIT_TRANSACTION	0xC7	Validates the previous write access permissions and credit permissions of all files within the selected AID

Supported command codes

Command Long Name	INS	Description
ABORT_TRANSACTION	0xA7	Invalidate the previous changes to the files within the selected AID
SELECT	0xA4	ISO7816-4 standard command support
GET_CHALLENGE	0x84	ISO7816-4 standard command support
EXTERNAL_AUTHENTICATE	0x82	ISO7816-4 standard command support
INTERNAL_AUTHENTICATE	0x88	ISO7816-4 standard command support
READ_BINARY	0xB0	ISO7816-4 standard command support
UPDATE_BINARY	0xD6	ISO7816-4 standard command support
READ_RECORDS	0xB2	ISO7816-4 standard command support
APPEND_RECORD	0xE2	ISO7816-4 standard command support

Data exchanges with the Chameleon DESFire configuration

```
>>> Select Application By AID:
-> 90 5a 00 00 03 00 00 00 | 00
<- 91 00

>>> Start AES Authenticate:
-> 90 aa 00 00 01 00 00
<- 54 b8 9e fe 19 9b c6 a5 | fd 8f 00 be c1 23 99 c0 | 91 af
-> 90 af 00 00 10 df a0 79 | 13 59 ac 4c 75 5f 81 69 |
   bc 9c 3e c6 7e 00
<- a9 e2 79 42 11 63 9c 14 | 07 b3 02 2f 2e 4b 2e c5 | 91 00

>>> Get AID List From Device:
-> 90 6a 00 00 00 00
<- 77 88 99 01 00 34 91 00

>>> CreateApplication command:
-> 90 ca 00 00 05 77 88 99 | 0f 03 00
<- 91 de

>>> Get AID List From Device:
-> 90 6a 00 00 00 00
<- 77 88 99 01 00 34 91 00
```

An Embedded Open Source DESFire Stack for the Chameleon Mini

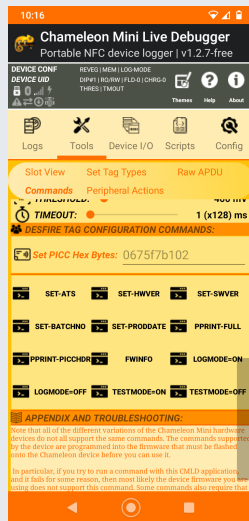
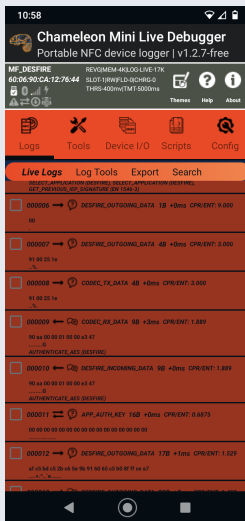
Extensions of the firmware sources to support DESFire tags

- ▶ New native AES support using hardware acceleration support
- ▶ Extensions of prior work to add hardware based DES and 3DES support to the firmware
- ▶ Changes to the codec layer of the firmware to support DESFire tags
- ▶ Enhancements and bug fixes to the LIVE logging functionality of the Chameleon RevG devices
- ▶ New default customized extension of the Chameleon terminal commands to enhance DESFire configuration support for users (see next slide)

Configuration of DESFire emulation support

```
> CONFIG=MF_DESFIRE
> DF_SETHDR=ATS 0675F7B102
> UID=2377000B99BF98
```

```
DF_SETHDR=ATS xxxxxxxxxxxx
DF_SETHDR=HardwareVersion xxxx
DF_SETHDR=SoftwareVersion xxxx
DF_SETHDR=BatchNumber xxxxxxxxxxxx
DF_SETHDR=ProductionDate xxxx
```



DESFire emulation support (anti-collision loop)

NFC reader: SCM Micro / SCL3711-NFC&RW opened

```
Sent bits:      26 (7 bits)
Received bits: 03 44
Sent bits:      93 20
Received bits: 88 23 77 00 dc
Sent bits:      93 70 88 23 77 00 dc 4b b3
Received bits: 04
Sent bits:      95 20
Received bits: 0b 99 bf 98 b5
Sent bits:      95 70 0b 99 bf 98 b5 2f 24
Received bits: 20
Sent bits:      e0 50 bc a5
Received bits: 75 77 81 02 80
Sent bits:      50 00 57 cd
```

Found tag with

UID: 2377000b99bf98

ATQA: 4403

SAK: 20

ATS: 75 77 81 02 80

Challenges with the implementation during development

- ▶ Approximately six to eight months of active development were required to complete the project
- ▶ Forced by local embedded system constraints to carefully optimize and organize our use of the embedded AVR memory to resolve insufficient memory type exceptions
- ▶ The speedup in computations for AES and 3DES operations provides an order of magnitude improvement compared to existing OSS libraries for AVR chips
- ▶ A complicated nested, quasi-linked pointer based structure was required to efficiently store the filesystem entries and tag accounting metadata

Concluding Remarks

Funding sources and support for the project

- ▶ Initial sources for the DESFire Chameleon firmware are due to Dmitry Janushkevich (**@devzzo**) (2017)
- ▶ Professor Josephine Yu in the School of Math at GA Tech in the US
- ▶ The original Kasper and Oswald (KAOS) developers of the Chameleon Mini hardware and software
- ▶ David Oswald from the University of Birmingham in the UK

Wrapping up: Selected quotes on open source software

That brings me to the most important piece of advice that I can give to all of you: if you've got a good idea, and it's a contribution, I want you to go ahead and DO IT. It is much easier to apologize than it is to get permission. – Grace Hopper

I think a lot of the basis of the open source movement comes from procrastinating students. – Andrew Tridgell







Life would be much easier if I had the source code. – Anonymous

Thank you for attending!

References I

-  Android HCE DESFire: A software implementation of Desfire in an Android app. <https://github.com/jekkos/android-hce-desfire>
-  Chameleon Mini Firmware (authoritative sources). <https://github.com/emsec/ChameleonMini>
-  ISO/IEC 14443, 15693 and 7816 Standards. Identification Cards - Contactless Integrated Circuit Cards. www.iso.org
-  Kasper T., von Maurich I., Oswald D., Paar C. (2011) Chameleon: A Versatile Emulator for Contactless Smartcards. In: Rhee KH., Nyang D. (eds) Information Security and Cryptology - ICISC 2010. ICISC 2010. Lecture Notes in Computer Science, vol 6829. Springer, Berlin, Heidelberg. https://doi.org/10.1007/978-3-642-24209-0_13
-  Kasper, T. and Oswald, D. Presentation slides on the history of the Chameleon Mini devices. https://raw.githubusercontent.com/wiki/emsec/ChameleonMini/Images/160110_ChameleonMini_history_smaller.pdf

References II

-  LibFreeFare: A convenience API for NFC cards manipulations on top of LibNFC. <https://github.com/nfc-tools/libfreefare>
-  LibNFC: A platform independent NFC library. <https://github.com/nfc-tools/libnfc>
-  Microchip. ATxmega1284U Data Sheet. <https://ww1.microchip.com/downloads/en/DeviceDoc/ATxmega128-64-32-16A4U-DataSheet-DS40002166A.pdf>
-  NXP Semiconductors. MIFARE DESFire Functional specification. Publicly available MF3ICD81 datasheet (2008). <https://tinycloud.com/kwweanp9>
-  Philips Semiconductors. Mifare DESFire: Contactless multi-application IC with DES and 3DES security. Publicly available MF3-IC-D40 datasheet (2004). <https://tinycloud.com/5era3dx2>
-  Proxmark III. A Radio Frequency IDentification Tool. <http://www.proxmark.org>

References III



Schmidt, M. D. Chameleon Mini DESFire Stack (development sources).
<https://github.com/maxieds/ChameleonMiniDESFireStack>



Schmidt, M. D. Chameleon Mini Live Debugger.
<https://github.com/maxieds/ChameleonMiniLiveDebugger>