The spear to break the security wall of S7CommPlus

CHENG LEI, NSFOCUS
Related Work

- Dillon Beresford. Exploiting Siemens Simatic S7 PLCs. Black Hat 2011 USA.
  S7Comm protocol

- Ralf Spenneberg et. al.
  PLC-Blaster: A Worm Living Solely in the PLC. Black Hat 2016 USA
  Early S7CommPlus protocol

- This talk mainly focuses on the current encrypted S7CommPlus protocol
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.
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. Function Packet — Stop PLC
S7CommPlus Protocol

• Session ID:

Session ID = Object ID + 0x80
S7CommPlus Protocol

• Encryption Part:

1. The second connection packet has two encryptions:

```
| d6 8b 1b e1 | 3e 67 2f 45 |
| f9 53 59 7b | ea 31 7b 0a |
| cb 10 c4 f0 | 42 48 1b f7 |
| bc d5 a7 55 | 42 0a a0 5c |
| f7 ff 66 bf | 3f 1d 4b 2d |
| 52 b2 1a 87 | 4b 6e 2c 13 |
| 4c 85 20 bf | 55 9c 2d 7e |
| c8 01 ce 62 | 94 44 bd 8a |
| 9d e1 7a 6f | 74 e9 95 66 |
| 82 00 02 00 | 17 00 00 01 |
| 3a 82 3b 00 | 04 83 00 00 |
| 04 84 80 c1 | 00 82 00 00 |
```

```
| f6 6c b1 a3 | 00 00 03 00 |
| 00 65 02 f0 | 80 72 03 00 |
| 56 20 68 ad | 71 74 34 cb |
| 34 89 19 4d | ae 03 0a d2 |
| e6 f5 7c 5e | c3 07 a9 89 |
| a5 5d 31 b0 | c2 23 42 80 |
| b8 fc 31 00 | 00 04 f2 00 |
| 00 00 0c 00 | 00 00 03 8f |
```

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

```c
+(BYTE +) = 1;

+DWORD +) = (a1 + 572) + a3;
if ( +DWORD +) = (a1 + 576)
{
    if ( = DWORD +) = (a1 + 576) 0x10
    
    at + +DWORD +) = (a1 + 576) + 580;
for ( = +) = +add +)
    +BYTE +) = = +BYTE +) = +add +);
    return 0;
}

= +DWORD +) = (a1 + 576) + 580;
for ( = 0; = +add +)
    +BYTE +) = = +BYTE +) = +add +);
    return 0;
}

= +DWORD +) = (a1 + 576) + 580;
for ( = 0; = +add +)
    +BYTE +) = = +BYTE +) = +add +);
    return 0;
}
```
Fun with 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
Fun with 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:

\[
\text{ConstanArray} + \text{Encryption3} = \text{Function Encryption (with Session ID)}
\]
Fun with 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