Rogue7:

Rouge Engineering-Station Attacks on Simatic S7 PLCs

Sara Bitan
CyberDay 2020

Joint work:

Eli Biham. Aviad Carmel, Alon Dankner, Uriel Malin, Avishai Wool

Technion Tel-Aviv University

Talk Topics

1. Uncovered design vulnerabilities in the S7 protocol
2. An exploit that performs remote stealth programming of an S7-1500 PLC

The Operator

The Engineer

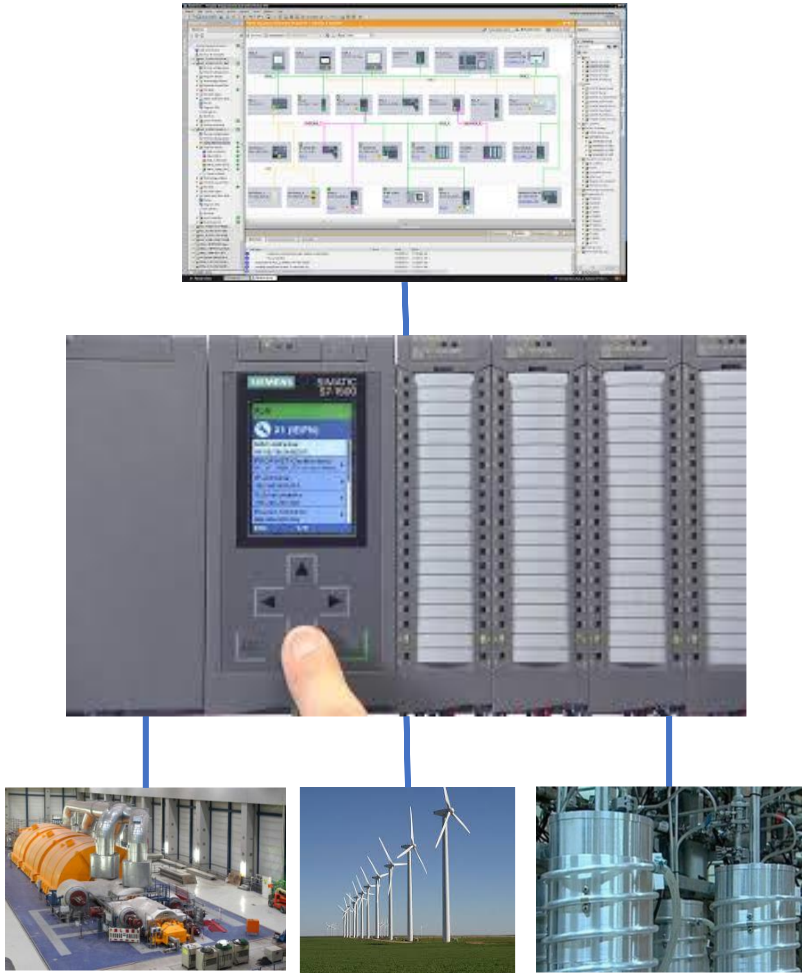
The Attacker

What are Industrial Control Systems?

- A distributed computerized system
- Operates and monitors physical devices
- Controls critical infrastructure

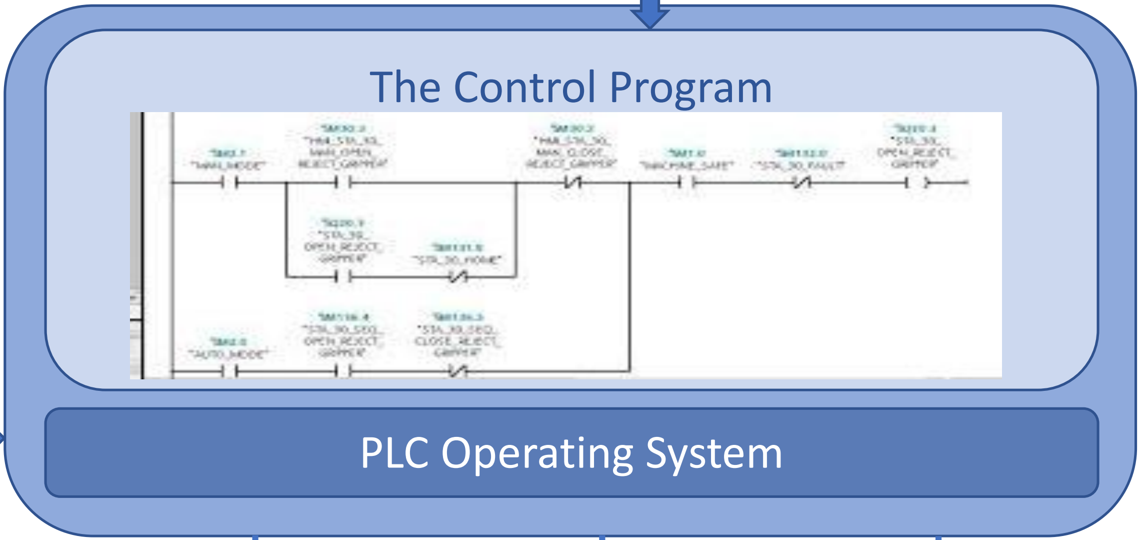
PLC - Programmable Logic Controller

- The core of the ICS
- A bridge between the virtual and the kinetic worlds
- The target of our attacks

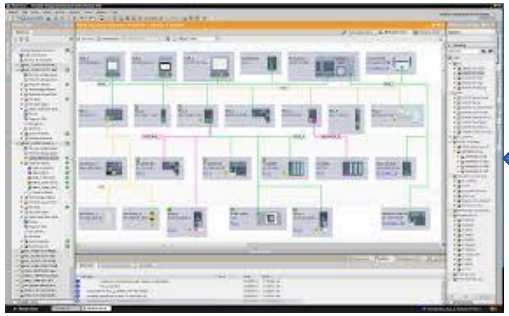


PLC Interfaces - Our Way In!

S7 Protocol

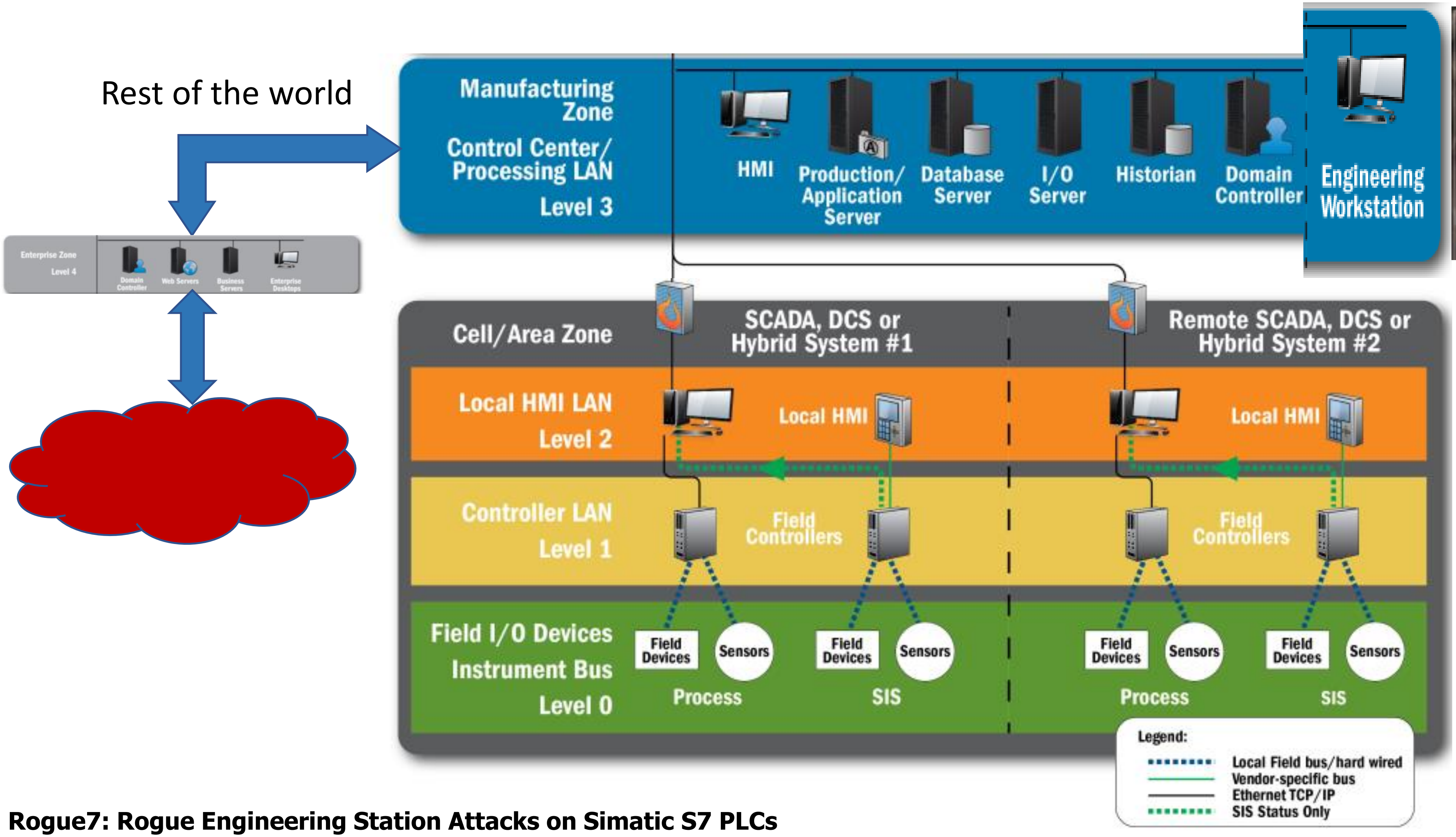

The Control Program
"MAN_MODE"
"HMI_STA_30_MAN_OPEN_REJECT_GRIPPER"
"HMI_STA_30_MAN_CLOSE_REJECT_GRIPPER"
"MACHINE_SAFE"
"STA_30_FAULT"
"STA_30_OPEN_REJECT_GRIPPER"
"STA_30_OPEN_REJECT_GRIPPER"
"STA_30_HOME"
"AUTO_MODE"
"STA_30_SEQ_OPEN_REJECT_GRIPPER"
"STA_30_SEQ_CLOSE_REJECT_GRIPPER"
PLC Operating System

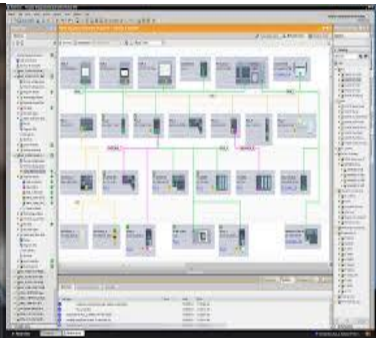
S7-1500

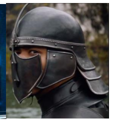


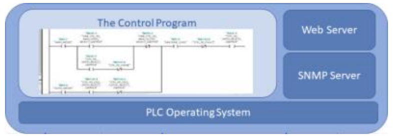
S7 Protocol

Secure ICS Topology









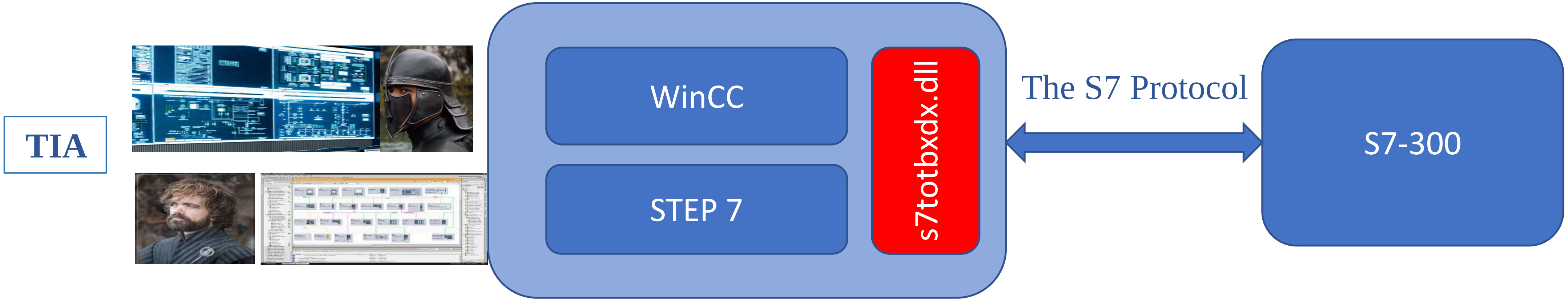
Source: NCCIC IR-18-214

ICS Security Challenges

- No automatic update or frequent patching
- No inline protection

Stuxnet Malware (9/2010)

- The most famous cyber-attack on ICS
- Targeted Siemens S7-300 PLC
- Infected both HMI and engineering station packages

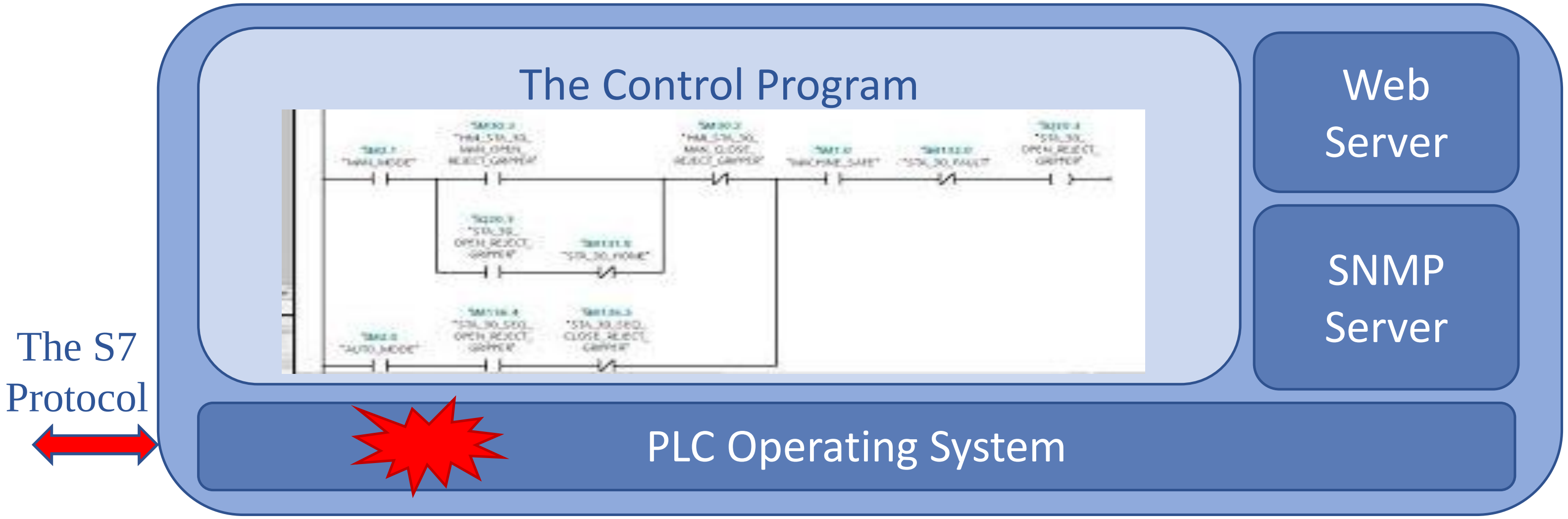


TIA as a Soft Belly

- Typically attacks are exploiting the engineering station vulnerabilities:
  - CVE-2012-3015 : untrusted search path vulnerability in Siemens SIMATIC STEP7 v5.5– July-26-2012
  - CVE-2019-10915: authentication bypass in TIA v15.1 –July-11-19 by Tenable Security

Our Attack

- Exploits vulnerabilities in the PLC Operating System
  - S7 protocol
- Any vulnerable station/ device in the network can serve as an attack machine

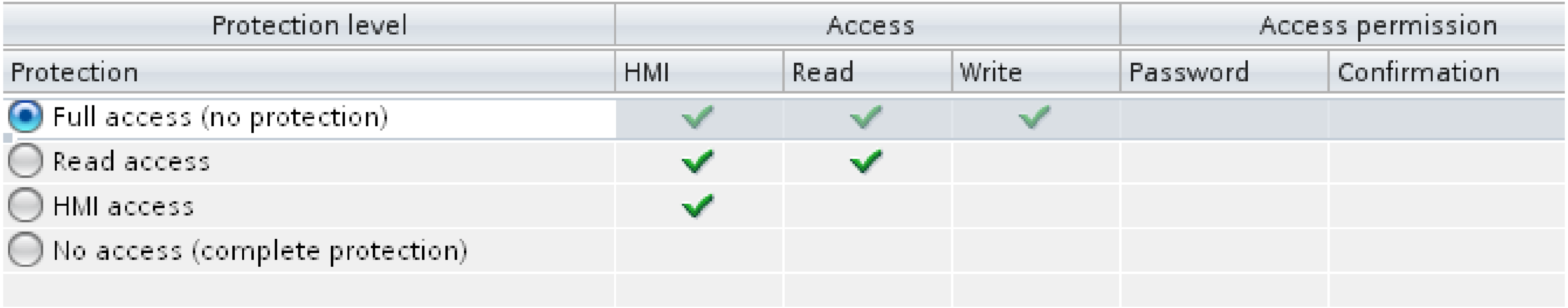


Siemens S7-1500 PLC

- One of two new members in the SIMATIC PLCs product line
  - S7-1500 is the high-end PLC
  - The other is S7-1200

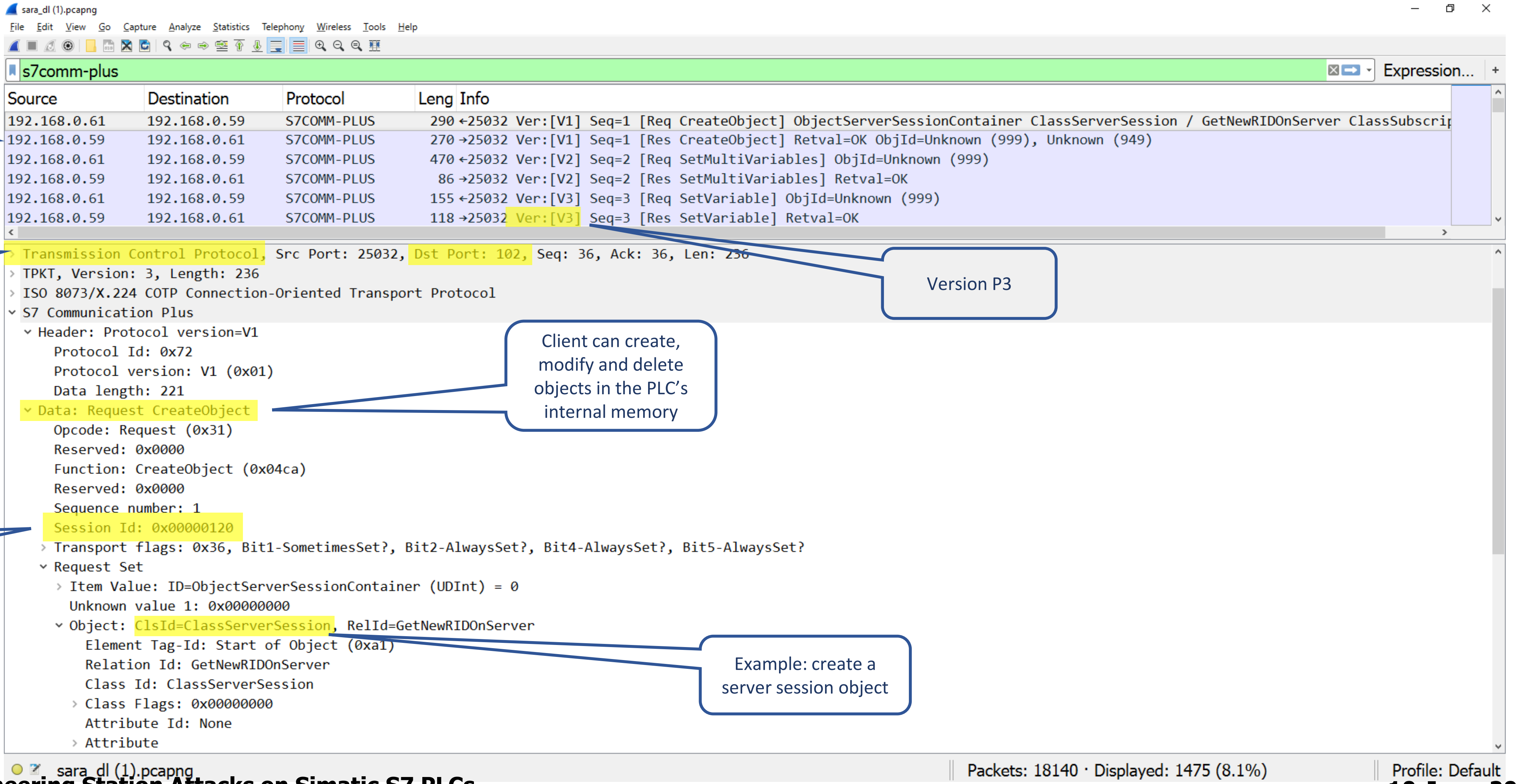
Why We Targeted S7 PLCs?

- Security enhancements of the S7 protocol
  - Integrity and replay protection of the messages
- PLC access control – password based
  - **Blocks our attack, but not always used**



Protection level	Access			Access permission	
Protection	HMI	Read	Write	Password	Confirmation
● Full access (no protection)	✓	✓	✓		
○ Read access	✓	✓			
○ HMI access	✓				
○ No access (complete protection)					

The S7 Protocol



s7comm-plus

```
Source         Destination    Protocol      Leng Info
192.168.0.61   192.168.0.59   S7COMM-PLUS    290 ←25032 Ver:[V1] Seq=1 [Req CreateObject] ObjectServerSessionContainer ClassServerSession / GetNewRIDOnServer ClassSubscrip
192.168.0.59   192.168.0.61   S7COMM-PLUS    270 →25032 Ver:[V1] Seq=1 [Res CreateObject] Retval=OK ObjId=Unknown (999), Unknown (949)
192.168.0.61   192.168.0.59   S7COMM-PLUS    470 ←25032 Ver:[V2] Seq=2 [Req SetMultiVariables] ObjId=Unknown (999)
192.168.0.59   192.168.0.61   S7COMM-PLUS     86 →25032 Ver:[V2] Seq=2 [Res SetMultiVariables] Retval=OK
192.168.0.61   192.168.0.59   S7COMM-PLUS    155 ←25032 Ver:[V3] Seq=3 [Req SetVariable] ObjId=Unknown (999)
192.168.0.59   192.168.0.61   S7COMM-PLUS    118 →25032 Ver:[V3] Seq=3 [Res SetVariable] Retval=OK
```

```
> Transmission Control Protocol, Src Port: 25032, Dst Port: 102, Seq: 36, Ack: 36, Len: 236
> TPKT, Version: 3, Length: 236
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
v S7 Communication Plus
  v Header: Protocol version=V1
      Protocol Id: 0x72
      Protocol version: V1 (0x01)
      Data length: 221
  v Data: Request CreateObject
      Opcode: Request (0x31)
      Reserved: 0x0000
      Function: CreateObject (0x04ca)
      Reserved: 0x0000
      Sequence number: 1
      Session Id: 0x00000120
    > Transport flags: 0x36, Bit1-SometimesSet?, Bit2-AlwaysSet?, Bit4-AlwaysSet?, Bit5-AlwaysSet?
    v Request Set
      > Item Value: ID=ObjectServerSessionContainer (UDInt) = 0
        Unknown value 1: 0x00000000
      v Object: ClsId=ClassServerSession, RelId=GetNewRIDOnServer
          Element Tag-Id: Start of Object (0xa1)
          Relation Id: GetNewRIDOnServer
          Class Id: ClassServerSession
        > Class Flags: 0x00000000
          Attribute Id: None
        > Attribute
```

sara_dl (1).pcapng | Packets: 18140 · Displayed: 1475 (8.1%) | Profile: Default

Session oriented. Session begins with a 4-ways handshake

ISO transport over TCP

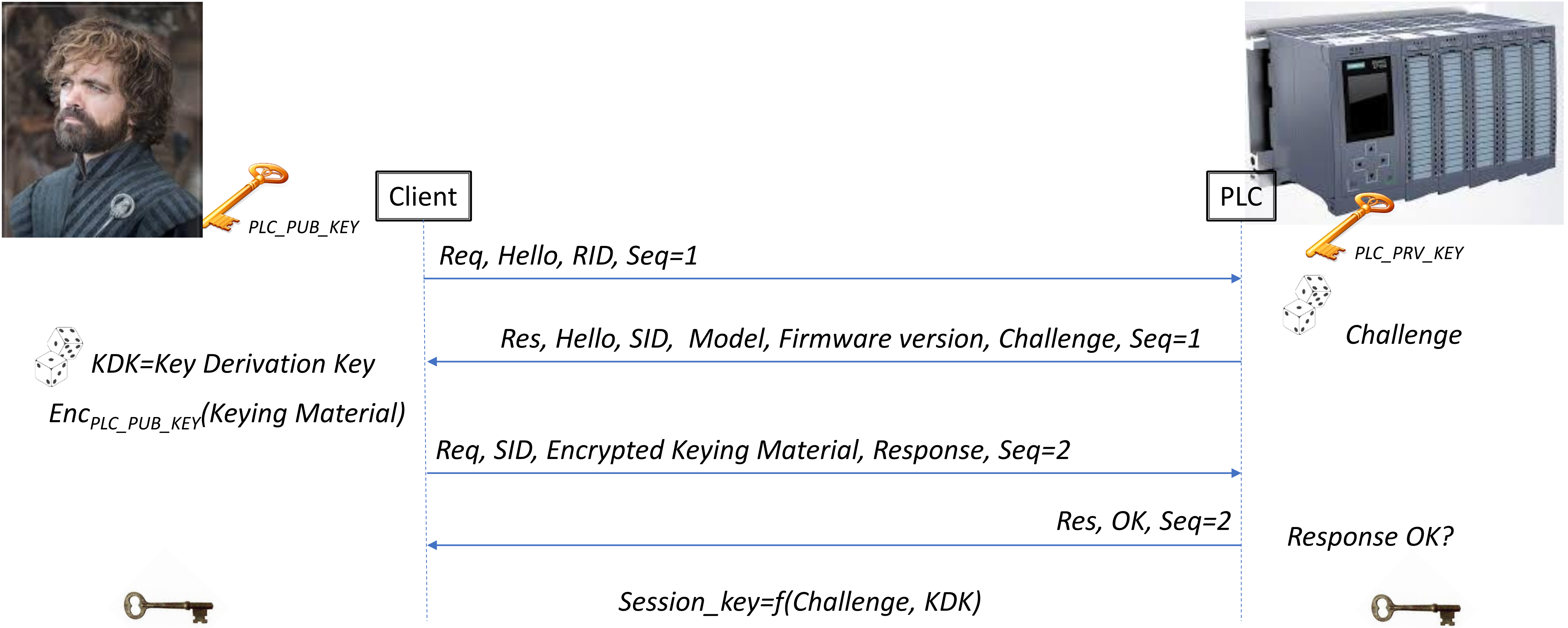
Version P3

Client can create, modify and delete objects in the PLC's internal memory

Session ID

Example: create a server session object

The P3 Handshake Protocol



PLC_PUB_KEY

Client

PLC

PLC_PRV_KEY

Req, Hello, RID, Seq=1

Challenge

Res, Hello, SID, Model, Firmware version, Challenge, Seq=1

KDK=Key Derivation Key

$Enc_{PLC\_PUB\_KEY}$(Keying Material)

Req, SID, Encrypted Keying Material, Response, Seq=2

Res, OK, Seq=2

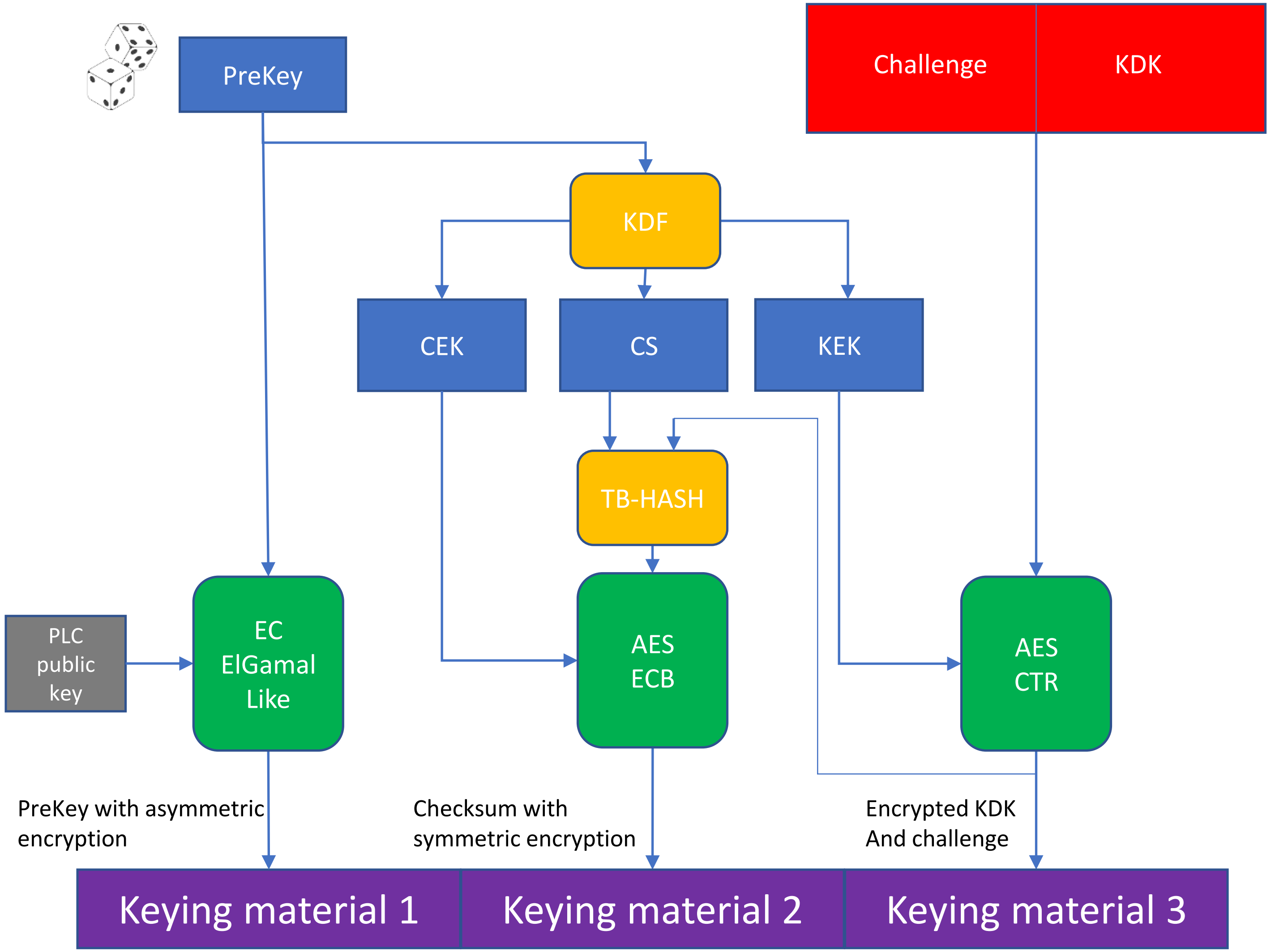
Response OK?

Session_key=f(Challenge, KDK)

- Integrity protection: hmac-sha256 over packet with Session_key

P3 – KDK Sharing

1. Generate 20 bytes PreKey
    1. Encrypt it using EC-ElGamal–like encryption with the plc public key and add it to Keying material
2. Calculate KDF on PreKey and get
    1. Checksum Encryption Key (CEK)
    2. Checksum Seed (CS)
    3. Key Encryption Key (KEK)
3. Concatenate the KDK to the challenge, encrypt them using AES-CTR with the KEK, and add to Keying material
4. Initiate a Tabulation Hash with CS and calculate checksum over (3)
5. Encrypt (4) using AES-ECB with CEK and add to Keying material



P3 – Asymmetric Keys

- The public keys are stored in compressed .key files at

  [TIA INSTALLATION]\Data\Hwcn\Custom

- Each key file contains
  - Metadata (version, key type, key family, etc.)
  - **Key data – PLC public key for the EC-ElGamal-like encryption**

P3 – An Example .key File

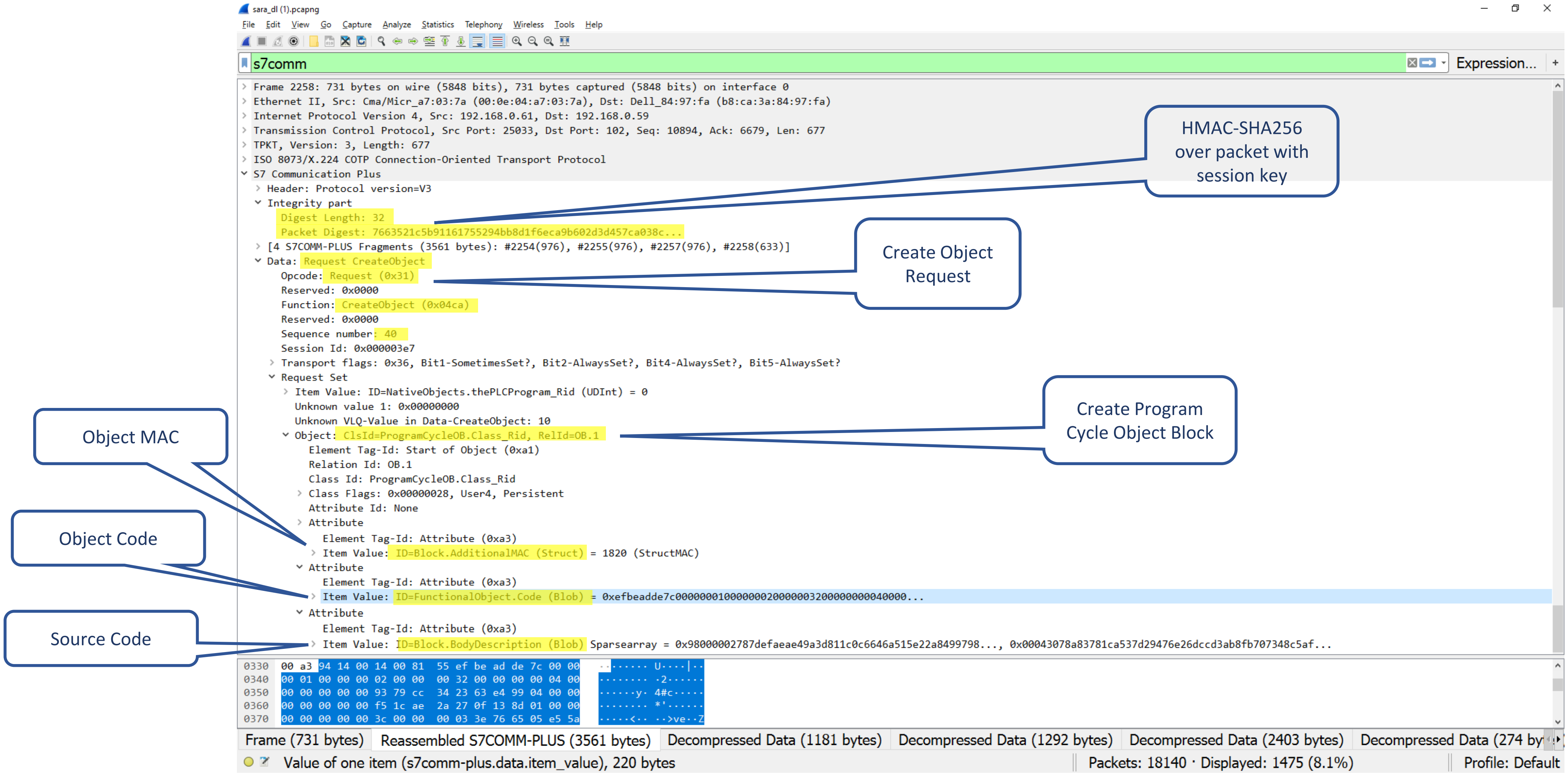
```
version: 1

orderNumber: s71500-connection

firmwareVersion:

keyType: connection

familyType: S7-1500

key data: 8456…
```

One Ring to Rule Them All

With Many Working Forged Copies

Attacking the P3 Program Download Exchange

Control Program Create Message



sara_dl (1).pcapng
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help
s7comm
Expression…
+

```
> Frame 2258: 731 bytes on wire (5848 bits), 731 bytes captured (5848 bits) on interface 0
> Ethernet II, Src: Cma/Micr_a7:03:7a (00:0e:04:a7:03:7a), Dst: Dell_84:97:fa (b8:ca:3a:84:97:fa)
> Internet Protocol Version 4, Src: 192.168.0.61, Dst: 192.168.0.59
> Transmission Control Protocol, Src Port: 25033, Dst Port: 102, Seq: 10894, Ack: 6679, Len: 677
> TPKT, Version: 3, Length: 677
> ISO 8073/X.224 COTP Connection-Oriented Transport Protocol
v S7 Communication Plus
  > Header: Protocol version=V3
  v Integrity part
      Digest Length: 32
      Packet Digest: 7663521c5b91161755294bb8d1f6eca9b602d3d457ca038c...
  > [4 S7COMM-PLUS Fragments (3561 bytes): #2254(976), #2255(976), #2257(976), #2258(633)]
  v Data: Request CreateObject
      Opcode: Request (0x31)
      Reserved: 0x0000
      Function: CreateObject (0x04ca)
      Reserved: 0x0000
      Sequence number: 40
      Session Id: 0x000003e7
    > Transport flags: 0x36, Bit1-SometimesSet?, Bit2-AlwaysSet?, Bit4-AlwaysSet?, Bit5-AlwaysSet?
    v Request Set
      > Item Value: ID=NativeObjects.thePLCProgram_Rid (UDInt) = 0
        Unknown value 1: 0x00000000
        Unknown VLQ-Value in Data-CreateObject: 10
      v Object: ClsId=ProgramCycleOB.Class_Rid, RelId=OB.1
          Element Tag-Id: Start of Object (0xa1)
          Relation Id: OB.1
          Class Id: ProgramCycleOB.Class_Rid
        > Class Flags: 0x00000028, User4, Persistent
          Attribute Id: None
        > Attribute
            Element Tag-Id: Attribute (0xa3)
          > Item Value: ID=Block.AdditionalMAC (Struct) = 1820 (StructMAC)
        v Attribute
            Element Tag-Id: Attribute (0xa3)
          > Item Value: ID=FunctionalObject.Code (Blob) = 0xefbeadde7c000000100000002000000032000000000040000...
        v Attribute
            Element Tag-Id: Attribute (0xa3)
          > Item Value: ID=Block.BodyDescription (Blob) Sparsearray = 0x98000002787defaeae49a3d811c0c6646a515e22a8499798..., 0x00043078a83781ca537d29476e26dccd3ab8fb707348c5af...
```

```
0330  00 a3 94 14 00 14 00 81  55 ef be ad de 7c 00 00   ········ U····|··
0340  00 01 00 00 00 02 00 00  00 32 00 00 00 00 04 00   ········ ·2······
0350  00 00 00 00 00 93 79 cc  34 23 63 e4 99 04 00 00   ······y· 4#c·····
0360  00 00 00 00 00 f5 1c ae  2a 27 0f 13 8d 01 00 00   ········ *'······
0370  00 00 00 00 00 3c 00 00  00 03 3e 76 65 05 e5 5a   ·····<·· ··>ve··Z
```

Frame (731 bytes)
Reassembled S7COMM-PLUS (3561 bytes)
Decompressed Data (1181 bytes)
Decompressed Data (1292 bytes)
Decompressed Data (2403 bytes)
Decompressed Data (274 by

Value of one item (s7comm-plus.data.item_value), 220 bytes

Packets: 18140 · Displayed: 1475 (8.1%)

Profile: Default

HMAC-SHA256 over packet with session key

Create Object Request

Create Program Cycle Object Block

Object MAC

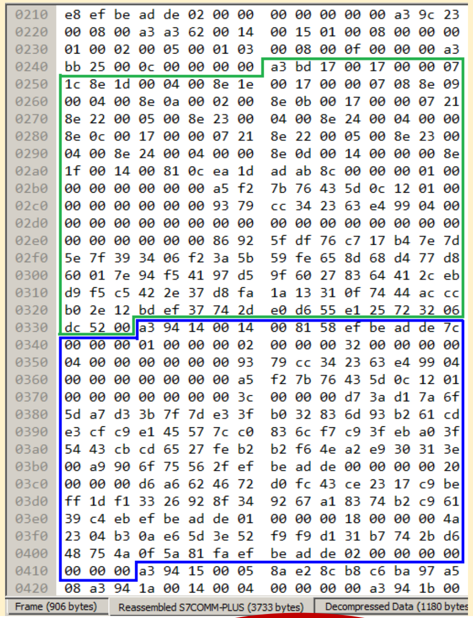
Object Code

Source Code

Control Program Representation

Object MAC

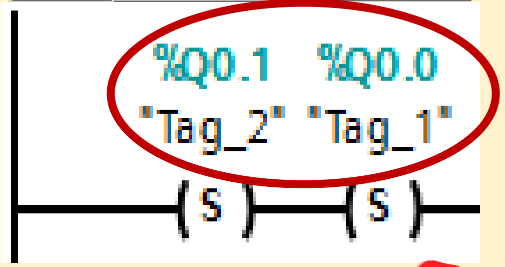
Object Code

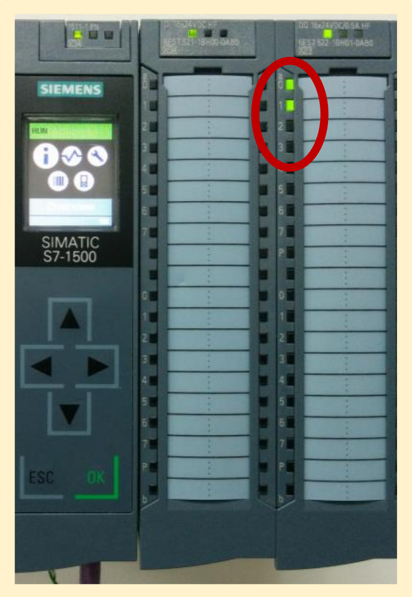


```
0210  e8 ef be ad de 02 00 00  00 00 00 00 00 a3 9c 23
0220  00 08 00 a3 a3 62 00 14  00 15 01 00 08 00 00 00
0230  01 00 02 00 05 00 01 03  00 08 00 0f 00 00 00 a3
0240  bb 25 00 0c 00 00 00 00  a3 bd 17 00 17 00 00 07
0250  1c 8e 1d 00 04 00 8e 1e  00 17 00 00 07 08 8e 09
0260  00 04 00 8e 0a 00 02 00  8e 0b 00 17 00 00 07 21
0270  8e 22 00 05 00 8e 23 00  04 00 8e 24 00 04 00 00
0280  8e 0c 00 17 00 00 07 21  8e 22 00 05 00 8e 23 00
0290  04 00 8e 24 00 04 00 00  8e 0d 00 14 00 00 00 8e
02a0  1f 00 14 00 81 0c ea 1d  ad ab 8c 00 00 00 01 00
02b0  00 00 00 00 00 00 a5 f2  7b 76 43 5d 0c 12 01 00
02c0  00 00 00 00 00 00 93 79  cc 34 23 63 e4 99 04 00
02d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02e0  00 00 00 00 00 00 86 92  5f df 76 c7 17 b4 7e 7d
02f0  5e 7f 39 34 06 f2 3a 5b  59 fe 65 8d 68 d4 77 d8
0300  60 01 7e 94 f5 41 97 d5  9f 60 27 83 64 41 2c eb
0310  d9 f5 c5 42 2e 37 d8 fa  1a 13 31 0f 74 44 ac cc
0320  b0 2e 12 bd ef 37 74 2d  e0 d6 55 e1 25 72 32 06
0330  dc 52 00 a3 94 14 00 14  00 81 58 ef be ad de 7c
0340  00 00 00 01 00 00 00 02  00 00 00 32 00 00 00 00
0350  04 00 00 00 00 00 00 93  79 cc 34 23 63 e4 99 04
0360  00 00 00 00 00 00 00 a5  f2 7b 76 43 5d 0c 12 01
0370  00 00 00 00 00 00 00 3c  00 00 00 d7 3a d1 7a 6f
0380  5d a7 d3 3b 7f 7d e3 3f  b0 32 83 6d 93 b2 61 cd
0390  e3 cf c9 e1 45 57 7c c0  83 6c f7 c9 3f eb a0 3f
03a0  54 43 cb cd 65 27 fe b2  b2 f6 4e a2 e9 30 31 3e
03b0  00 a9 90 6f 75 56 2f ef  be ad de 00 00 00 00 20
03c0  00 00 00 d6 a6 62 46 72  d0 fc 43 ce 23 17 c9 be
03d0  ff 1d f1 33 26 92 8f 34  92 67 a1 83 74 b2 c9 61
03e0  39 c4 eb ef be ad de 01  00 00 00 18 00 00 00 4a
03f0  23 04 b3 0a e6 5d 3e 52  f9 f9 d1 31 b7 74 2b d6
0400  48 75 4a 0f 5a 81 fa ef  be ad de 02 00 00 00 00
0410  00 00 00 a3 94 15 00 05  8a e2 8c b8 c6 ba 97 a5
0420  08 a3 94 1a 00 14 00 04  00 00 00 00 a3 94 1b 00
```

Frame (906 bytes) | Reassembled S7COMM-PLUS (3733 bytes) | Decompressed Data (1180 bytes

Source Code

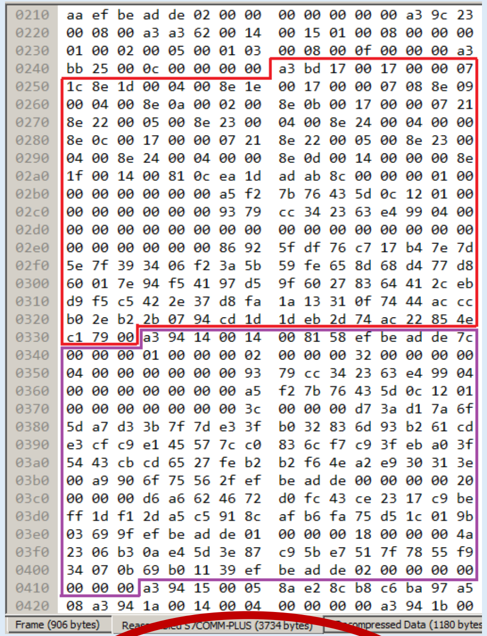




Yellow Program

Object MAC

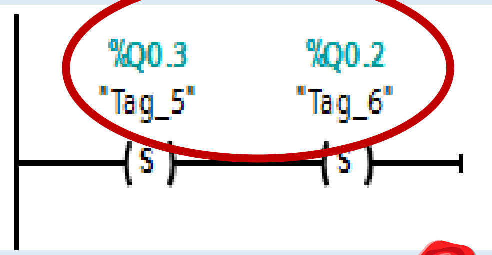
Object Code

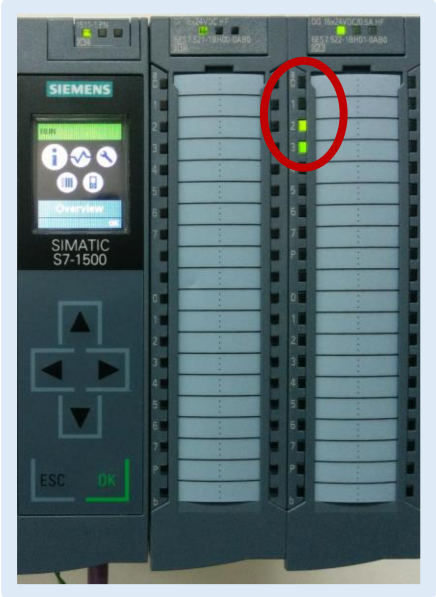


```
0210  aa ef be ad de 02 00 00  00 00 00 00 00 a3 9c 23
0220  00 08 00 a3 a3 62 00 14  00 15 01 00 08 00 00 00
0230  01 00 02 00 05 00 01 03  00 08 00 0f 00 00 00 a3
0240  bb 25 00 0c 00 00 00 00  a3 bd 17 00 17 00 00 07
0250  1c 8e 1d 00 04 00 8e 1e  00 17 00 00 07 08 8e 09
0260  00 04 00 8e 0a 00 02 00  8e 0b 00 17 00 00 07 21
0270  8e 22 00 05 00 8e 23 00  04 00 8e 24 00 04 00 00
0280  8e 0c 00 17 00 00 07 21  8e 22 00 05 00 8e 23 00
0290  04 00 8e 24 00 04 00 00  8e 0d 00 14 00 00 00 8e
02a0  1f 00 14 00 81 0c ea 1d  ad ab 8c 00 00 00 01 00
02b0  00 00 00 00 00 00 a5 f2  7b 76 43 5d 0c 12 01 00
02c0  00 00 00 00 00 00 93 79  cc 34 23 63 e4 99 04 00
02d0  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00
02e0  00 00 00 00 00 00 86 92  5f df 76 c7 17 b4 7e 7d
02f0  5e 7f 39 34 06 f2 3a 5b  59 fe 65 8d 68 d4 77 d8
0300  60 01 7e 94 f5 41 97 d5  9f 60 27 83 64 41 2c eb
0310  d9 f5 c5 42 2e 37 d8 fa  1a 13 31 0f 74 44 ac cc
0320  b0 2e b2 2b 07 94 cd 1d  1d eb 2d 74 ac 22 85 4e
0330  c1 79 00 a3 94 14 00 14  00 81 58 ef be ad de 7c
0340  00 00 00 01 00 00 00 02  00 00 00 32 00 00 00 00
0350  04 00 00 00 00 00 00 93  79 cc 34 23 63 e4 99 04
0360  00 00 00 00 00 00 00 a5  f2 7b 76 43 5d 0c 12 01
0370  00 00 00 00 00 00 00 3c  00 00 00 d7 3a d1 7a 6f
0380  5d a7 d3 3b 7f 7d e3 3f  b0 32 83 6d 93 b2 61 cd
0390  e3 cf c9 e1 45 57 7c c0  83 6c f7 c9 3f eb a0 3f
03a0  54 43 cb cd 65 27 fe b2  b2 f6 4e a2 e9 30 31 3e
03b0  00 a9 90 6f 75 56 2f ef  be ad de 00 00 00 00 20
03c0  00 00 00 d6 a6 62 46 72  d0 fc 43 ce 23 17 c9 be
03d0  ff 1d f1 2d a5 c5 91 8c  af b6 fa 75 d5 1c 01 9b
03e0  03 69 9f ef be ad de 01  00 00 00 18 00 00 00 4a
03f0  23 06 b3 0a e4 5d 3e 87  c9 5b e7 51 7f 78 55 f9
0400  34 07 0b 69 b0 11 39 ef  be ad de 02 00 00 00 00
0410  00 00 00 a3 94 15 00 05  8a e2 8c b8 c6 ba 97 a5
0420  08 a3 94 1a 00 14 00 04  00 00 00 00 a3 94 1b 00
```

Frame (906 bytes) | Reassembled S7COMM-PLUS (3734 bytes) | Decompressed Data (1180 bytes

Source Code





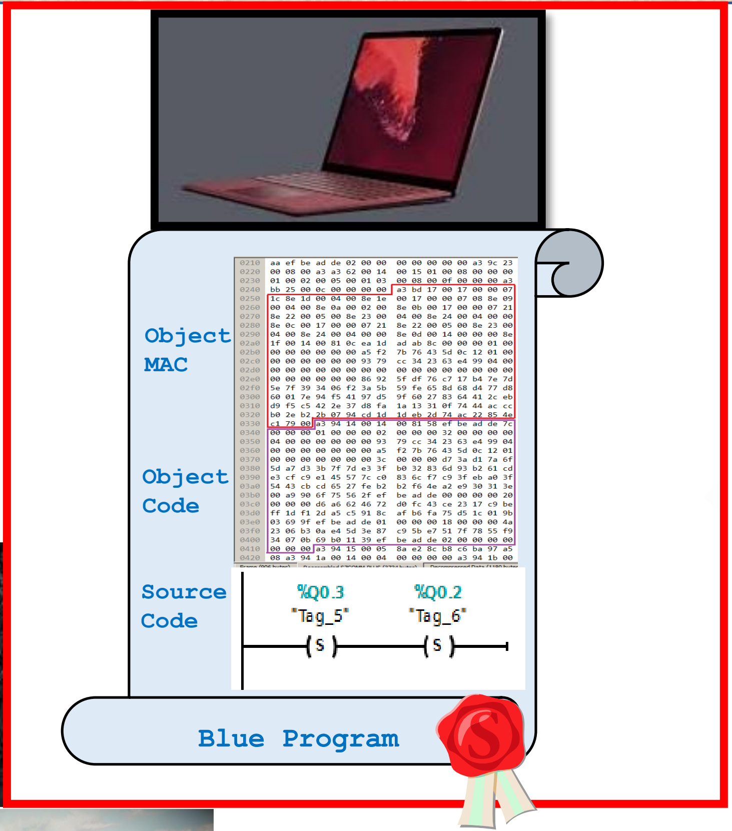
Blue Program

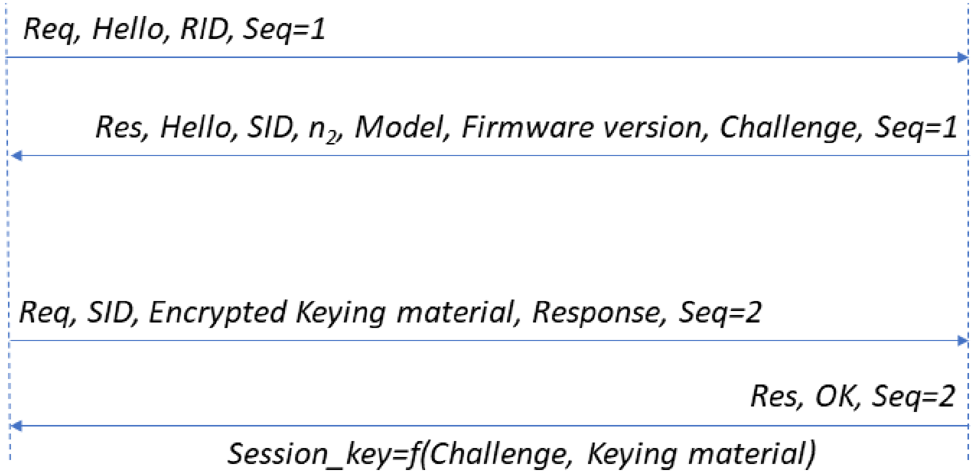
Rogue Engineering Station

Rogue Engineering Station

- An attack script that impersonates a TIA

Rogue Engineering Workstation Program Download Attack





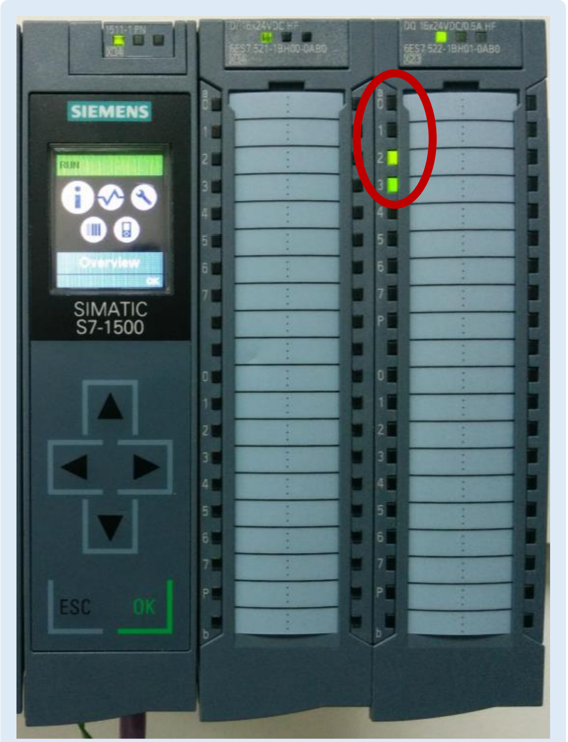
Req, Hello, RID, Seq=1

Res, Hello, SID, n_2, Model, Firmware version, Challenge, Seq=1

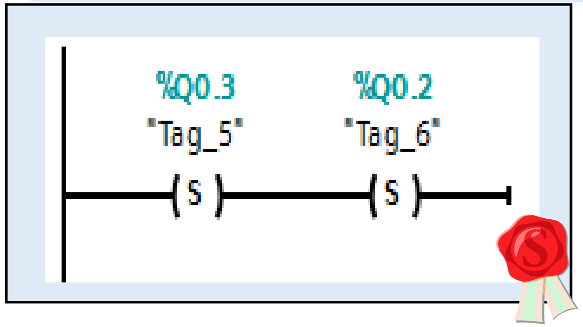
Req, SID, Encrypted Keying material, Response, Seq=2

Res, OK, Seq=2

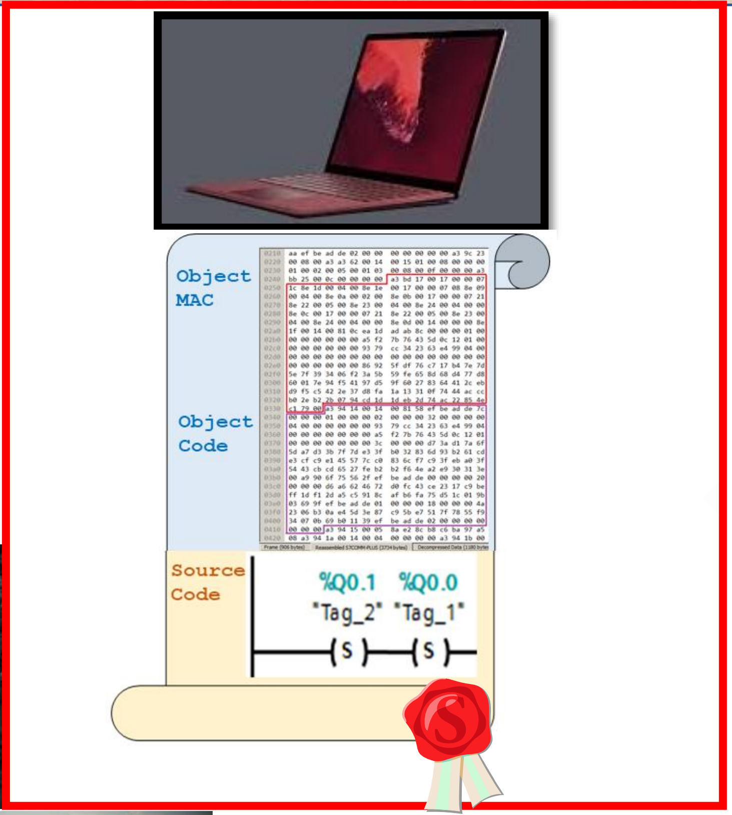
Session_key=f(Challenge, Keying material)

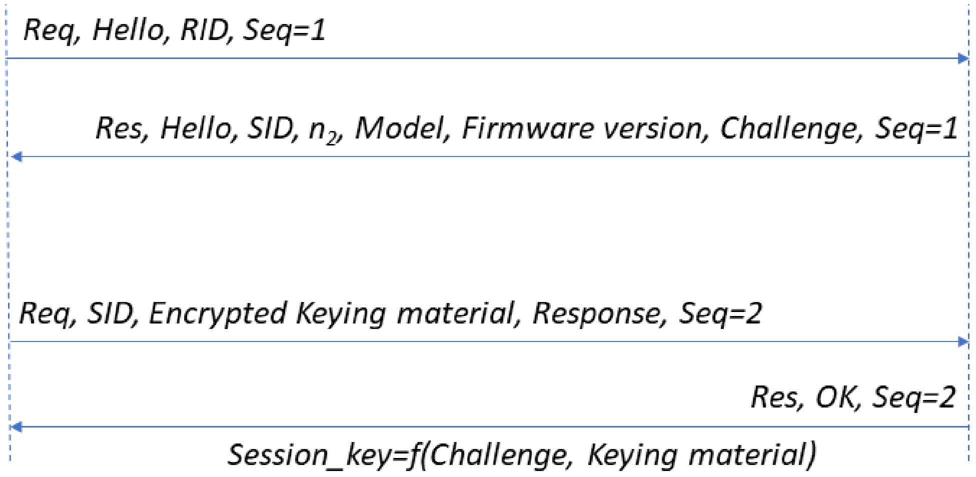


Run



Rogue Engineering Workstation
Stealth Program Injection





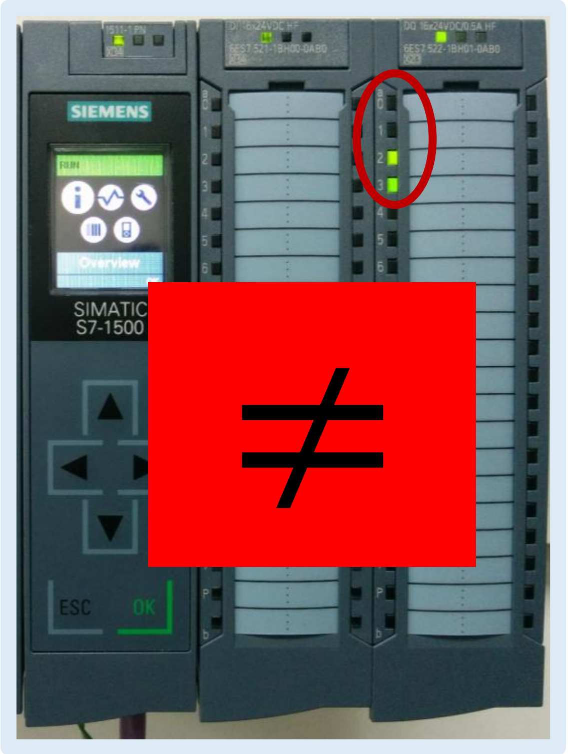
Req, Hello, RID, Seq=1

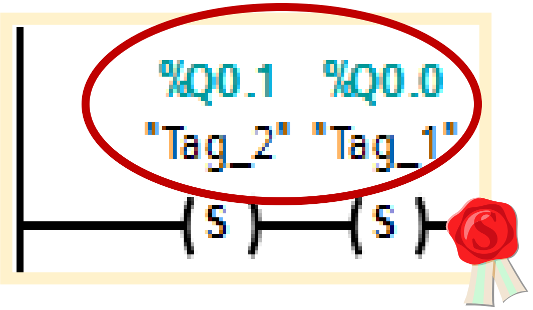
Res, Hello, SID, n_2, Model, Firmware version, Challenge, Seq=1

Req, SID, Encrypted Keying material, Response, Seq=2

Res, OK, Seq=2

Session_key=f(Challenge, Keying material)





Run

Step7 Impersonation

My Lab

The Wall

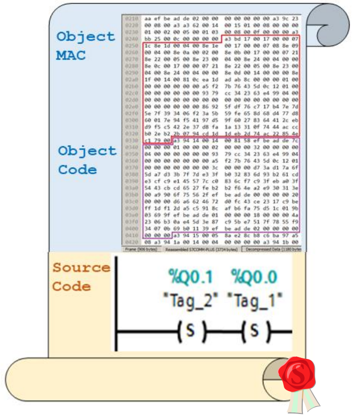
King’s Landing

Rogue Engineering Station
Stealth Program Injection

Attack Demo

Summary

- Vulnerabilities in the S7 protocol – P3
  - TIA is not authenticated
  - “One Ring to Rule them All”
- A Python attack tool that impersonates TIA
  - Download a recorded program to any S7-1500 PLC
  - Stealth program injection attack



Thank you!

SaraB@cs.technion.ac.il