

ISC 2019 第七届互联网安全大会

# 泰坦之剑-潜析针对工控设备的攻击方法

程擂

信联智控科技首席安全专家

小鹅助理



扫码添加小鹅助理，与数万科技圈人士  
分享重量级活动PPT、干货培训课程、高端会议免费  
门票



第七届中国信息安全大会

# 泰坦之剑— 潜析针对工控设备的攻击方法

程播

信联智控科技有限公司

首席安全专家



## 关于信联智控

北京信联智控科技有限公司成立于2018年6月，总部位于北京，致力于工业信息安全领域的创新型高科技公司，目前设有北京总部和西安研发中心。

公司的创始团队是由业界资深的领域专家和商业精英组成，同时拥有一批具有具有多年从业经验和技術底蘊深厚的技術專家。

我們的願景是為工業環境保駕護航，為行業用戶提供安全穩定的網絡環境，為員工提供持續學習和良好職業發展的平台。



## 关于我

信联智控首席科学家，5年DCS软件研发与技术支持，3年工控安全研究

Xpwn2016 西门子设备破解

Blackhat2017、Defcon2017演讲者—The spear to break the security wall of S7commPlus

CS3 2018演讲者— Attacking PLCs by PLC in deep

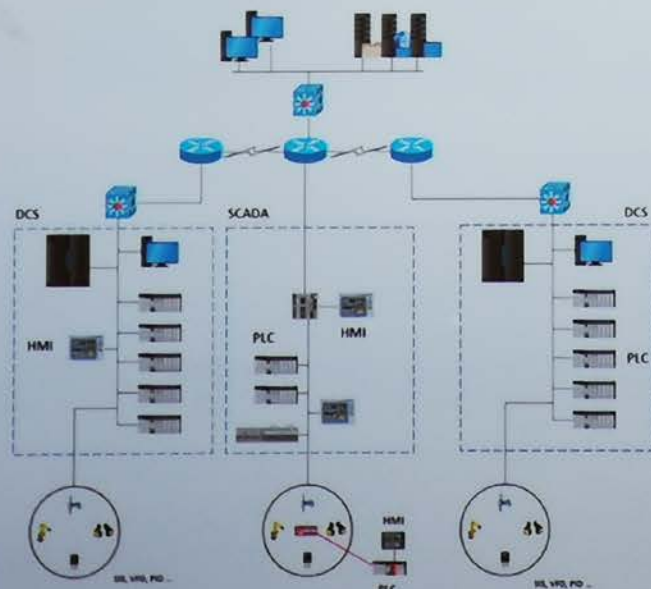






第七届中国安全大会

## 工业控制系统



PLC：可编程逻辑控制器

DCS：分布式控制系统

SCADA：数据采集与监视控制系统

SIS：安全仪表系统





第七十届国际信息安全大会

## 工业控制系统面临的安全问题

### 工业工控系统自身安全脆弱性



工业控制系统协议缺乏足够的安全性考虑，易被攻击者利用



严重漏洞难以及时处理，系统安全风险巨大



缺乏违规操作、越权访问行为审计能力



面对新型的APT攻击，缺乏有效的应对措施



### 泰坦之剑

1. 利用工业协议攻击
2. 构造恶意代码攻击
3. 窃取机密数据
4. 获取控制权
5. 造成系统拒绝服务





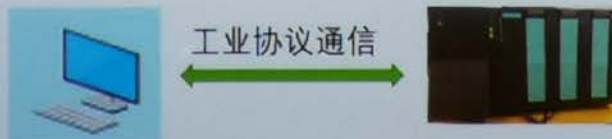
第七届中国网络安全大会

## 泰坦之剑属性一之工业协议攻击

工业控制设备通过工业协议进行监控，如下装、启动、停止、读值、写值等操作

由于工业控制系统协议缺乏足够的安全性考虑，易被攻击者利用

通过协议重放攻击，是最简便也最直接的针对工业控制设备的攻击手段







第七届中国网络安全大会

## 工业控制系统面临的安全问题

### 工业工控系统自身安全脆弱性



工业控制系统协议缺乏足够的安全性考虑，易被攻击者利用



严重漏洞难以及时处理，系统安全风险巨大



缺乏违规操作、越权访问行为审计能力



面对新型的APT攻击，缺乏有效的应对措施



### 泰坦之剑

- 1、利用工业协议攻击
- 2、构造恶意代码攻击
- 3、窃取机密数据
- 4、获取控制权
- 5、造成系统拒绝服务





## 泰坦之剑属性一之工业协议攻击 西门子PLC

### S7-300



- S7-300、S7-400系列采用S7Comm通信协议

### S7-1200



- S7-1200 V3.0以下版本使用早期的S7Comm-Plus通信协议

### S7-1500



- S7-1200 V3.0以上版本以及S7-1500采用最新的S7Comm-Plus通信协议



第七届中国网络安全大会

# 泰坦之剑属性一之工业协议攻击 西门子PLC

## S7CommPlus协议

No.	Time	Source	Destination	Protocol	Length	Info
1000	2017-02-24 13:37:26.264282	10.65.96.89	10.65.68.73	TCP	60	5200->102 [SYN] Seq=0 Win=0 Len=0 MSS=1460 WS=0 SACK_PERM=1
TCP Connection						60 102->5200 [SYN, ACK] Seq=0 Ack=1 Win=0 Len=0 MSS=1460
1022	2017-02-24 13:37:26.266509	10.65.96.89	10.65.68.73	TCP	54	5200->102 [ACK] Seq=1 Ack=1 Win=64240 Len=0
java net: 10.65.96.89:3726->10.65.68.73:5200						89 CR TPOU src-ref: 0x0001 dst-ref: 0x0000
COTP Connection						89 CC TPOU src-ref: 0x0001 dst-ref: 0x0001
1026	2017-02-24 13:37:26.276317	10.65.96.89	10.65.68.73	S7COMM-PLUS	289	+5200 PDU-Type: [Connect] Op: [Request] Function: [CreateObject] S-
1027	2017-02-24 13:37:26.286598	10.65.68.73	10.65.96.89	S7COMM-PLUS	251	+5200 PDU-Type: [Connect] Op: [Response] Function: [CreateObject] S-
S7CommPlus						61 DT TPOU (0) [COTP fragment, 0 bytes]
1036	2017-02-24 13:37:26.331976	10.65.96.89	10.65.68.73	S7COMM-PLUS	472	+5200 PDU-Type: [Data] Op: [Request] Function: [SetMultiVariables] -
1039	2017-02-24 13:37:26.360997	10.65.68.73	10.65.96.89	TCP	60	102->5200 [ACK] Seq=233 Ack=696 Win=8192 Len=0
1054	2017-02-24 13:37:26.459946	10.65.68.73	10.65.96.89	S7COMM-PLUS	86	-5200 PDU-Type: [Data] Op: [Response] Function: [SetMultiVariables] -
S7CommPlus						61 DT TPOU (0) [COTP fragment, 0 bytes]
1056	2017-02-24 13:37:26.468261	10.65.96.89	10.65.68.73	COTP	60	102->5200 [ACK] Seq=265 Ack=703 Win=8192 Len=0
1072	2017-02-24 13:37:26.556834	10.65.68.73	10.65.96.89	S7COMM-PLUS	155	+5200 PDU-Type: [DataFwd_S] Op: [Request] Function: [GetVarSubStrea-
1092	2017-02-24 13:37:26.693001	10.65.96.89	10.65.68.73	S7COMM-PLUS	129	+5200 PDU-Type: [DataFwd_S] Op: [Response] Function: [GetVarSubStrea-
1093	2017-02-24 13:37:26.697051	10.65.68.73	10.65.96.89	S7COMM-PLUS	61	DT TPOU (0) [COTP fragment, 0 bytes]
1094	2017-02-24 13:37:26.697967	10.65.96.89	10.65.68.73	COTP	155	+5200 PDU-Type: [DataFwd_S] Op: [Request] Function: [SetVariable] S-
1130	2017-02-24 13:37:27.081596	10.65.96.89	10.65.68.73	S7COMM-PLUS	118	+5200 PDU-Type: [DataFwd_S] Op: [Response] Function: [SetVariable] -
S7CommPlus Function						61 DT TPOU (0) [COTP fragment, 0 bytes]
-Stop PLC						60 102->5200 [ACK] Seq=1221 Ack=1780 Win=8192 Len=0
1163	2017-02-24 13:37:27.246673	10.65.96.89	10.65.68.73	S7COMM-PLUS	149	+5200 PDU-Type: [DataFwd_S] Op: [Request] Function: [DeleteObject] -
1165	2017-02-24 13:37:27.251260	10.65.68.73	10.65.96.89	S7COMM-PLUS	121	+5200 PDU-Type: [DataFwd_S] Op: [Response] Function: [DeleteObject] -



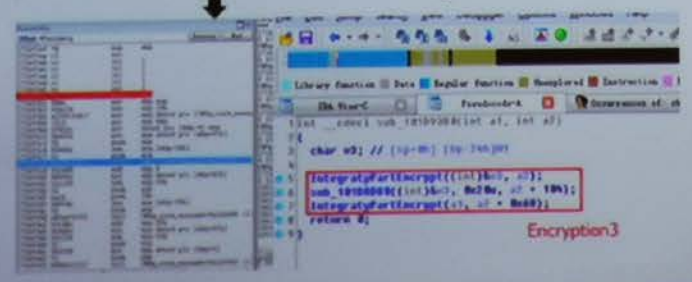
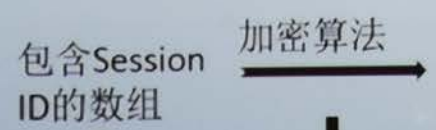


第七届中国网络安全大会

# 泰坦之剑属性一之工业协议攻击 西门子PLC

## S7CommPlus协议

一个包含Session ID的数组作为输入，通过西门子私有的加密算法，最终生成S7CommPlus中的加密部分





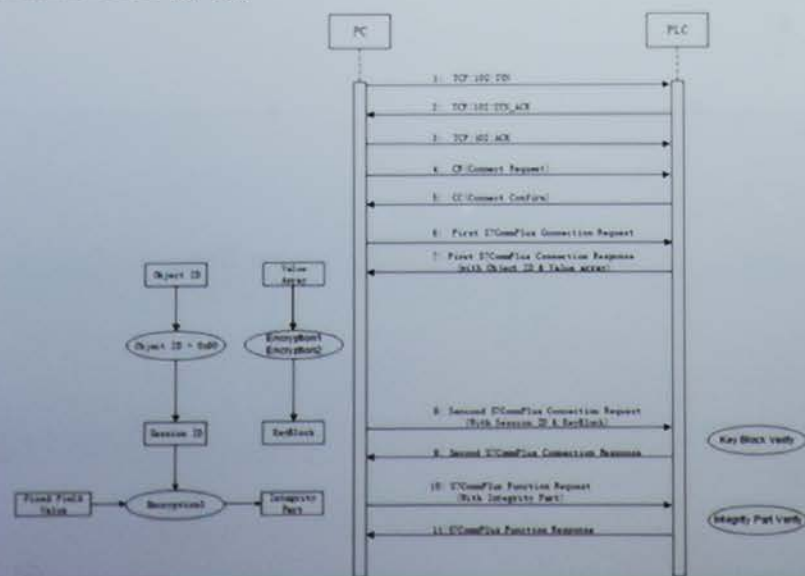


第七届中国网络安全大会

# 泰坦之剑属性一之工业协议攻击

## 西门子PLC

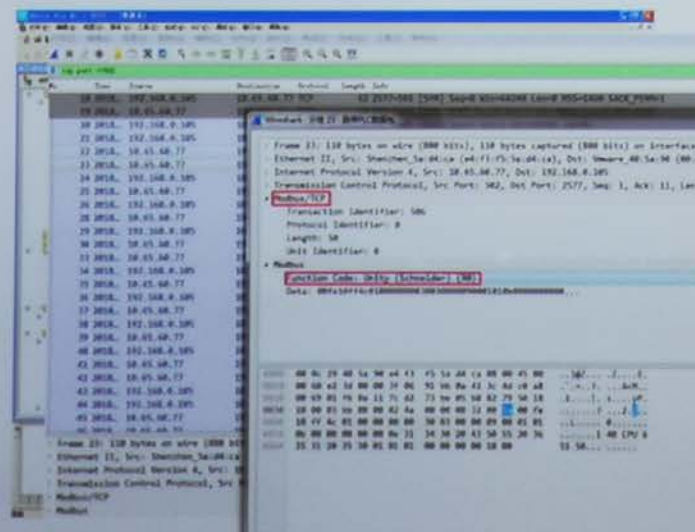
### S7CommPlus协议





第七届中国工控安全大会

## 泰坦之剑属性一之工业协议攻击 施耐德PLC



Unity Pro

ModBus/TCP

端口: 502

功能码: 90



第七届中国网络安全大会

## 泰坦之剑属性一之工业协议攻击 施耐德PLC

### 1. 获取Session ID

58	2018-01-05 10:30:04.077351	10.65.60.77	192.168.0.105	Modbus/TCP	1085 Response: Trans:	599; Unit: 0; Func: 90: Unity (Schneider)
59	2018-01-05 10:30:04.090915	192.168.0.105	10.65.60.77	Modbus/TCP	73 Query: Trans:	600; Unit: 0; Func: 90: Unity (Schneider)
61	2018-01-05 10:30:04.143871	10.65.60.77	192.168.0.105	Modbus/TCP	283 Response: Trans:	600; Unit: 0; Func: 90: Unity (Schneider)
62	2018-01-05 10:30:04.155349	192.168.0.105	10.65.60.77	Modbus/TCP	73 Query: Trans:	601; Unit: 0; Func: 90: Unity (Schneider)
63	2018-01-05 10:30:04.209992	10.65.60.77	192.168.0.105	Modbus/TCP	167 Response: Trans:	601; Unit: 0; Func: 90: Unity (Schneider)
64	2018-01-05 10:30:04.219750	192.168.0.105	10.65.60.77	Modbus/TCP	73 Query: Trans:	602; Unit: 0; Func: 90: Unity (Schneider)
65	2018-01-05 10:30:04.276737	10.65.60.77	192.168.0.105	Modbus/TCP	223 Response: Trans:	602; Unit: 0; Func: 90: Unity (Schneider)
66	2018-01-05 10:30:04.285534	192.168.0.105	10.65.60.77	Modbus/TCP	84 Query: Trans:	603; Unit: 0; Func: 90: Unity (Schneider)
68	2018-01-05 10:30:04.343571	10.65.60.77	192.168.0.105	Modbus/TCP	65 Response: Trans:	603; Unit: 0; Func: 90: Unity (Schneider)
69	2018-01-05 10:30:04.348725	192.168.0.105	10.65.60.77	Modbus/TCP	64 Query: Trans:	604; Unit: 0; Func: 90: Unity (Schneider)
70	2018-01-05 10:30:04.409923	10.65.60.77	192.168.0.105	Modbus/TCP	138 Response: Trans:	604; Unit: 0; Func: 90: Unity (Schneider)
71	2018-01-05 10:30:04.413263	192.168.0.105	10.65.60.77	Modbus/TCP	68 Query: Trans:	605; Unit: 0; Func: 90: Unity (Schneider)
72	2018-01-05 10:30:04.476851	10.65.60.77	192.168.0.105	Modbus/TCP	74 Response: Trans:	605; Unit: 0; Func: 90: Unity (Schneider)
73	2018-01-05 10:30:04.477771	192.168.0.105	10.65.60.77	Modbus/TCP	68 Query: Trans:	606; Unit: 0; Func: 90: Unity (Schneider)
75	2018-01-05 10:30:04.543543	10.65.60.77	192.168.0.105	Modbus/TCP	71 Response: Trans:	606; Unit: 0; Func: 90: Unity (Schneider)

#### Modbus

Function Code: Unity (Schneider) (90)

[Request Frame: 66]

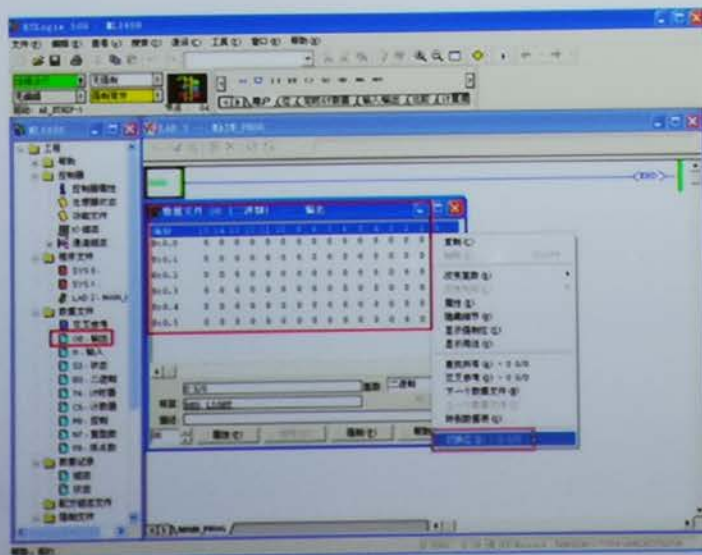
Data: 00f6df

```
0000 00 0c 29 40 5a 90 e4 f3 f5 5a d4 ca 08 00 45 00 ..)@Z... .Z....E.
0010 00 33 e2 55 00 00 3f 06 91 d0 0a 41 3c 4d c0 a8 .3.U..?. ...AcM..
0020 00 69 01 f6 0a 11 7c d2 05 6b 05 b8 8b 72 50 18 .1....|. .k...rP.
0030 10 00 15 fa 00 00 02 5b 00 00 00 05 00 5a 00 74 .....{ .....Z.
0040 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```





RSLogix







端口: 44818

212 2018.. 10.45.60.189	10.45.60.78 TCP	82 Register-Session (Req), Session: 0000000000
213 2018.. 10.45.60.189	10.45.60.78 TCP	82 Register-Session (Req), Session: 0000000000
214 2018.. 10.45.60.189	10.45.60.78 TCP	54 1000-04018 [ACK] Seq=1 Ack=1 Win=64248 len=0
217 2018.. 10.45.60.189	10.45.60.78 INDP	79 Unknown Command (0x0001) (Req)
218 2018.. 10.45.60.189	10.45.60.78 INDP	78 List Services (Req)
219 2018.. 10.45.60.189	10.45.60.78 INDP	79 List Interfaces (Req)
222 2018.. 10.45.60.78	10.45.60.1 INDP	100 Unknown Command (0x0001) (Exp)
234 2018.. 10.45.60.78	10.45.60.1 INDP	104 List Services (Req), Communications
235 2018.. 10.45.60.189	10.45.60.78 TCP	54 1000-04018 [ACK] Seq=7 Ack=17 Win=44124 len=0
236 2018.. 10.45.60.78	10.45.60.1 INDP	80 List Interfaces (Req)
237 2018.. 10.45.60.189	10.45.60.78 INDP	82 Register-Session (Req), Session: 0000000000
238 2018.. 10.45.60.78	10.45.60.1 INDP	82 Register-Session (Req), Session: 0000000000
239 2018.. 10.45.60.189	10.45.60.78 TCP	112 Class (Req?) - Service (Req?)
240 2018.. 10.45.60.78	10.45.60.1 TCP	134 Success: Class (Req?) - Service (Req?)
241 2018.. 10.45.60.189	10.45.60.78 TCP CH	104 Connection Manager - Forward Open (Message Router)
242 2018.. 10.45.60.189	10.45.60.1 TCP CH	124 Success: Connection Manager - Forward Open
243 2018.. 10.45.60.78	10.45.60.78 TCP	123 Class (Req?) - Service (Req?)
245 2018.. 10.45.60.78	10.45.60.1 TCP	150 Success: Class (Req?) - Service (Req?)
246 2018.. 10.45.60.78	10.45.60.78 TCP	123 Class (Req?) - Service (Req?)
247 2018.. 10.45.60.78	10.45.60.1 TCP	150 Success: Class (Req?) - Service (Req?)
248 2018.. 10.45.60.189	10.45.60.78 TCP	123 Class (Req?) - Service (Req?)
252 2018.. 10.45.60.78	10.45.60.78 TCP	139 Success: Class (Req?) - Service (Req?)
253 2018.. 10.45.60.189	10.45.60.78 TCP	123 Class (Req?) - Service (Req?)

```
Frame 218: 78 bytes on wire (624 bits), 78 bytes captured (624 bits) on interface 0
Ethernet II, Src: VMware_Fc:30:ac:00:00:29:Fc:30:ac, Dst: Ruckus11_97:a7:80 (f4:54:53:97:a7:80)
Internet Protocol Version 4, Src: 10.65.60.189, Dst: 10.65.60.78
Transmission Control Protocol, Src Port: 1889, Dst Port: 4433, Seq: 25, Ack: 1, Len: 24
Ethernet/IPv4 (Industrial Protocol), Session: 0000000000, List Services
```

[illegible]



### 1. EtherNet/IP 连接数据包

EtherNet/IP连接数据包如下图所示，包含4个ENIP数据包，其Command参数分别为0x0001(Unknown), 0x0004(ListServices), 0x0064(ListInterfaces) and 0x0065(Register Session)。在Register Session的响应数据包中，包含一个Session ID

[illegible][illegible][illegible]



第七届中国网络安全大会

# 泰坦之剑属性一之工业协议攻击

## 罗克韦尔 AB PLC

### 2. CIP 连接数据包





第七届中国网络安全大会

# 泰坦之剑属性一之工业协议攻击

## 罗克韦尔 AB PLC

### 2. CIP 连接数据包

每一个连接数据包都会使用CIP连接响应数据包中的O->T Network Connection ID 以及原始序列号，如下图中的红色框以及蓝色框，每一个连接数据包的 Sequence Count需满足递增，如下图绿色框所示

```
Frame 464: 123 bytes on wire (984 bits), 123 bytes captured (984 bits) on interface 0
Ethernet II, Src: Dell_Bd:b4:b9 (64:00:6a:b4:b9), Dst: Rockwell_97:e7:80 (f4:54:33:97:e7:80)
Internet Protocol Version 4, Src: 10.65.60.89, Dst: 10.65.60.78
Transmission Control Protocol, Src Port: 24455, Dst Port: 44818, Seq: 187, Ack: 241, Len: 69
Ethernet/IP (Industrial Protocol), Session: 0x3f36cfs, Send Unit Data
  Encapsulation Header
  Command Specific Data
    Interface Handle: CIP (0x00000000)
    Timeout: 1
  Item Count: 2
    Type ID: Connected Address Item (0x00a1)
      Length: 4
      Connection ID: 0x5dcdfed
    Type ID: Connected Data Item (0x00d1)
      Length: 25
      Sequence Count: 0x0001
      [Response ID: 0x0001]
  Common Industrial Protocol
  CIP Class Generic
    Command Specific Data
      Data: 074000034052c4f0034a9a22c00000000
000000  f4 54 33 97 e7 80 64 00 6a b4 b9 00 00 45 00  .f....d.....f.
000010  00 64 14 21 40 00 00 06 00 00 0a 41 3c 59 0a 41  .m. @... ..-BY.A
000020  3c 4a 5f 87 af 12 06 fd 91 6f 04 20 45 20 50 18  .M.....o..f.P.
000030  fa 00 8d 80 00 00 70 80 28 00 f5 6c f3 33 00 00  .....P.....l..
000040  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
000050  00 00 01 00 02 00 a1 00 04 00 2f 6c 73 b1 00 00  .....
000060  18 00 01 00 02 20 87 24 01 07 4d 00 01 40 85 00  .K. g $..M..g.
000070  0f 00 34 e9 a2 2c 00 00 00 00 00 00 00 00 00 00  .f.....
000080  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....
```





第七届中国网络安全大会

# 泰坦之剑属性一之工业协议攻击

## 罗克韦尔 AB PLC

### 3. 启动PLC数据包

```
Frame 2068: 119 bytes on wire (952 bits), 119 bytes captured (952 bits) on Interface 0
Ethernet II, Src: VMware_fc:36:ac (00:0c:29:fc:36:ac), Dst: Rockwell_97:a7:88 (14:54:33:97:a7:88)
Internet Protocol Version 4, Src: 10.65.60.189, Dst: 10.65.60.78
Transmission Control Protocol, Src Port: 1040, Dst Port: 64818, Seq: 22885, Ack: 26238, Len: 65
Ethernet/IP (Industrial Protocol), Session: 0xc07f575, Send Unit Data
+ Encapsulation Header
  Command: Send Unit Data (0x0070)
  Length: 41
  Session Handle: 0xc07f575
  Status: Success (0x00000000)
  Sender Context: 0000000000000000
  Options: 0x00000000
+ Command Specific Data
  Interface Handle: CIP (0x00000000)
  Timeout: 1
+ Item Count: 2
+ Type ID: Connected Address Item (0x00a1)
  Length: 4
  Connection ID: 0x10af6511
+ Type ID: Connected Data Item (0x00b1)
  Length: 21
  Sequence Count: 0x0055
  [Response.fc..26238]
+ Common Industrial Protocol
+ CIP Class Generic
+ Command Specific Data
  Data: 87a00d039a710c0e15028006
```

0000	14 54 33 97 a7 88 00 0c	29 fc 36 ac 00 00 45 00	..T.....6...f..
0010	00 09 02 71 40 00 80 06	6a d1 0a 41 1c bd 0a 41	..L.....j..d..A
0020	1c 4e 04 10 a7 12 7e 4e	1a ad 70 f4 f2 59 50 18	<.....x..VP
0030	fa 07 8a c1 00 00 70 00	29 00 75 e5 71 cd 00 00	.....D..U.....
0040	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	.....
0050	00 00 01 00 02 00 a1 00	04 00 51 fa e4 75 b1 00	.....0..W...
0060	15 00 ac 00 40 83 20 67	24 01 1c 00 00 17 00	...K..g \$..
0070	00 00 00 00 00 00 00 00		

启动PLC数据包如下图所示，红色框是CIP连接响应数据包中的O->T Network Connection ID，蓝色框是CIP连接响应数据包中的Originator Serial Number，绿色框为Sequence Count，黄色框代表功能码，“0x55, 0x01”表示该数据包是启动PLC的数据包



### 5. 写DO点值数据包

- Frame 1602: 127 bytes on wire (1016 bits), 127 bytes captured (1016 bits) on Interface 0
- Ethernet II, Src: VMware\_fc:36:a8:00:c0:29:f6:a6, Dst: Rockwell\_97:e7:b0:(f4:54:33:97:e7:b0)
- Internet Protocol Version 4, Src: 10.65.60.109, Dst: 10.65.60.78
- Transmission Control Protocol, Src Port: 1099, Dst Port: 44318, Seq: 11798, Ack: 1795142776, Len:  
- EtherNet/IP [Industrial Protocol], Session: bnt79c9e4, Send Unit Data
  - Encapsulation Header
- Command Specific Data
  - Interface Handle: IP {0x00000000}
  - Timeout: 1
- Item Count: 2
  - Type ID: Connected Address Item {0xb0a1}
    - Length: 4
    - Connection ID: bndc3d954
  - Type ID: Connected Data Item {0xb0b1}
    - Length: 29
    - Sequence Count: bndc3d4
- [Response In: 1605]
- Common Industrial Protocol
  - CIP Class Generic
    - Command Specific Data
      - Data: 07400000ca72c0000000baac0000200820000000000000

[illegible]

写DO点值数据包如下图所示，红色框是CIP连接响应数据包中的O->T Network Connection ID，蓝色框是CIP连接响应数据包中的Originator Serial Number，绿色框为Sequence Count，黄色框代表写DO点值功能码，紫色框为写点值的地址，橙色框为写点的值。





第七届中国网络安全大会

## 泰坦之剑属性一之工业协议攻击 某知名厂商DCS

The screenshot displays a network traffic analysis tool. The top pane shows a list of captured packets, with the selected packet (No. 453) highlighted. The bottom pane provides a detailed view of this packet, showing it is a UDP packet from 172.21.8.178 to 172.21.8.2 on port 12288. The packet length is 64 bytes. The bottom pane also shows a list of loaded protocols, including various industrial protocols like Modbus, OPC, and others.

No.	Time	Source	Destination	Protocol	Length	Info
453	25.242778	172.21.8.178	172.21.8.2	UDP	64	12545->12288 Len=32
455	25.271558	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
475	36.267511	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
488	36.382272	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
495	35.717936	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
499	35.835175	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
514	32.108954	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
538	32.158158	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
576	33.544938	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
578	33.544481	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
579	34.194821	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28
578	34.057964	172.21.8.178	172.21.8.2	UDP	58	12545->12288 Len=28

UDP通信

私有协议

端口: 12288



信息安全等级保护

## 泰坦之剑属性一之工业协议攻击

### 某知名厂商DCS

No.	Time	Source	Destination	Protocol	Length	Info
52	5.540601	172.21.0.178	224.0.0.252	LLMNR	66	Standard query 0x88aa A is...
64	3.743528	172.21.0.178	172.21.255.255	NBNS	92	Name query NB [SATAP<00>
68	4.507615	172.21.0.178	172.21.255.255	NBNS	92	Name query NB [SATAP<00>
84	5.271998	172.21.0.178	172.21.255.255	NBNS	92	Name query NB [SATAP<00>
96	5.787215	172.21.0.178	172.21.255.255	NBNS	92	Name query NB TX-TEST1-PC<
97	5.788343	172.21.0.129	172.21.0.178	NBNS	116	Name query response NB 172...
193	12.445805	172.21.0.178	172.21.0.2	UDP	64	12547-12288 Len=22
192	12.445806	172.21.0.178	172.21.0.3	UDP	64	12547-12288 Len=22
193	12.447753	172.21.0.3	172.21.0.178	UDP	576	12288-12547 Len=534
194	12.450174	172.21.0.2	172.21.0.178	UDP	576	12288-12547 Len=534
208	13.446384	172.21.0.178	172.21.0.2	UDP	318	12547-12288 Len=268
209	13.446886	172.21.0.178	172.21.0.3	UDP	318	12547-12288 Len=268
218	13.542879	172.21.0.2	172.21.0.178	UDP	642	12288-12547 Len=620
224	14.468285	172.21.0.178	172.21.0.2	UDP	318	12547-12288 Len=268
225	14.468781	172.21.0.178	172.21.0.3	UDP	318	12547-12288 Len=268
226	14.548934	172.21.0.2	172.21.0.178	UDP	642	12288-12547 Len=620
245	15.474273	172.21.0.178	172.21.0.2	UDP	318	12547-12288 Len=268
246	15.474758	172.21.0.178	172.21.0.3	UDP	318	12547-12288 Len=268
247	15.542997	172.21.0.2	172.21.0.178	UDP	642	12288-12547 Len=620
262	16.487708	172.21.0.178	172.21.0.2	UDP	78	12547-12288 Len=28
263	16.487825	172.21.0.178	172.21.0.3	UDP	78	12547-12288 Len=28





第七届中国网络安全大会

## 泰坦之剑属性一之工业协议攻击

### 某知名厂商DCS





第七届中国网络安全大会

## 泰坦之剑属性一之工业协议攻击 某知名厂商DCS



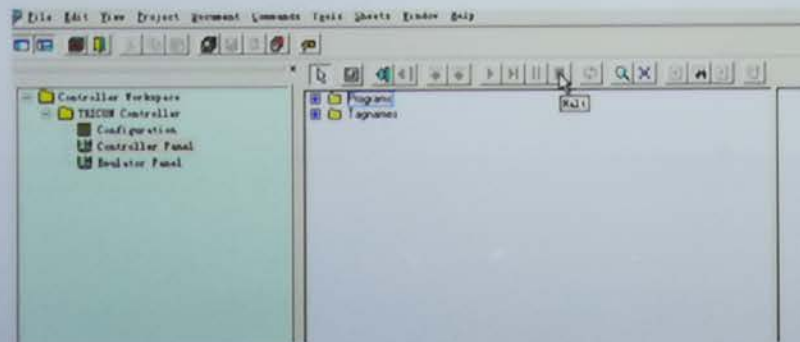
The screenshot shows a software interface for a Distributed Control System (DCS). On the left is a tree view of the system hierarchy. The main area displays a table of control loops. A context menu is open over the row for 'x10', showing options like '编辑...' (Edit), '启动' (Start), and '停止' (Stop).

名称	运行状态	输入关闭状态	输出关闭状态	运行时间(毫秒)
x77	运行	数活	数活	0.050
x11	停止	数活	数活	0.006
x10	运行	数活	数活	0.005
x1c	运行	数活	数活	0.011
x1c	运行	数活	数活	0.124
x11	运行	数活	数活	0.652
x10	运行	数活	数活	0.674
x11	运行	数活	数活	0.603
x12	运行	数活	数活	0.581
x13	运行	数活	数活	0.595
x14	运行	数活	数活	0.581
x15	运行	数活	数活	0.593
x16	运行	数活	数活	0.595



第七届中国工控安全大会

## 泰坦之剑属性一之工业协议攻击 某知名厂商SIS系统



UDP通信

私有协议

端口: 1502





第七届中国网络安全大会

# 泰坦之剑属性一之工业协议攻击

## 某知名厂商SIS系统

### 1. 停止控制器数据包

No.	Time	Source	Destination	Protocol	Length	Info
1	2018-	192.168.0.10	192.168.0.1	UDP	48	50218→1502 Len=6
2	2018-	192.168.0.1	192.168.0.10	UDP	60	1502→50218 Len=6
3	2018-	192.168.0.10	192.168.0.1	UDP	58	50218→1502 Len=16
4	2018-	192.168.0.1	192.168.0.10	UDP	60	1502→50218 Len=16
5	2018-	192.168.0.10	192.168.0.1	UDP	60	50218→1502 Len=18
6	2018-	192.168.0.1	192.168.0.10	UDP	60	1502→50218 Len=18
7	2018-	192.168.0.10	192.168.0.1	UDP	58	50218→1502 Len=16

Frame 3: 58 bytes on wire (464 bits), 58 bytes captured (464 bits) on interface 0

Ethernet II, Src: Dell\_eb:2f:fd (14:fe:b5:eb:2f:fd), Dst: 40:00:00:00:1e:01 (40:00:00:00:1e:01)

Internet Protocol Version 4, Src: 192.168.0.10, Dst: 192.168.0.1

User Datagram Protocol, Src Port: 50218, Dst Port: 1502

Data (16 bytes)

Data: 05000a0000001507000030000a00a34e

0000	40 00 00 00 1e 01 14 fe	b5 eb 2f fd 08 00 45 00	@..... ./...E.
0010	00 2c 09 bc 00 00 80 11	00 00 c0 a8 00 0a c0 a8	.....
0020	00 01 c4 2a 05 de 00 18	81 85 05 00 0a 00 00 00	...*....
0030	15 00 00 00 00 0a 00 a3 4e		...0...!

序号 Session CRC校验



第七届中国网络安全大会

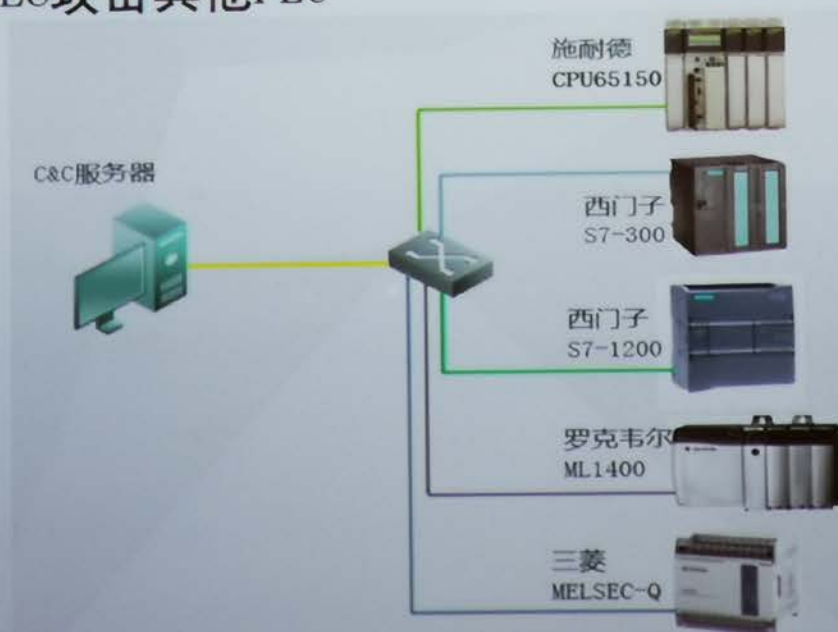
## 泰坦之剑属性一之工业协议攻击 某知名厂商SIS系统

```
data:10320845 align 4
data:10320846 dd offset aWorkfileUtilbdr : "@(*) $workfile: UTILITY.CPP $Revision: 1.2 $ModTime: 9"
data:10320847 off_1032084C dd offset aTriconexIsThew : DATA_XREF: BDR_verifyPassword(char const *,char const *)e
data:10320848 ; BDR_verifyPassword(char const *,char const *)e
data:10320849 ; "TRICONEX is the world leader."
data:10320850 dword_10320850 dd 1 ; DATA_XREF: sub_1020F200
data:10320851 ; sub_1020F200
data:10320852 dword_10320854 dd 1 ; DATA_XREF: sub_1020F200
data:10320853 ; sub_1020F200
data:10320854 aTriconexIsThew db "x is the world leader.",0 ; DATA_XREF: sub_1020F200
data:10320855 ; DATA_XREF: sub_1020F200
data:10320856 align 4
data:10320857 aWorkfileUtilbdr db "@(*) $workfile: UTILITY.CPP $Revision: 1.2 $ModTime: 9"
data:10320858 ; DATA_XREF: sub_1020F200
data:10320859 db "eb 25 2000 10:48:46 $",0
data:1032085A ; char aHex_R[]
data:1032085B aHex_0 db "0000",0 ; DATA_XREF: BDR_CreateSessionID(void)+1879
data:1032085C align 4
```



第七届中国工控安全大会

## 泰坦之剑属性二之恶意代码攻击 通过PLC攻击其他PLC

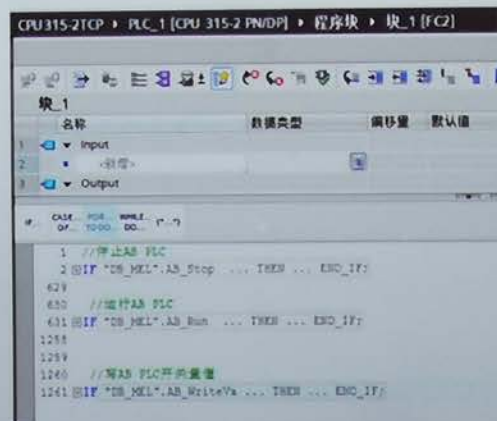
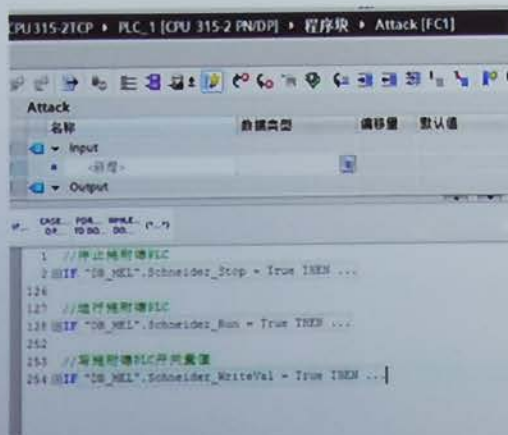






第七版工控网络安全大会

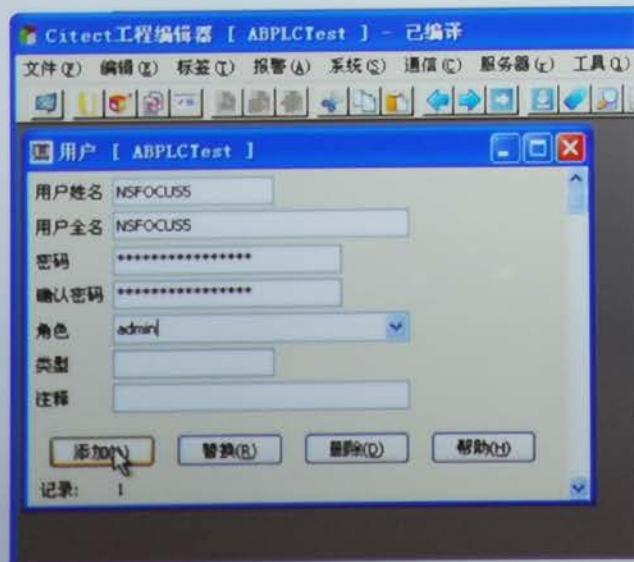
## 泰坦之剑属性二之恶意代码攻击 通过PLC攻击其他PLC





第七届中国国际信息安全大会

## 泰坦之剑属性三之窃取机密数据 Citect SCADA工程密码破译





## 泰坦之剑属性三之窃取机密数据 Citect SCADA工程密码破译

使用动态、静态调试分析，找到Citect软件密码计算的代码，位于CtUtil32.dll中

[illegible]

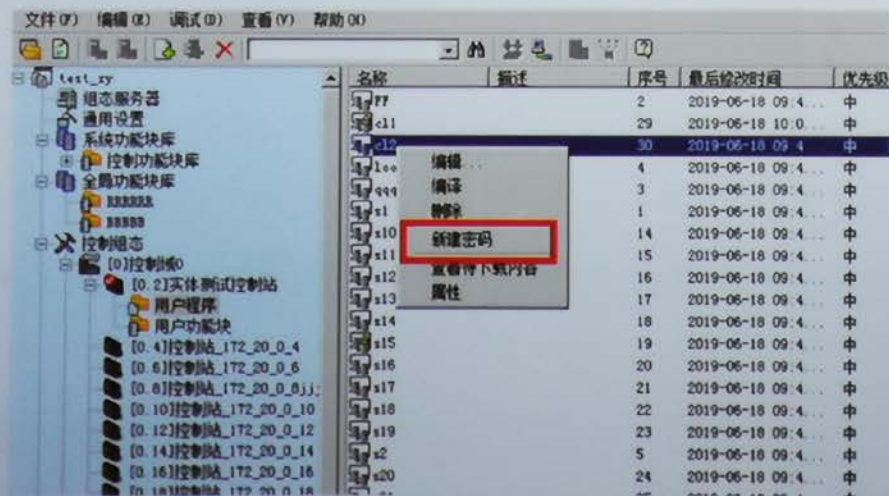




第七届中国国际信息安全大会

## 泰坦之剑属性三之窃取机密数据 某DCS软件控制器程序密码破译

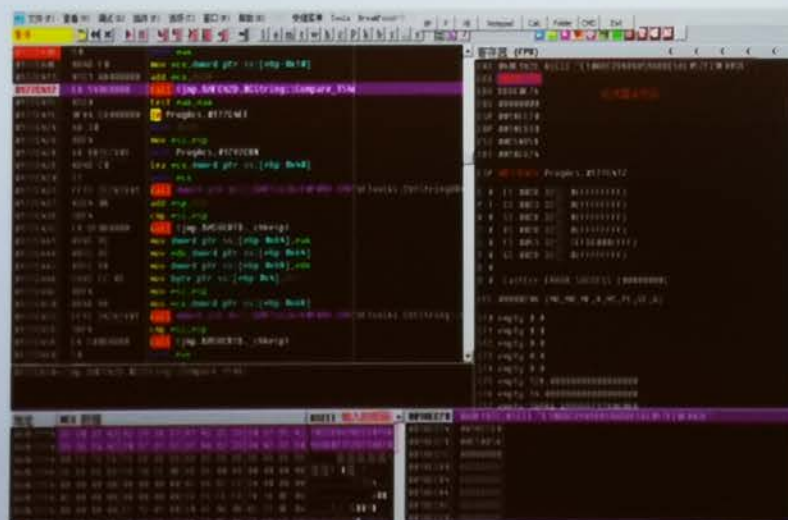
该系统控制器程序可以进行加密，对于加密的程序，需输入正确密码方可看到程序逻辑





通过逆向调试，发现程序进行密码对比时，使用密文对比，另外其加密算法比较复杂

通过逆向调试，发现程序进行密码对比时，使用密文对比，另外其加密算法比较复杂

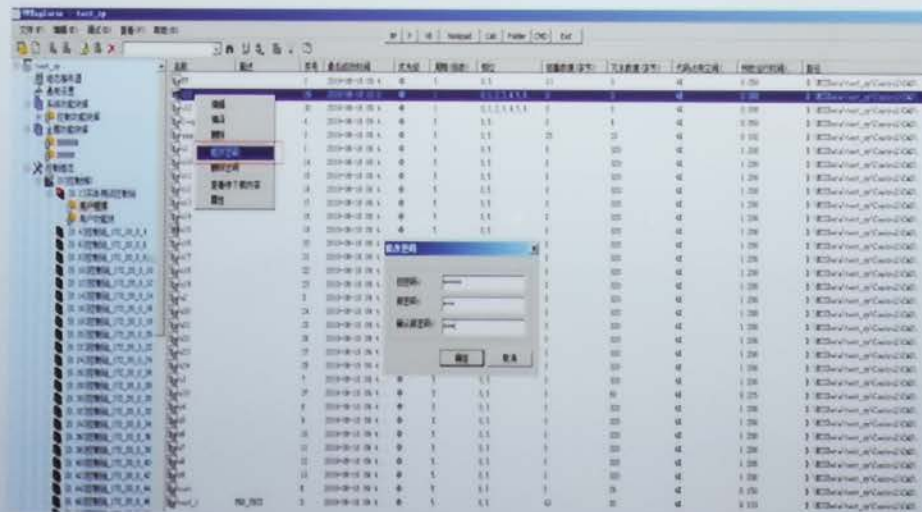




第七届中国信息安全大会

## 泰坦之剑属性三之窃取机密数据 某DCS软件控制器程序密码破译

继续研究发现对于已加密的程序可以进行密码修改，如下图所示







# 某DCS软件控制器程序密码破译

Address	Disassembly	Comment	Hex Dump
00401000	JMP EBX		
00401001	CALL EBX		
00401002	CALL EBX		
00401003	CALL EBX		
00401004	CALL EBX		
00401005	CALL EBX		
00401006	CALL EBX		
00401007	CALL EBX		
00401008	CALL EBX		
00401009	CALL EBX		
0040100A	CALL EBX		
0040100B	CALL EBX		
0040100C	CALL EBX		
0040100D	CALL EBX		
0040100E	CALL EBX		
0040100F	CALL EBX		
00401010	CALL EBX		
00401011	CALL EBX		
00401012	CALL EBX		
00401013	CALL EBX		
00401014	CALL EBX		
00401015	CALL EBX		
00401016	CALL EBX		
00401017	CALL EBX		
00401018	CALL EBX		
00401019	CALL EBX		
0040101A	CALL EBX		
0040101B	CALL EBX		
0040101C	CALL EBX		
0040101D	CALL EBX		
0040101E	CALL EBX		
0040101F	CALL EBX		
00401020	CALL EBX		
00401021	CALL EBX		
00401022	CALL EBX		
00401023	CALL EBX		
00401024	CALL EBX		
00401025	CALL EBX		
00401026	CALL EBX		
00401027	CALL EBX		
00401028	CALL EBX		
00401029	CALL EBX		
0040102A	CALL EBX		
0040102B	CALL EBX		
0040102C	CALL EBX		
0040102D	CALL EBX		
0040102E	CALL EBX		
0040102F	CALL EBX		
00401030	CALL EBX		
00401031	CALL EBX		
00401032	CALL EBX		
00401033	CALL EBX		
00401034	CALL EBX		
00401035	CALL EBX		
00401036	CALL EBX		
00401037	CALL EBX		
00401038	CALL EBX		
00401039	CALL EBX		
0040103A	CALL EBX		
0040103B	CALL EBX		
0040103C	CALL EBX		
0040103D	CALL EBX		
0040103E	CALL EBX		
0040103F	CALL EBX		
00401040	CALL EBX		
00401041	CALL EBX		
00401042	CALL EBX		
00401043	CALL EBX		
00401044	CALL EBX		
00401045	CALL EBX		
00401046	CALL EBX		
00401047	CALL EBX		
00401048	CALL EBX		
00401049	CALL EBX		
0040104A	CALL EBX		
0040104B	CALL EBX		
0040104C	CALL EBX		
0040104D	CALL EBX		
0040104E	CALL EBX		
0040104F	CALL EBX		
00401050	CALL EBX		
00401051	CALL EBX		
00401052	CALL EBX		
00401053	CALL EBX		
00401054	CALL EBX		
00401055	CALL EBX		
00401056	CALL EBX		
00401057	CALL EBX		
00401058	CALL EBX		
00401059	CALL EBX		
0040105A	CALL EBX		
0040105B	CALL EBX		
0040105C	CALL EBX		
0040105D	CALL EBX		
0040105E	CALL EBX		
0040105F	CALL EBX		
00401060	CALL EBX		
00401061	CALL EBX		
00401062	CALL EBX		
00401063	CALL EBX		
00401064	CALL EBX		
00401065	CALL EBX		
00401066	CALL EBX		
00401067	CALL EBX		
00401068	CALL EBX		
00401069	CALL EBX		
0040106A	CALL EBX		
0040106B	CALL EBX		
0040106C	CALL EBX		
0040106D	CALL EBX		
0040106E	CALL EBX		
0040106F	CALL EBX		
00401070	CALL EBX		
00401071	CALL EBX		
00401072	CALL EBX		
00401073	CALL EBX		
00401074	CALL EBX		
00401075	CALL EBX		



第七届中国国际工控展

## 泰坦之剑属性四之获取控制权 西门子PLC通信密码破解

西门子PLC可以通过设置私钥密码，来对设备进行安全保护，即Protection Level，如图1所示。当在组态程序设置Protection Level密码后，PLC设备具备读写保护权限，即每次修改寄存器值、下装程序、启动/停止PLC时都需要输入密码，只有密码验证成功后才会继续其操作

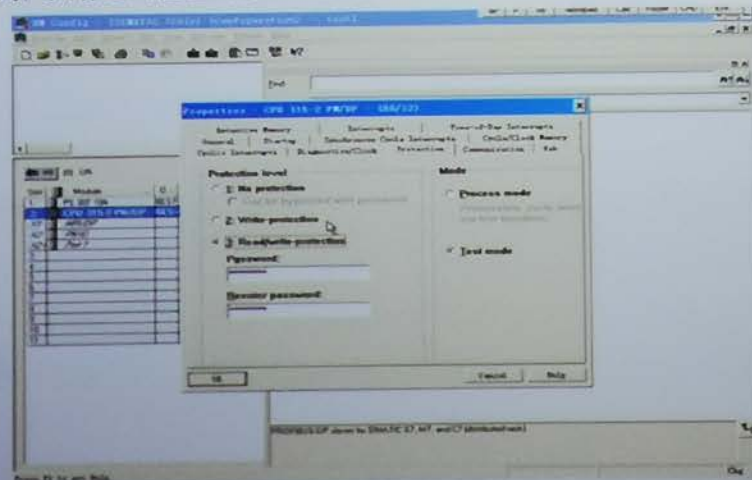




圖 4 臺灣地區 2000 年之人口密度

## 泰坦之剑属性四之获取控制权

# 西门子PLC通信密码破解

计算完成后, 该密码存储于

工程文件夹中\hOmSave7\S7HK31AX\HATTRME1.DBT文件中,如下图所示

[illegible]



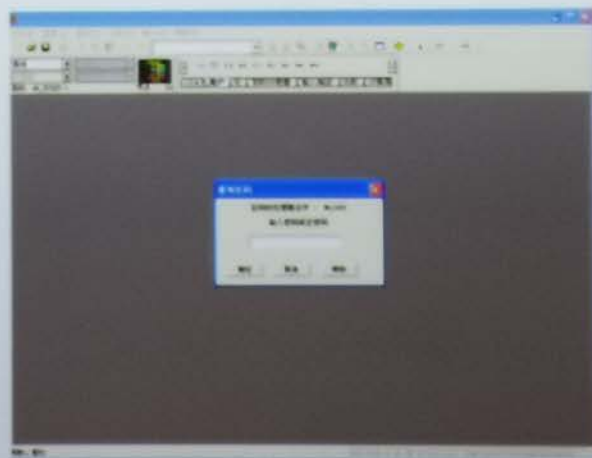
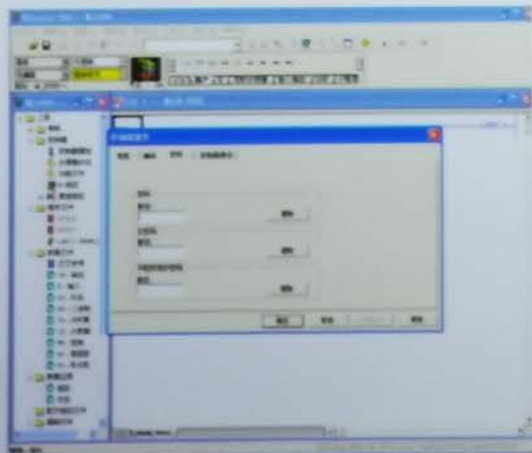


浙江工业职业技术学院

## 泰坦之剑属性四之获取控制权

### 罗克韦尔AB PLC通信密码破解

罗克韦尔Allen-Bradley PLC可以通过RSLogix 500组态软件，对工程设置密码、主密码、子程序保护密码，来实现控制器的权限保护。



[illegible]



WUHAN UNIVERSITY

## 泰坦之剑属性四之获取控制权 某知名厂商SIS系统

该SIS系统可通过设置通信密码，用于连接授权，防止第三方非授权用户连接控制器设备，如下图所示。

### Operating Parameters

Target System      Tricon v9 - 3006 Main Processor

☒ Password Required for Connection

Password: [REDACTED]

☐ Disable Stop on Keyswitch

☒ Disable Remote Changes to Outputs

☐ Allow Disabling of Points

☐ Enable Tricon Mode Time Synchroniz





信息安全等级保护

## 泰坦之剑属性四之获取控制权 某知名厂商SIS系统

该设备存在密码绕过漏洞，授权流程如图所示，当发送特定的一个请求数据包后，控制器会回复包含密码密文信息的数据包，本地解密后和输入的连接密码进行对比，解密码密文的函数如下所示。

```
void __cdecl UTI_PasswordDecrypt(const char *Source, struct CString *a2)
{
    signed int v2; // eax
    char Dest[8]; // [esp+0h] [ebp-Ch]
    char v4; // [esp+0h] [ebp-4h]
    if ( Source && strlen(Source) != 0 )
    {
        Dest[0] = 0;
        strcat(Dest, Source, 8u);
        v4 = 0;
        v2 = 0;
        do // A1 23 11 99 12 33 31 FE
        {
            Dest[v2] -= g_key_tab_byte_1032ECC4[v2];
            ++v2;
        }
        while ( v2 < 8 );
        CString::operator=(a2, Dest);
    }
}
```

因此，可以通过向控制器发送一个特定的数据包，获取到含有密码信息的密文数据后，解密即可得到控制器通信密码，最终获取与控制器通信的控制权



第七届中国网络安全大会

## 泰坦之剑属性五之拒绝服务攻击 西门子PLC系统

Profinet-DCP协议是发现和基本配置协议，用于发现无IP地址的节点，然后设置其IP地址、默认网关、子网掩码。帧格式如下图所示：



DevicePropertiesOption共有6种子选项，如下表所示：

值	含义	访问方式
0x01	SuboptionDeviceVender	Read
0x02	SuboptionNameOfStaion	Read/Write
0x03	SuboptionDeviceID	Read
0x04	SuboptionDeviceRole	Read
0x05	SuboptionDeviceOptions	Read
0x06	SuboptionAliasName	Read
其他	保留	



## 泰坦之剑属性五之拒绝服务攻击 西门子PLC系统

通过逆向分析，该程序在对每一个block进行处理时，使用new语句分配了一个固定大小的内存，如果block数目过多，会造成内存空间不够，引起堆溢出，造成拒绝服务。

```
sub_1400001000( ),
}
if ( v11 == 1 )
{
    v17 = operator new(0x580ui64);
    memset(v17, 0, 0x580ui64); // chenglei 分配内存为定值
    v39 = 0i64;
    v40 = 0;
    LOBYTE(r14_0) = 1;
    if ( v10 == 3 )
    {
        LODWORD(v32) = sub_1400251E0(v12, *(_QWORD *) &a5, (unsigned __int16) a7);
        LOBYTE(v32) = 1;
        v34 = v32;
        sub_14002CA40(v32, &v39, v33);
        if ( (unsigned __int64) v39 <= 0x580 )
        {
```





第七届中国工控安全大会

## 总结



工业控制系统  
协议缺乏足够的  
安全性考虑



严重漏洞难以  
及时处理

### 泰坦之剑

1. 利用工业协议攻击
2. 构造恶意代码攻击
3. 窃取机密数据
4. 获取控制权
5. 造成系统拒绝服务



面对新型的  
APT攻击,  
缺乏有效的  
应对措施



缺乏违规操作、  
越权访问行为  
审计能力



第七届国际科学大会

## 总结



小鹅助理



# 谢谢!

扫码添加小鹅助理，与数万科技圈人士  
分享重量级活动PPT、干货培训课程、高端会议免费门票