The spear to break the security wall of S7CommPlus

CHENG LEI, NSFOCUS
Overview

- PLC and Siemens PLC introduction

- 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

<table>
<thead>
<tr>
<th>PLC Model</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>S7-300</td>
<td>• S7-200, S7-300, S7-400 using the S7Comm protocol</td>
</tr>
<tr>
<td>S7-1200</td>
<td>• S7-1200v3.0 using the early S7CommPlus protocol</td>
</tr>
<tr>
<td>S7-1500</td>
<td>• S7-1200v4.0, S7-1500 using the current encrypted S7CommPlus protocol</td>
</tr>
</tbody>
</table>
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

   First Connection Encryption

   3e 67 2f 45 3a 60 2b 2e 61 6f 62 65 6d
   6f 72 61 64 69 6e 67 74 7d

   Second Connection Encryption

   e1 7a 6f 74 95 66 82 00 02 00 17 00 01

2. The function packet has one encryption (Integrity Part)
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.
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.
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.
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 calculate the encryption result as follows:

Constant Array ➔ Encryption3 ➔ Function 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 ➔ Encryption3 ➔ Function Encryption
Demonstration
The Encryption

3. S7CommPlus Communication with Encryption

Object ID → Value Array

Object ID + 0x80 → Encryption1 → Encryption2

Session ID → KeyBlock

Fixed Field Value → Encryption3

Integrity Part

1: TCP:102:SYN
2: TCP:102:SYN_ACK
3: TCP:102:ACK
4: CR (Connect Request)
5: CC (Connect Confirm)
6: First S7CommPlus Connection Request
7: First S7CommPlus Connection Response (with Object ID & Value array)
8: Second S7CommPlus Connection Request (with Session ID & KeyBlock)
9: Second S7CommPlus Connection Response
10: S7CommPlus Function Request (with Integrity Part)
11: S7CommPlus Function Response

Key Block Verify

Integrity Part Verify
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