The spear to break the security wall of S7CommPlus

CHENG LEI , NSFOCUS

OverView

- PLC and Siemens PLC intorduction
- S7CommPlus protocol
- Encryption Part Analyze
- Protections

Related Work

- Dillon Beresford. Exploiting Siemens Simatic S7 PLCs. Black Hat 2011 USA.

- Ralf Spenneberg et. al.
  PLC-Blaster: A Worm Living Solely in the PLC. Black Hat
  2016 USA

- This talk mainly focus on the current encrypted S7CommPlus protocol

What is PLC

Programmable Logic Controllers (PLC) is responsible for process control in industrial control system. A PLC contains a Central Processing Unit (CPU), some digital/analog inputs and outputs modules, communication module and some process modules like PID.

Siemens PLCs

S7-300

- S7-200,S7-300,S7-400 using the S7Comm protocol

S7-1200

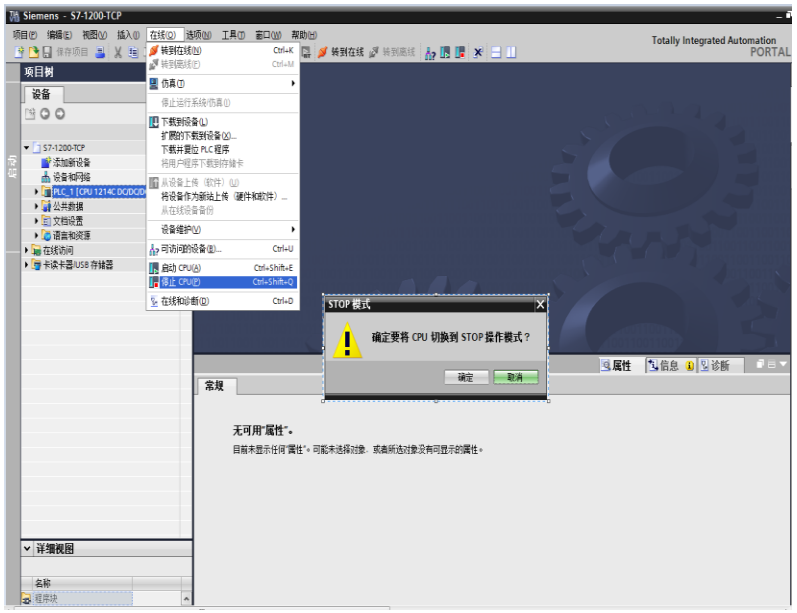
- S7-1200v3.0 using the early S7CommPlus protocol

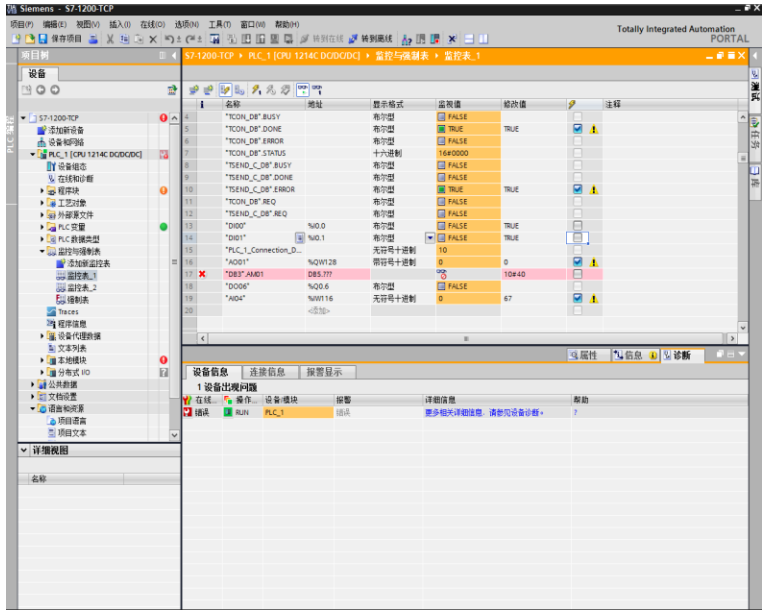
S7-1500

- S7-1200v4.0, S7-1500 using the current encrypted S7CommPlus protocol

TIA Portal

TIA Portal is the configuration and programming software for Siemens PLCs.





Replay Attack

- Replay attacks have been widely used in PLC attacks.
- Get the communication sequence packets with the help of Wireshark

No.	Time	Source	Destination	Protocol	Length	Info
1019	2017-02-24 13:37:26.264282	10.65.96.89	10.65.60.73	TCP	66	5208→102 [SYN] Seq=0 Win=8192 Len=0 MSS=1460 WS=4 SACK_PERM=1
[illegible]	[illegible]:37:26.266384	10.65.60.73	10.65.96.89	TCP	60	102→5208 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
1022	2017-02-24 13:37:26.266509	10.65.96.89	10.65.60.73	TCP	54	5208→102 [ACK] Seq=1 Ack=1 Win=64240 Len=0
1023	2017-02-24 13:37:26.267364	10.65.96.89	10.65.60.73	COTP	89	CR TPDU src-ref: 0x0003 dst-ref: 0x0000
1025	2017-02-24 13:37:26.269514	10.65.60.73	10.65.96.89	COTP	89	CC TPDU src-ref: 0x0001 dst-ref: 0x0003
1026	2017-02-24 13:37:26.276317	10.65.96.89	10.65.60.73	S7COMM-PLUS	289	→5208 PDU-Type: [Connect] Op: [Request] Function: [CreateObject] Se…
1027	2017-02-24 13:37:26.286598	10.65.60.73	10.65.96.89	S7COMM-PLUS	251	→5208 PDU-Type: [Connect] Op: [Response] Function: [CreateObject] S…
16[illegible]	[illegible] 13:37:26.287630	10.65.96.89	10.65.60.73	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
16[illegible]	[illegible] 13:37:26.331976	10.65.96.89	10.65.60.73	S7COMM-PLUS	472	→5208 PDU-Type: [Data] Op: [Request] Function: [SetMultiVariables] …
1039	2017-02-24 13:37:26.360397	10.65.60.73	10.65.96.89	TCP	60	102→5208 [ACK] Seq=233 Ack=696 Win=8192 Len=0
1054	2017-02-24 13:37:26.459946	10.65.60.73	10.65.96.89	S7COMM-PLUS	86	→5208 PDU-Type: [Data] Op: [Response] Function: [SetMultiVariables]…
1056	2017-02-24 13:37:26.460261	10.65.96.89	10.65.60.73	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
1072	2017-02-24 13:37:26.556614	10.65.60.73	10.65.96.89	TCP	60	102→5208 [ACK] Seq=265 Ack=703 Win=8192 Len=0
1092	2017-02-24 13:37:26.693001	10.65.96.89	10.65.60.73	S7COMM-PLUS	155	→5208 PDU-Type: [DataFW1_5] Op: [Request] Function: [GetVarSubStrea…
1093	2017-02-24 13:37:26.697851	10.65.60.73	10.65.96.89	S7COMM-PLUS	129	→5208 PDU-Type: [DataFW1_5] Op: [Response] Function: [GetVarSubStre…
1094	2017-02-24 13:37:26.697987	10.65.96.89	10.65.60.73	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
1150	2017-02-24 13:37:27.081996	10.65.96.89	10.65.60.73	S7COMM-PLUS	155	→5208 PDU-Type: [DataFW1_5] Op: [Request] Function: [SetVariable] S…
1151	2017-02-24 13:37:27.087581	10.65.60.73	10.65.96.89	S7COMM-PLUS	118	→5208 PDU-Type: [DataFW1_5] Op: [Response] Function: [SetVariable] …
[illegible]	[illegible]27.087691	10.65.96.89	10.65.60.73	COTP	61	DT TPDU (0) [COTP fragment, 0 bytes]
[illegible]	[illegible]27.157371	10.65.60.73	10.65.96.89	TCP	60	102→5208 [ACK] Seq=1221 Ack=1780 Win=8192 Len=0
1163	2017-02-24 13:37:27.246673	10.65.96.89	10.65.60.73	S7COMM-PLUS	149	→5208 PDU-Type: [DataFW1_5] Op: [Request] Function: [DeleteObject] …
1165	2017-02-24 13:37:27.251266	10.65.60.73	10.65.96.89	S7COMM-PLUS	121	→5208 PDU-Type: [DataFW1_5] Op: [Response] Function: [DeleteObject]…

TCP Connection

COTP Connection

S7CommPlus Connection

S7CommPlus Function

--Stop PLC

S7CommPlus Protocol

- The current S7CommPlus protocol including the S7CommPlus Connection packets and S7CommPlus Function packets has a similar structure.
- 1. First Connection Setup Request
  2. First Connection Setup Response
  3. Second Connection Setup Request
  4. Second Connection Setup Response

Session ID

Encryption length

Encryption Part

```
0030  f6 6c b1 a3 00 00 03 00  00 65 02 f0 80 72 03 00   .l...... .e...r..
0040  56 20 68 ad 71 74 34 cb  34 89 19 4d ae 03 0a d2   V h.qt4. 4..M....
0050  e6 f5 7c 5e c3 07 a9 89  a5 5d 31 b0 c2 23 42 80   ..|^.... .]1..#B.
0060  b8 fc 31 00 00 04 f2 00  00 00 0c 00 00 03 8f 34   ..      .......4
0070  00 00 00 34 01 90 77 00  08 01 00 00 04 e8 89 69   ...4..w. .......i
0080  00 12 00 00 00 00 89 6a  00 13 00 89 6b 00 04 00   .......j ....k...
0090  00 00 03 00 00 00 00 72  03 00 00                  .......r ...
```

Session ID

Type:Request

SubType:SetVariable

```
0120  f9 33 39 73 e7 ad 3f 7b  26 46 8f 4f 08 3b bb 22   .3fd..?{ &F.O.;.
0130  cb 10 c4 f0 42 48 1b f7  bc d5 a7 55 42 0a a0 5c   ....BH.. ...UB..\
0140  f7 ff 66 bf 3f 1d 4b 2d  52 b2 1a 87 4b 6e 2c 13   ..f.?.K- R...Kn,.
0150  4c 85 20 bf 55 9c 2d 7e  c8 01 ce 62 94 44 bd 8a   L. .U.-~ ...b.D..
0160  9d e1 7a 6f 74 e9 95 66  82 00 02 00 17 00 00 01   ..zot..f ........
0170  3a 82 3b 00 04 83 [illegible]                      :.;..... <.....=.
0180  04 84 80 c1 00 82 [illegible]                      ......>. ......?.
0190  15 00 82 40 00 15 1a 31  3b 36 45 53 37 20 32 31   ...@...1 ;6ES7 21
01a0  34 2d 31 41 47 34 30 2d  30 58 42 30 3b 56 34 2e   4-1AG40- 0XB0;V4.
01b0  30 82 41 00 03 00 03 00  00 00 00 04 e8 89 69 00   0.A..... ......i.
01c0  12 00 00 00 00 89 6a 00  13 00 89 6b 00 04 00 00   ......j. ...k....
01d0  00 00 00 00 72 02 00 00                            ....r...
```

Second Connection Encryption

Frame Boundary

S7CommPlus Protocol

- Session ID :

Session ID = Object ID+0x80

Object ID

```
80 72 01 00
02 87 0f 87
```

Session ID

```
0 00 03 00  01 a2 02 f0 80 72 0
5 42 00 00  00 02 00 00 03 8f 3
```

S7CommPlus Protocol

- Encryption Part :

1. The second connection packet has two encryptions

```
d6 8b 1b e                                  3e 67 2f 45   ....n.H. ..a.>g/E
f9 53 59 7                                  08 3b bb 22   .SYu..?{ &F.O.;."
cb 10 c4 f0 42 48 1b f7  bc d5 a7 55 42 0a a0 5c   ....BH.. ...UB..\
f7 ff 66 bf 3f 1d 4b 2d  52 b2 1a 87 4b 6e 2c 13   ..f.?.K- R...Kn,.
4c 85 20 bf 55 9c 2d 7e  c8 01 ce 62 94 44 bd 8a   L. .U.-~ ...b.D..
9d e1 7a 6f 74 e9 95 66  82 00 02 00 17 00 00 01   ..zot..f ........
3a 82 3b 00 04 83                                  :.;..... <.....=.
04 84 80 c1 00 82                                  ......>. ......?.
```

First Connection Encryption

Second Connection Encryption

2. The function packet has one encryption (Integrity Part)

Encryption length

Encryption Part

```
030  f6 6c b1 a3 00 00 03 00  00 65 02 f0 80 72 03 00   .l...... .e...r..
040  56 20 68 ad 71 74 34 cb  34 89 19 4d ae 03 0a d2   V h.qt4. 4..M....
050  e6 f5 7c 5e c3 07 a9 89  a5 5d 31 b0 c2 23 42 80   ..|^.... .]1..#B.
060  b8 fc 31 00 00 04 f2 00  00 00 0c 00 00 03 8f 34   ..      .......4
070  00 00 00 34 01 90 77 00  08 01 00 00 04 e8 89 69   ...4..w. ........i
```

Session ID

The Encryption

- Using reverse debugging techniques, we found these encryption is calculated by TIA Portal through a file named OMSp_core_managed.dll

1. Connection packet encryption

Input parameter for this encryption is a random value array generated by the PLC in the first connection response packet.

```
0070  15 10 4f 4d 53 50 2e 52  45 4c 2e 37 30 37 30 2e   ..OMSP.R EL.7070.
0080  31 34 a3 82 2f 10 02 14  1c 16 84 ed 01 be 4f fc   14../... ......O.
0090  2d dd 3c 34 d4 a1 83 aa  3b 61 56 03 a3 82 32 00   -.<4.... ;aV...2.
00a0  17 00 00 01 3a 82 [illegible] 3c 00 04 83   ....:.;. ..@.<...
00b0  00 82 3d 00 04 84 [illegible] 04 84 80 c1   ..=..... @.>.....
00c0  00 82 3f 00 15 1[illegible] 20 32 31 34   ..?...1; 6ES7 214
```

Connection Response Value Array

The Encryption

（1） First encryption in the connection packet

Using XOR (we call this Encryption1), the first encryption can be calculated with the input parameter Value Array.

Value Array → Encryption1 → First Encryption

```
0030  20 00 df 31 00 00 03 00  00 c5 02 f0 80 72 01 00   ..1.... .....r..
0040  b6 32 00 00 04 ca 00 00  00 01 36 00 02 87 53 87   .2...... ..6...S.
0050  4a a1 00 00 01 20
0060  30 31 a3 82 2b 00
0070  15 10 4f 4d 5
0080  31 34 a3 82 2f 10
0090  52 9f 99 47 90 1c
00a0  17 00 00 01 3a 82
00b0  00 82 3d 00 04 84
00c0
00d0
00e0
00f0
```

Valu

```
  *(_BYTE *)a1 = 1;
}
*(_DWORD *)(a1 + 572) += a3;
if ( *(_DWORD *)(a1 + 576) )
{
  if ( a3 + *(_DWORD *)(a1 + 576) < 0x10 )
  {
    v11 = a1 + *(_DWORD *)(a1 + 576) + 580;
    for ( i = 0; i < a3; ++i )
      *(_BYTE *)(i + v11) = *(_BYTE *)(i + a2);
    *(_DWORD *)(a1 + 576) += a3;
    return 0;
  }
  v9 = a1 + *(_DWORD *)(a1 + 576) + 580;
  for ( j = 0; j < 16 - *(_DWORD *)(a1 + 576); ++j )
    *(_BYTE *)(j + v9) = *(_BYTE *)(j + a2);
  sub_101DAA30(a1 + 556, (int)&v13, a1 + 20);
  sub_101DC810(a1 + 556);
  v13 ^= (*(_BYTE *)(a1 + 0x247) << 24) | (*(_BYTE *)(a1 + 0x246)
  v14 ^= (*(_BYTE *)(a1 + 587) << 24) | (*(_BYTE *)(a1 + 586) <<
  v15 ^= (*(_BYTE *)(a1 + 591) << 24) | (*(_BYTE *)(a1 + 590) <<
  v16 ^= (*(_BYTE *)(a1 + 595) << 24) | (*(_BYTE *)(a1 + 594) <<
  sub_101DA9A0((int)&v13, 4u, a4);
  a2 += 16 - *(_DWORD *)(a1 + 0x240);
  a4 += 16;
  v12 += 16;
```

Encrypti

```
0030  fa 08 b2 e0 00 00 03 00  01 a2 02 f0 80 72 02 01   ........ .....r..
0040  93 31 00 00 05 42 00 00  00 02 00 00 03 d3 34 00   .1...B.. ......4.
0050  00 03 d3 02 02 8e 26 82  32 01 00 17 00 00 07 08   ......&. 2.......
0060  8e 09 00 04 00 8e 0a 00  02 00 8e 0b 00 17 00 00   ........ ........
0070  07 21 8e                                            ...
0080  23 00 04                                            ...
0090  00 00 07                                            ...
00a0  ec 8e 23                                            ...
00b0  00 14 00                                            ...
00c0  00 01 00                                            ...
00d0  00 00 00                                            ...
00e0  00 00 00                                            .o.
00f0  bf fa d9                                            ...
0100  60 55 35                                            ...
0110  d6 8b 1b e5                                 61 9b 3e 67 2f 45   ....n.H. ..a.>g/E
0120  f9 53 59 75 e7 ad 3f 7b  2b 4b 8f 4f 08 3b bb 22   .SYu..?{ &F.O.;."
0130  cb e4 f6 25 ff 6b 16 88  fe 70 d4 11 ff 59 c0 cb   ...%.k.. .p...Y..
0140  f5 ff 66 bf 3f 1d 4b 2d  52 b2 1a 87 4b 6e 2c 13   ..f.?.K- R...Kn,.
```

```
OMSp_core_managed+0x1dd056:
182cd056 83c40c          add     esp,0Ch
0:024:x86> dd 1913703c
1913703c  ff25f6e4 fe88166b ff11d470 f5cbc052
1913704c  00000000 00000000 00000000 00000000
1913705c  00000000 00000000 00000000 00000000
1913706c  00000000 00000000 00000000 6b7a1837
1913707c  80000000 006f020f 0075006d 0069006e
1913708c  00610063 0069007a 006e006f 003a0065
1913709c  00540020 00610072 0073006e 007a0061
191370ac  006f0069 0065006e 00440020 00540050
0:024:x86>
```

First Encryption

Calculated using Windbg

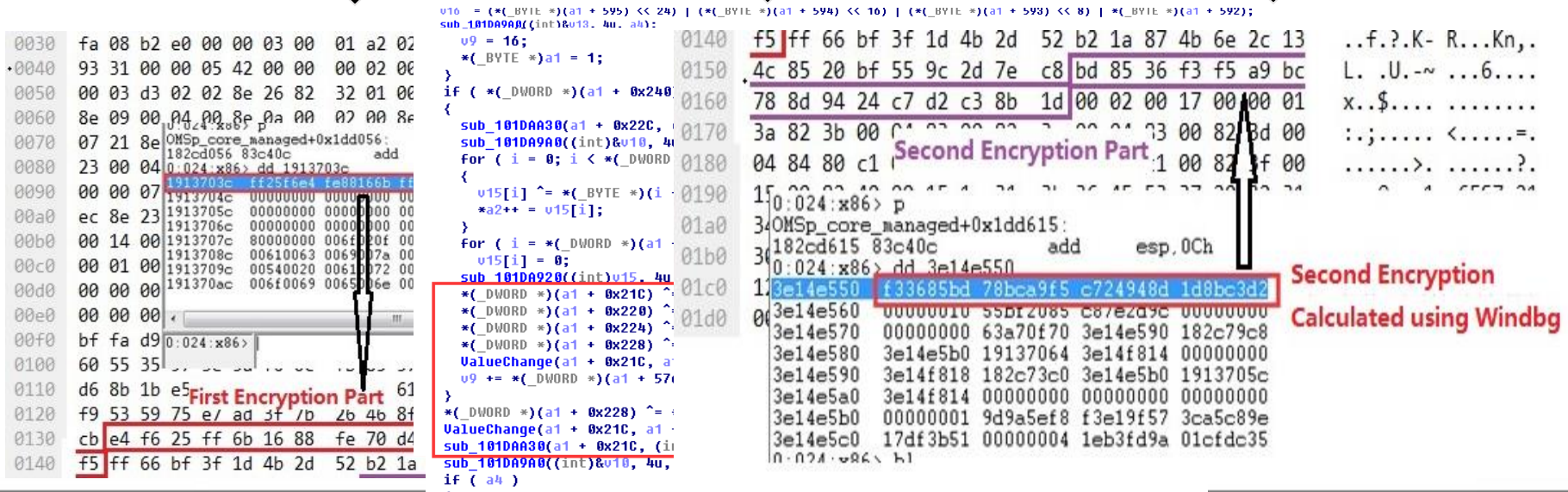
First Encryption Part

The Encryption

（2） Second encryption in the connection packet

Using the result of the first encryption as input parameter, the second encryption is calculated through a more complex Siemens-private algorithm.

First Encryption → Encryption2 → Second Encryption

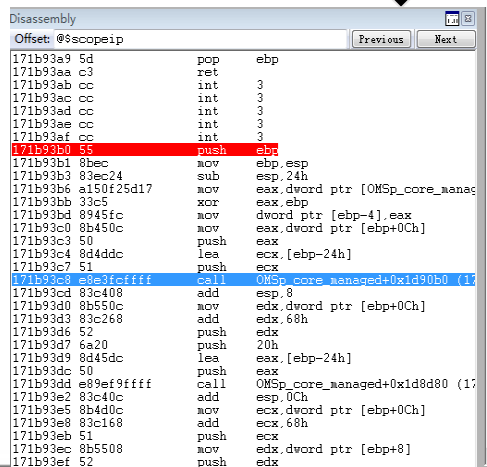


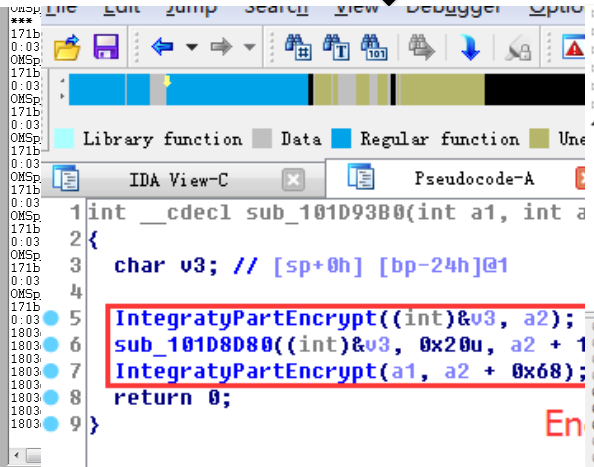
The Encryption

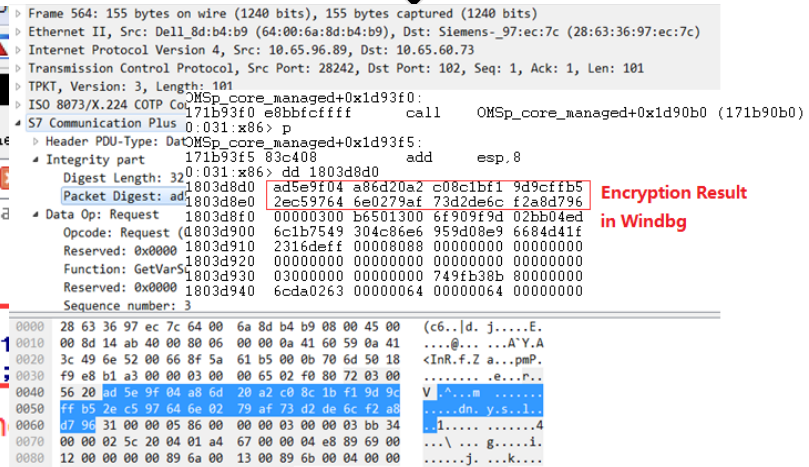
2. Function packet encryption

A fixed field array with Session ID is the input parameter. A complex algorithm (we call this Encryption3) is used to calculated the encryption result as follow:

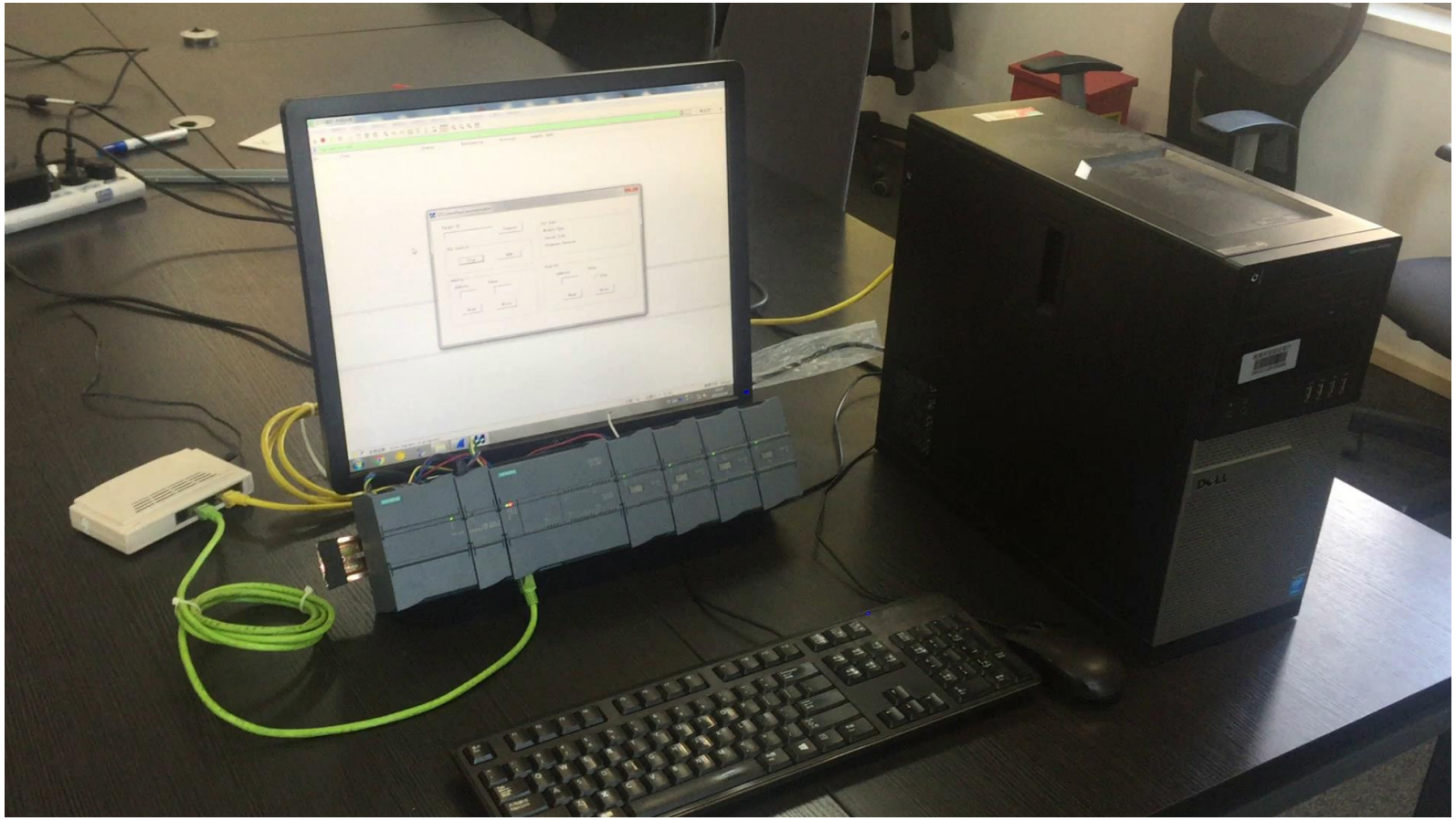
Constant Array (with Session ID) → Encryption3 → Function Encryption





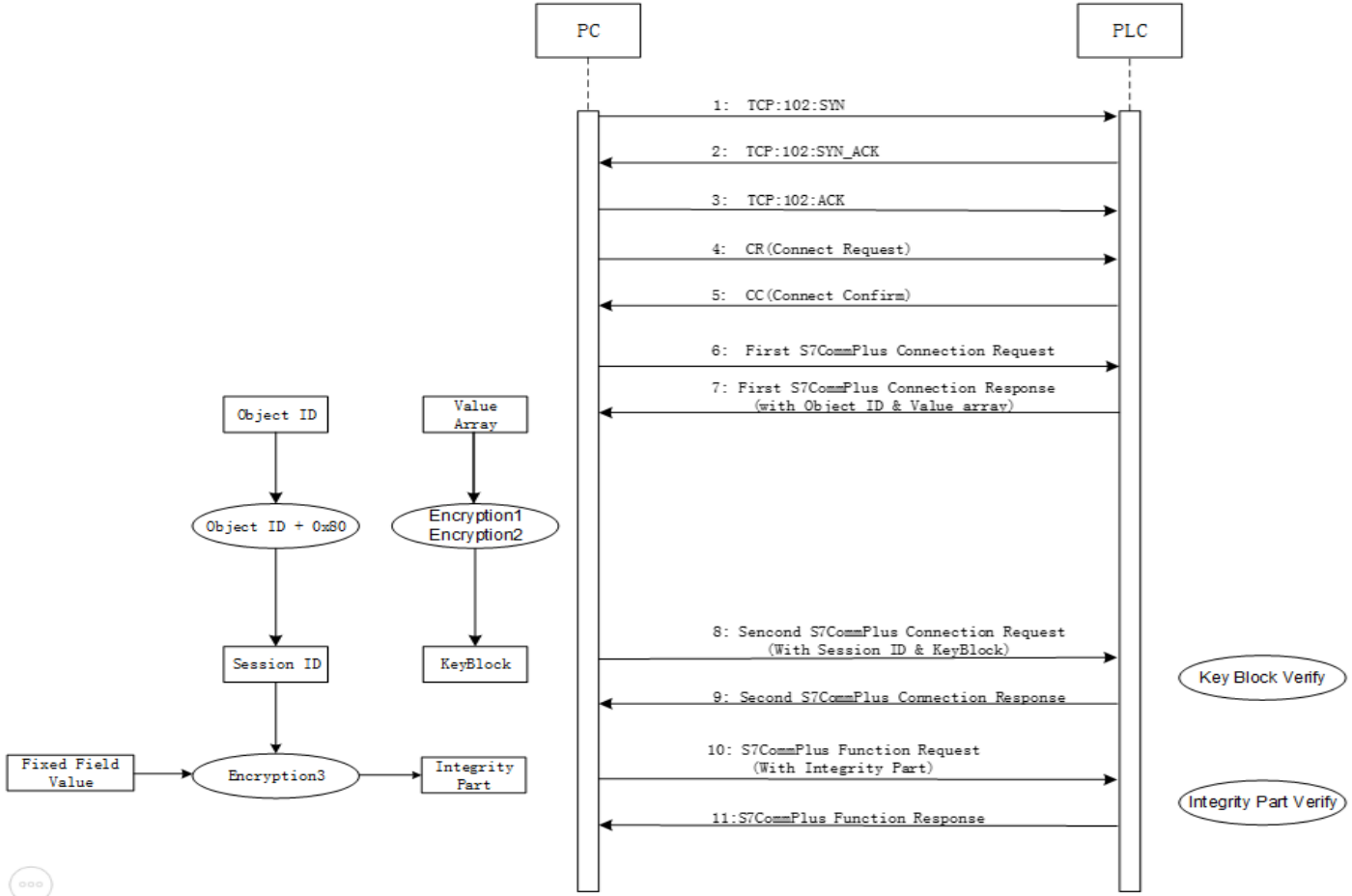


Demonstration



The Encryption

3. S7CommPlus Communication with Encryption



Protections

Code level:

-- Use code confusion techniques and anti-Debug techniques for the key DLL files

Design level

-- use a private key as an input parameter for encryption algorithm in the communication between Siemens software and PLCs.

Protocol level

-- Encrypt the whole packets instead of the key byte encryption

Thank You!

chengleim19@gmail.com