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

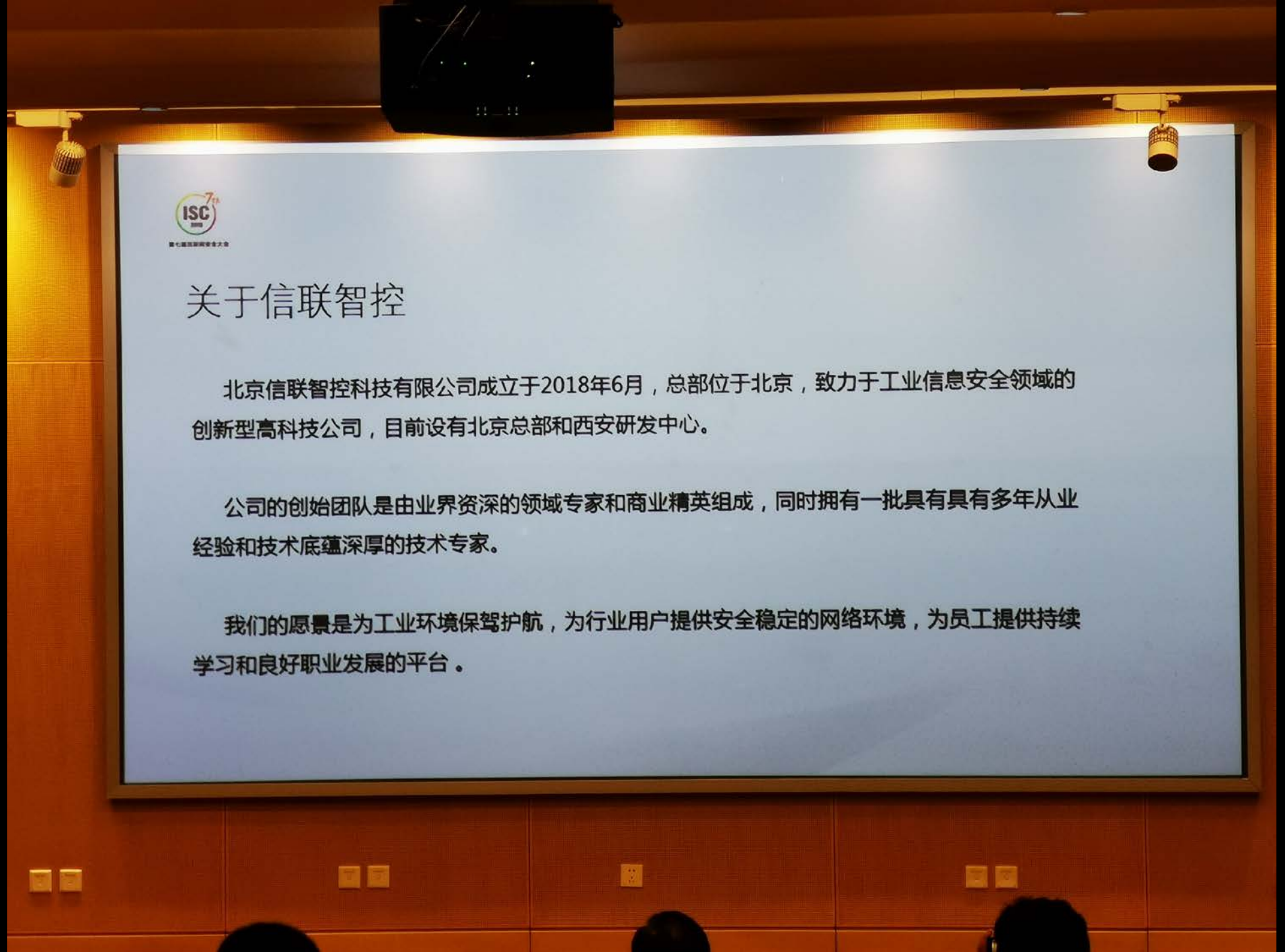
小鹅助理

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


ISC
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术底蕴深厚的技术专家。
我们的愿景是为工业环境保驾护航，为行业用户提供安全稳定的网络环境，为员工提供持续学习和良好职业发展的平台 。

关于我

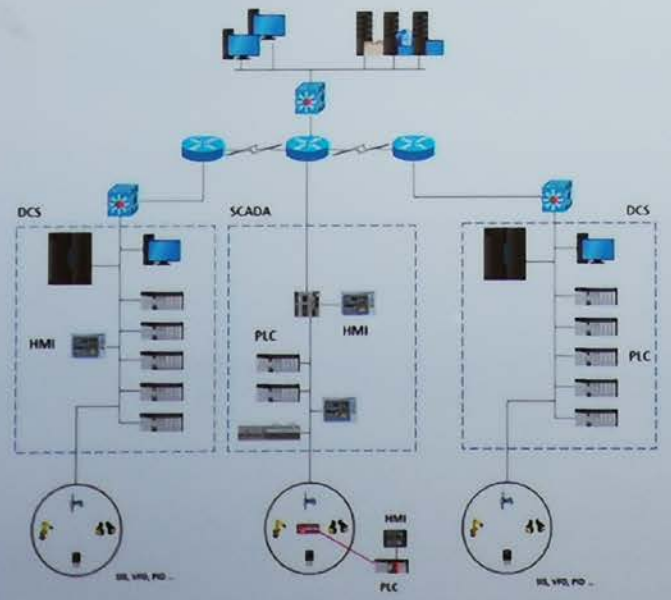
信联智控首席科学家，5年DCS软件研发与技术支持，3年工控安全研究

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

工业控制系统



PLC：可编程逻辑控制器

DCS：分布式控制系统

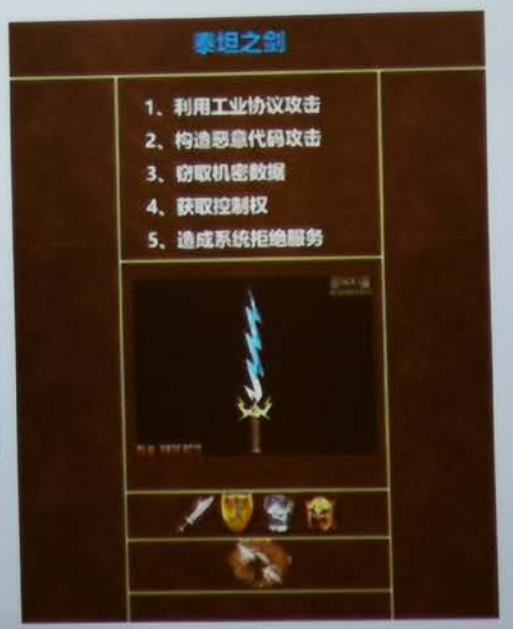
SCADA：数据采集与监视控制系统

SIS：安全仪表系统

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

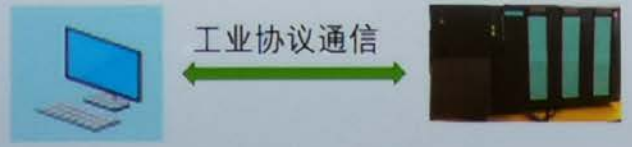


泰坦之剑属性一之工业协议攻击

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



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

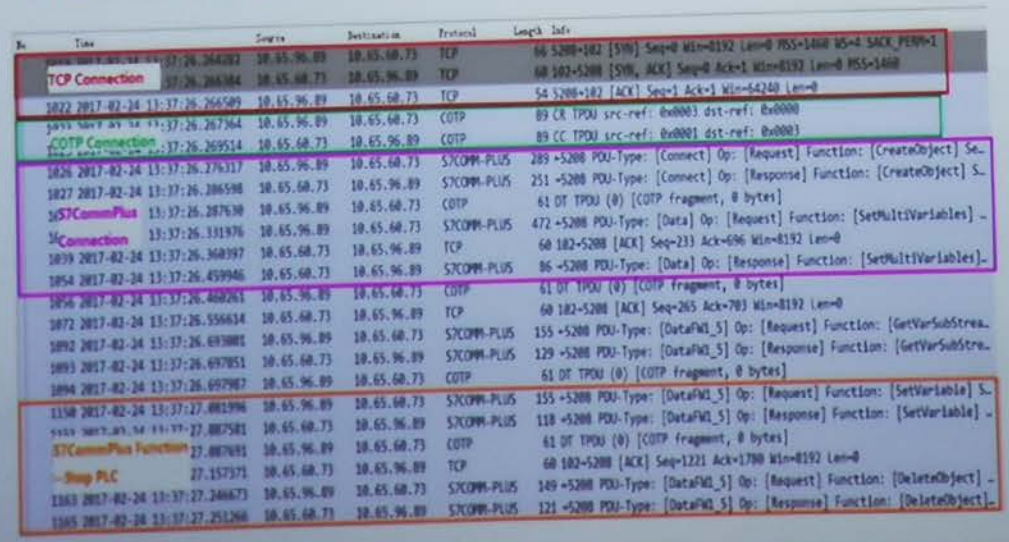
S7-1500

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

泰坦之剑属性一之工业协议攻击

西门子PLC

S7CommPlus协议



泰坦之剑属性一之工业协议攻击

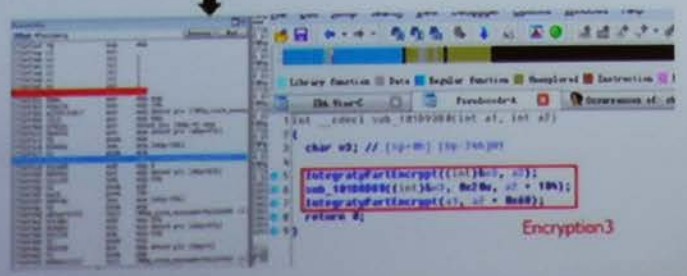
西门子PLC

S7CommPlus协议

一个包含Sesssion 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

包含Session ID的数组

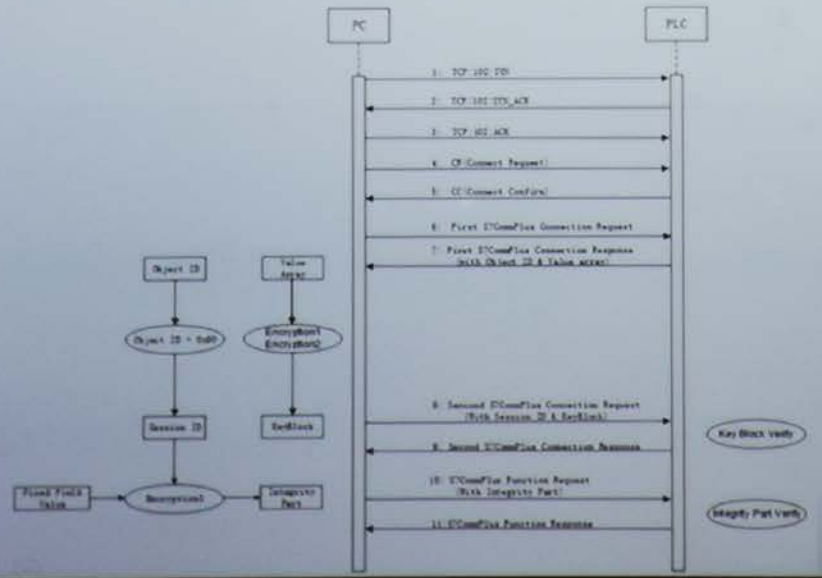
加密算法



泰坦之剑属性一之工业协议攻击

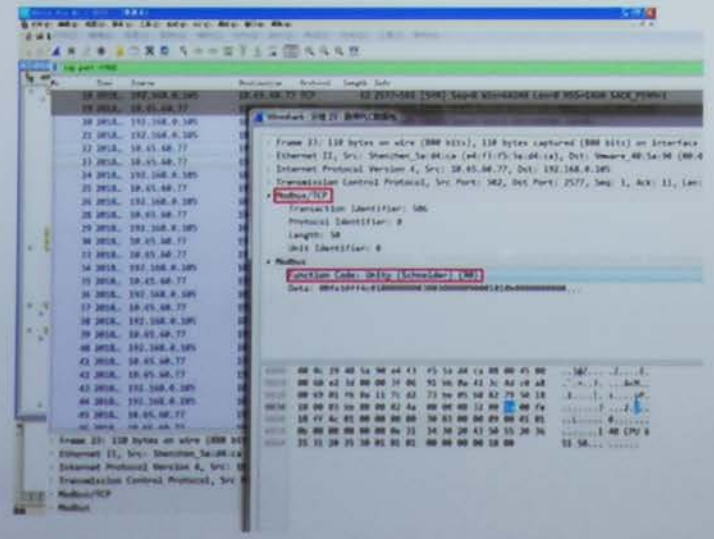
西门子PLC

S7CommPlus协议



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

泰坦之剑属性一之工业协议攻击

施耐德PLC

1. 获取Session ID

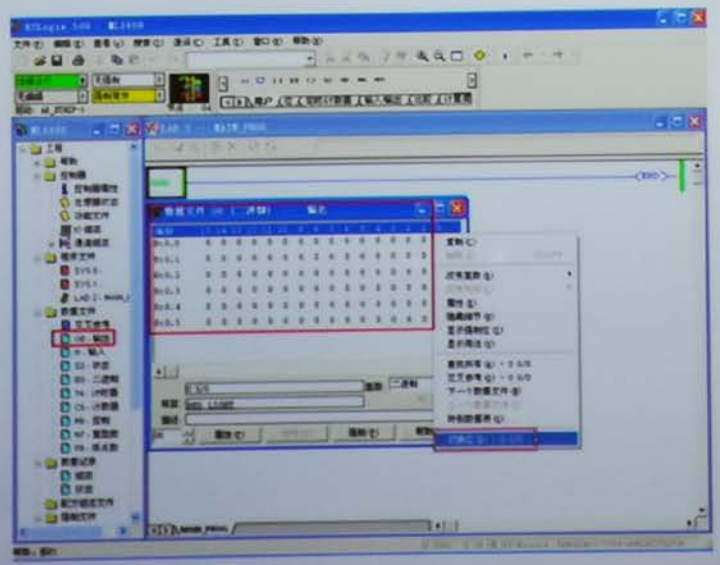
59	2018-01-05 10:30:04.090915	192.168.0.105	10.65.60.77	Modbus/TCP	73	Query:	Trans:	600;	Unit:	0, Func: 90: Unity (Sch…
61	2018-01-05 10:30:04.143871	10.65.60.77	192.168.0.105	Modbus/TCP	283	Response:	Trans:	600;	Unit:	0, Func: 90: Unity (Sch…
62	2018-01-05 10:30:04.155349	192.168.0.105	10.65.60.77	Modbus/TCP	73	Query:	Trans:	601;	Unit:	0, Func: 90: Unity (Sch…
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 (Sch…
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 (Sch…
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 (Sch…
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 (Sch…
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 (Sch…
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 (Sch…
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 (Sch…
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 (Sch…
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 (Sch…
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 (Sch…
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 (Sch…

```
▸ Modbus
    Function Code: Unity (Schneider) (90)
    [Request Frame: 66]
    Data: 00fedf
```

```
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..?. ...A<M..
0020  00 69 01 f6 0a 11 7c d2  85 6b 05 b8 8b 72 50 18   .i....|. .k...rP.
0030  10 00 15 fa 00 00 02 5b  00 00 00 05 00 5a 00 fe   .......[ .....Z..
0040  df                                                 .
```

泰坦之剑属性一之工业协议攻击

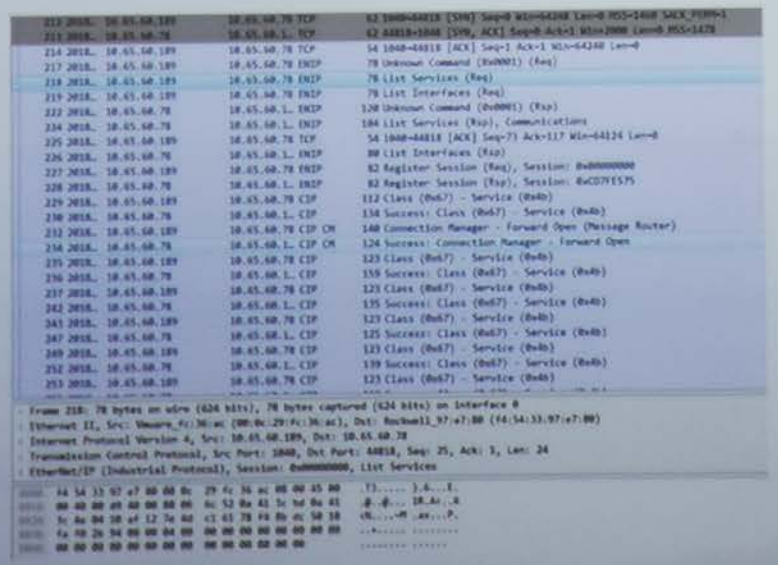
罗克韦尔 AB PLC



RSLogix

泰坦之剑属性一之工业协议攻击

罗克韦尔 AB PLC



RSLogix

EtherNet/IP&CIP

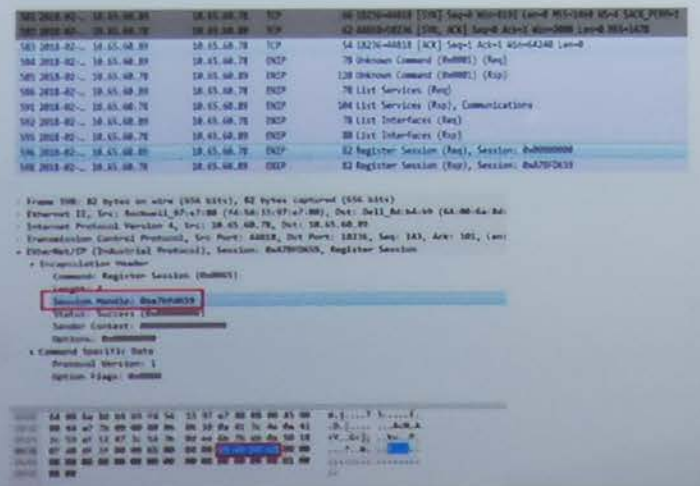
端口: 44818

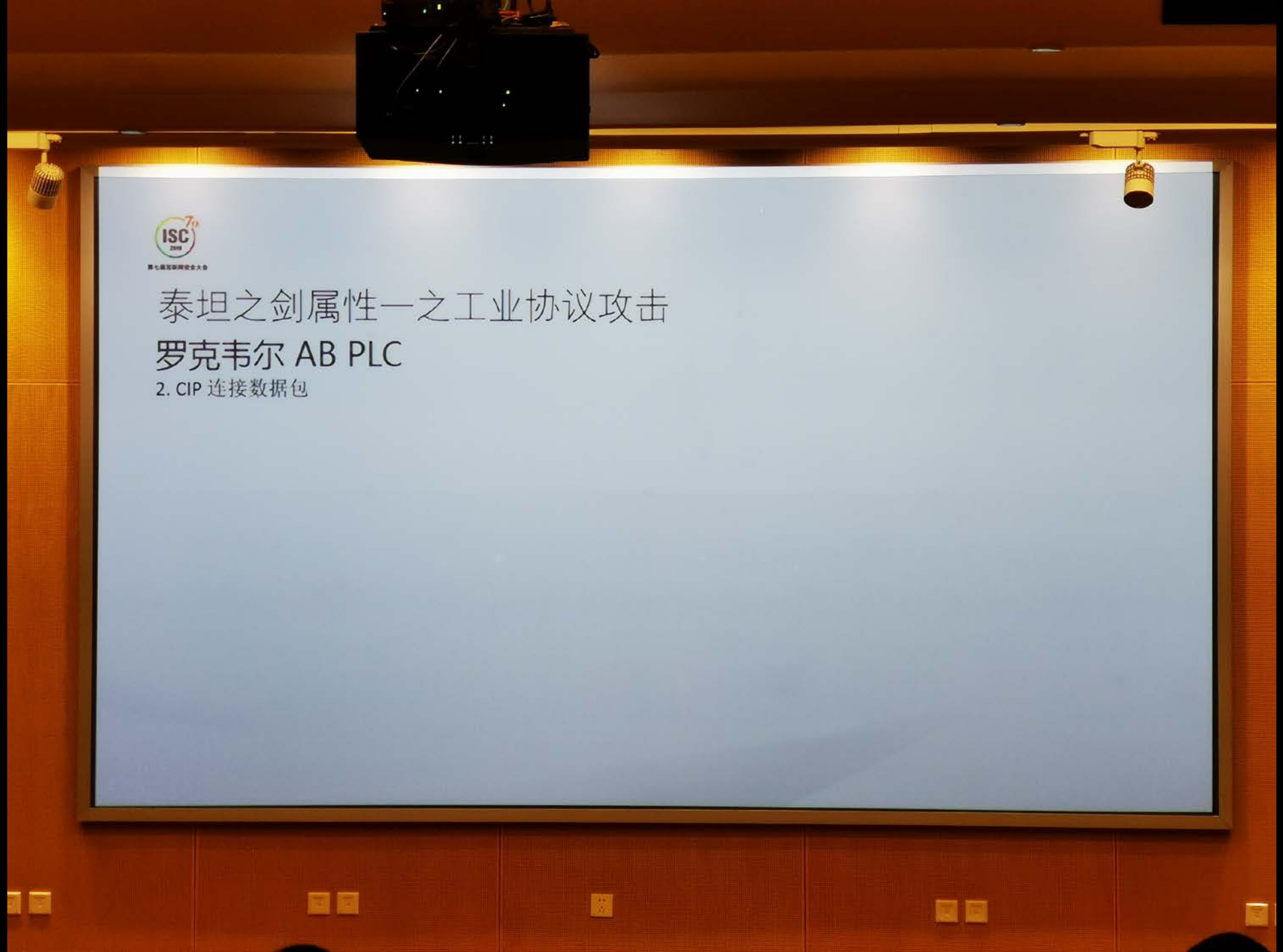
泰坦之剑属性一之工业协议攻击

罗克韦尔 AB PLC

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



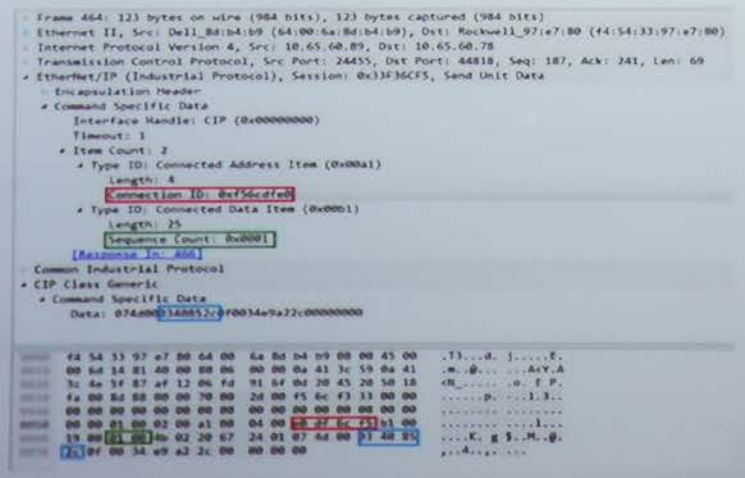

ISC
泰坦之剑属性一之工业协议攻击
罗克韦尔 AB PLC
2. CIP 连接数据包

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

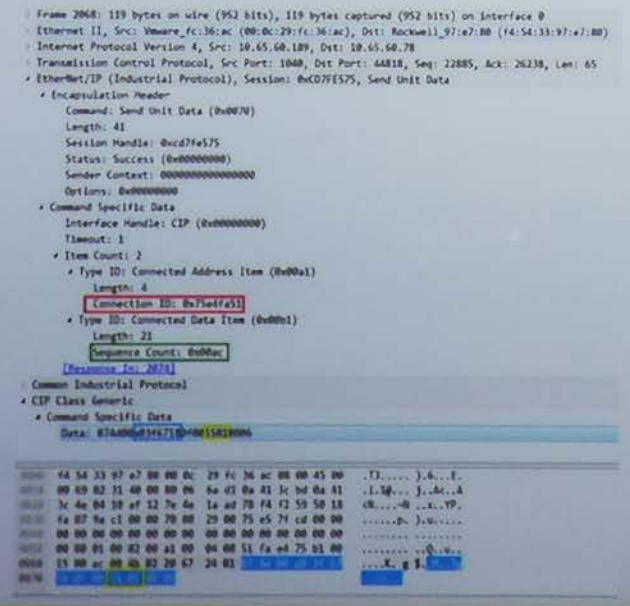
每一个连接数据包都会使用CIP连接响应数据包中的O->T Network Connection ID 以及原始序列号，如下图中的红色框以及蓝色框，每一个连接数据包的Sequence Count需满足递增，如下图绿色框所示



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

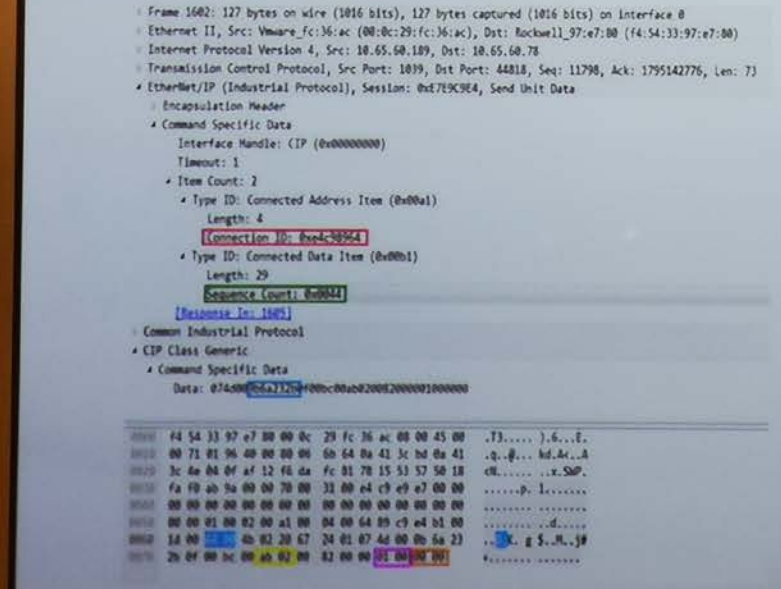


启动PLC数据包如下图所示，红色框是CIP连接响应数据包中的O->T Network Connection ID，蓝色框是CIP连接响应数据包中的Originator Serial Number，绿色框为Sequence Count，黄色框代表功能码，“0x55, 0x01”表示该数据包是启动PLC的数据包

泰坦之剑属性一之工业协议攻击

罗克韦尔 AB PLC

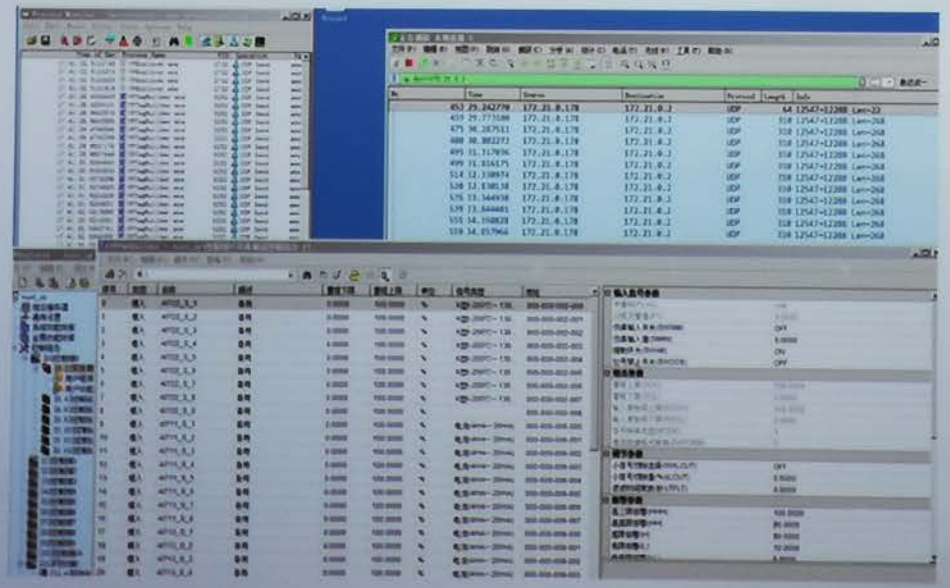
5. 写DO点值数据包



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

泰坦之剑属性一之工业协议攻击

某知名厂商DCS



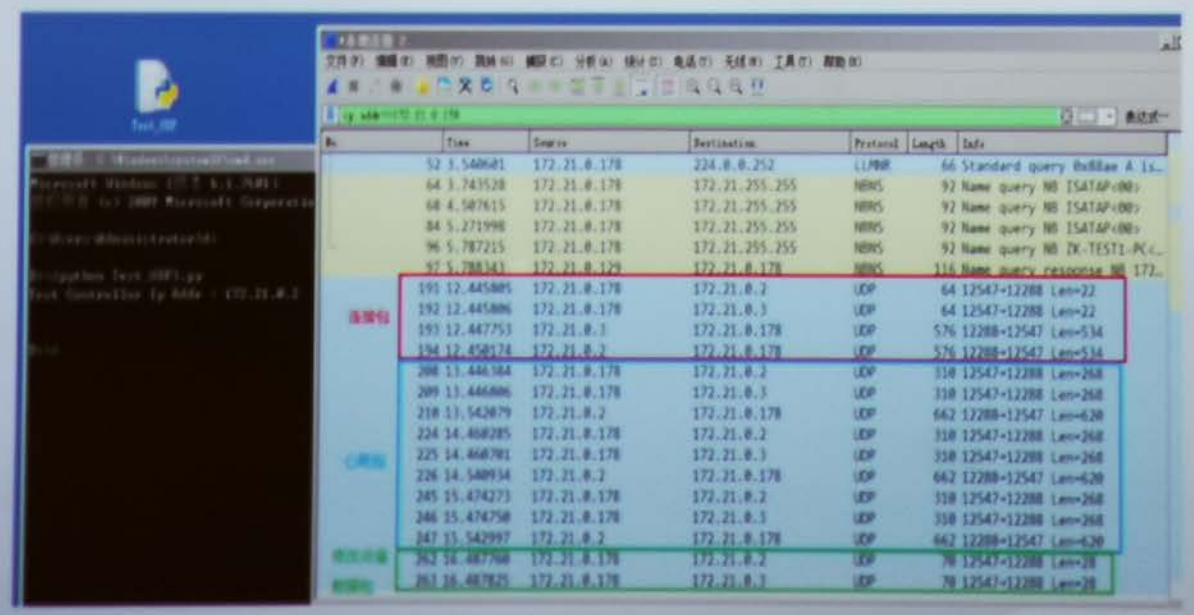
UDP通信

私有协议

端口: 12288

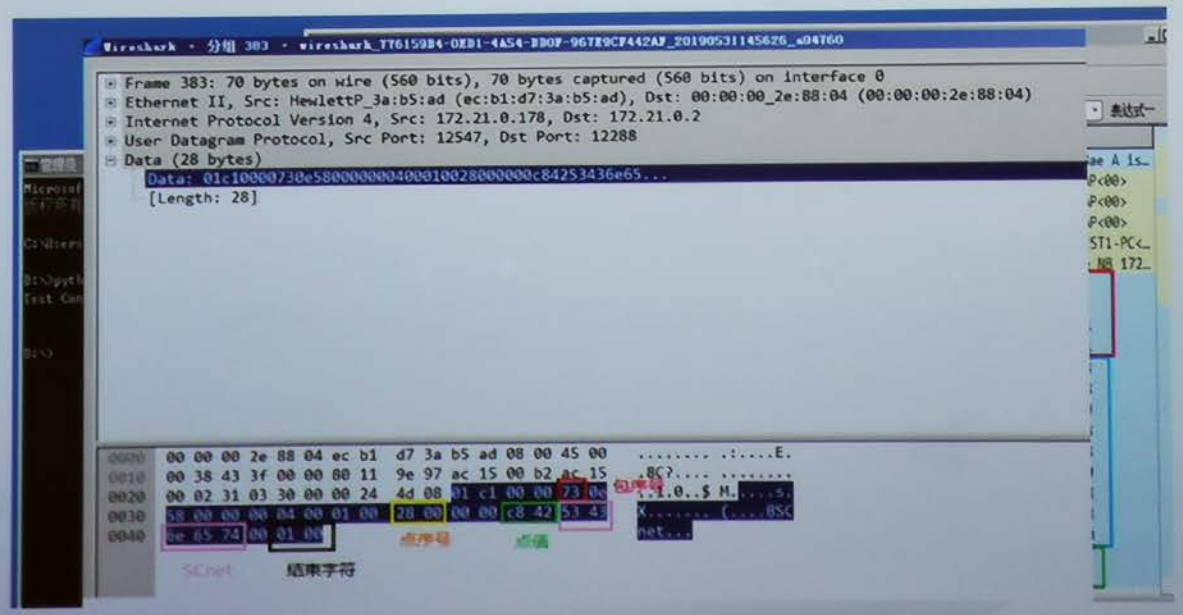
泰坦之剑属性一之工业协议攻击

某知名厂商DCS



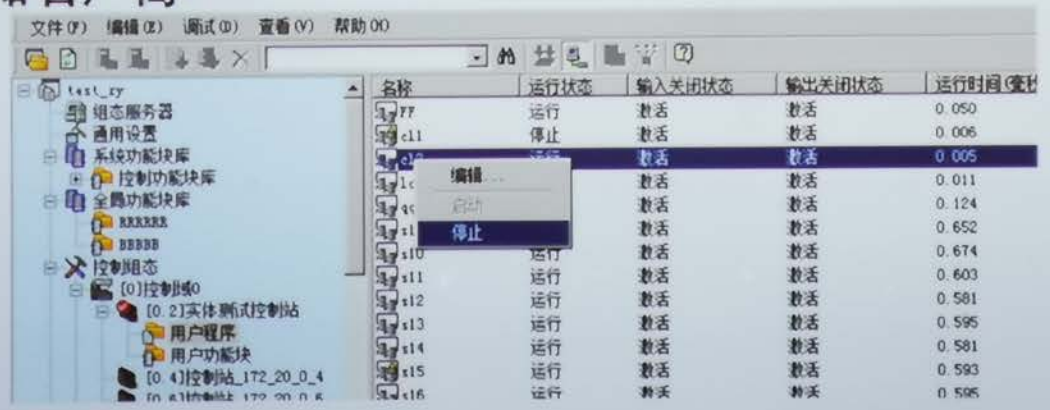
泰坦之剑属性一之工业协议攻击

某知名厂商DCS



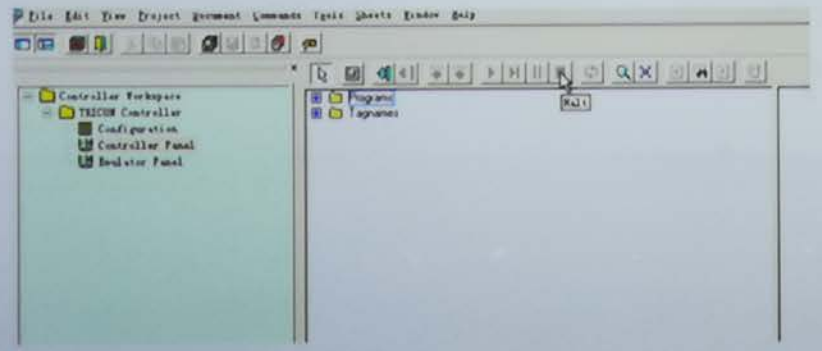
泰坦之剑属性一之工业协议攻击

某知名厂商DCS



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

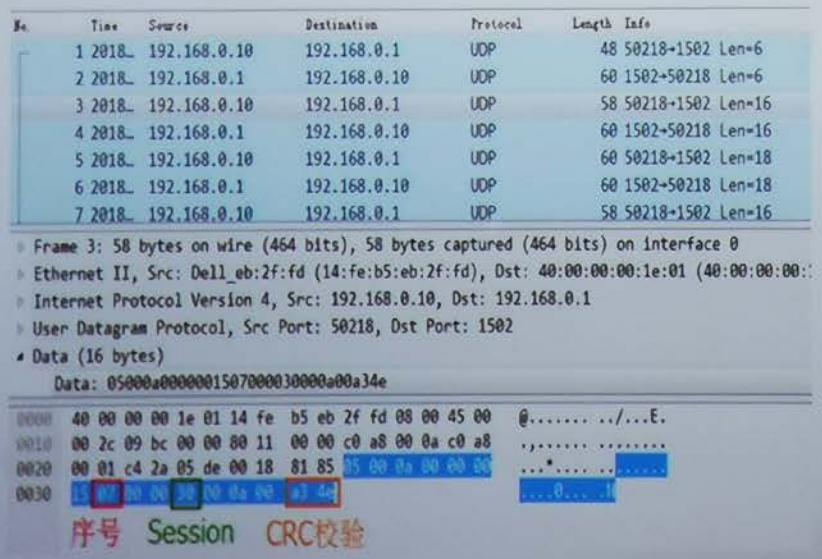
私有协议

端口: 1502

泰坦之剑属性一之工业协议攻击

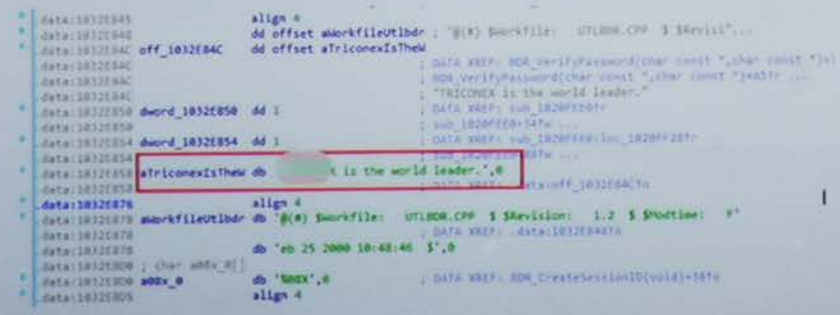
某知名厂商SIS系统

1. 停止控制器数据包



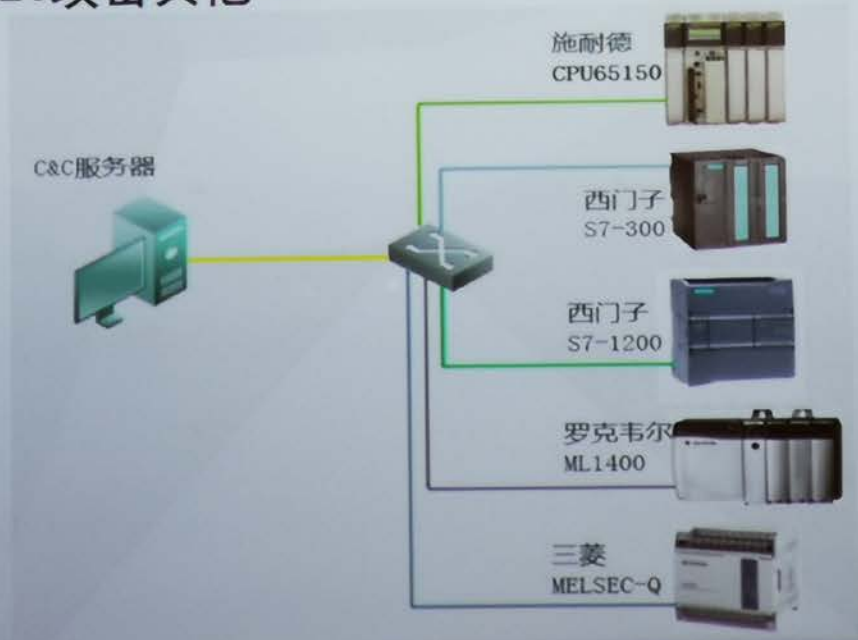
泰坦之剑属性一之工业协议攻击

某知名厂商SIS系统



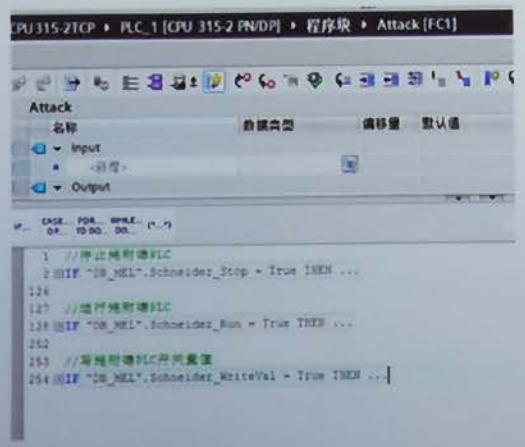
泰坦之剑属性二之恶意代码攻击

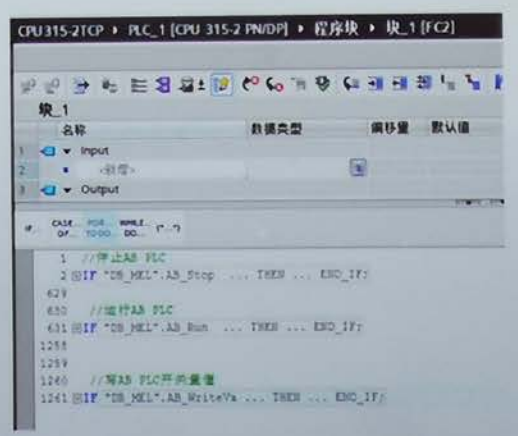
通过PLC攻击其他PLC



泰坦之剑属性二之恶意代码攻击

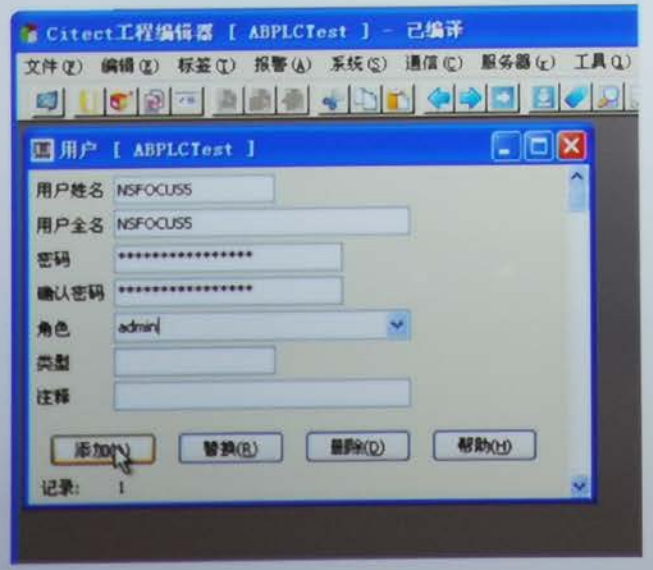
通过PLC攻击其他PLC





泰坦之剑属性三之窃取机密数据

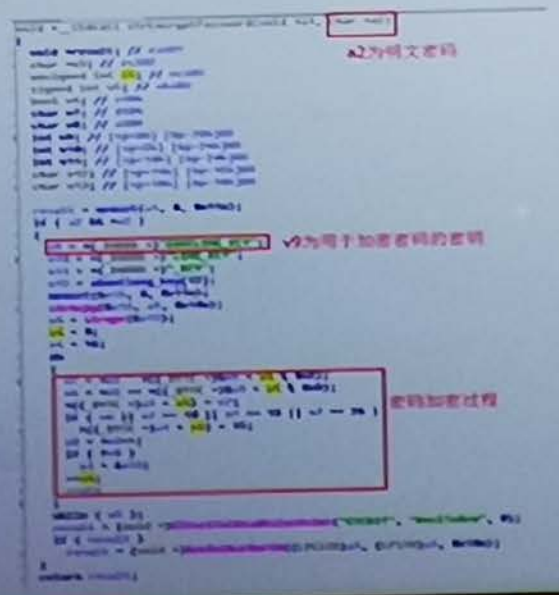
Citect SCADA工程密码破译



泰坦之剑属性三之窃取机密数据

Citect SCADA工程密码破译

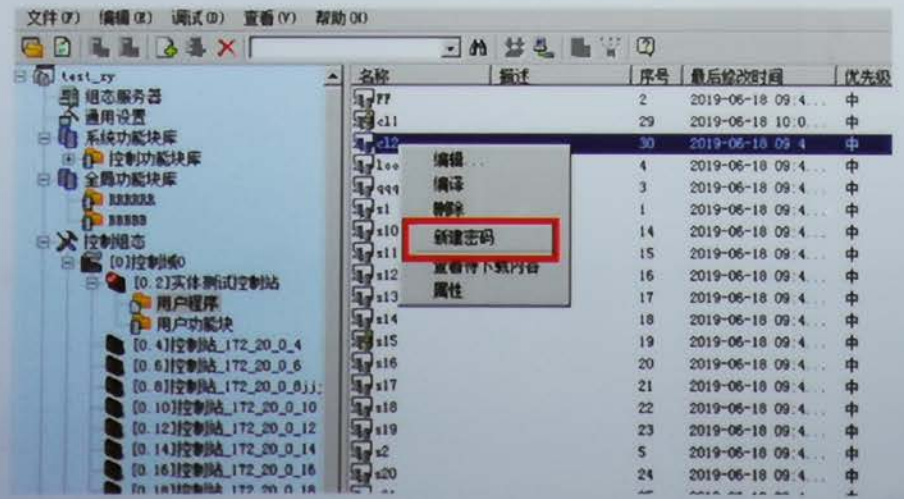
使用动态、静态调试分析，找到Citect软件密码计算的代码，位于CtUtil32.dll中



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

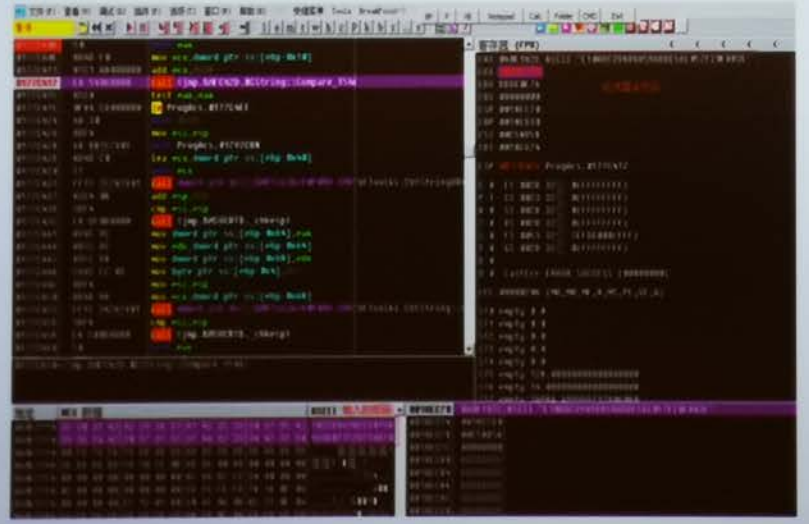
该系统控制器程序可以进行加密，对于加密的程序，需输入正确密码方可看到程序逻辑



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

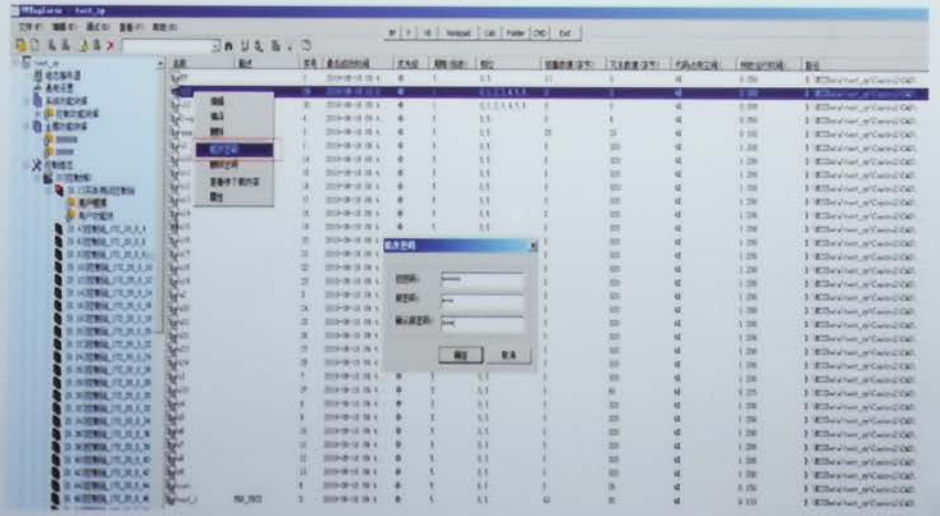
通过逆向调试，发现程序进行密码对比时，使用密文对比，另外其加密算法比较复杂



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

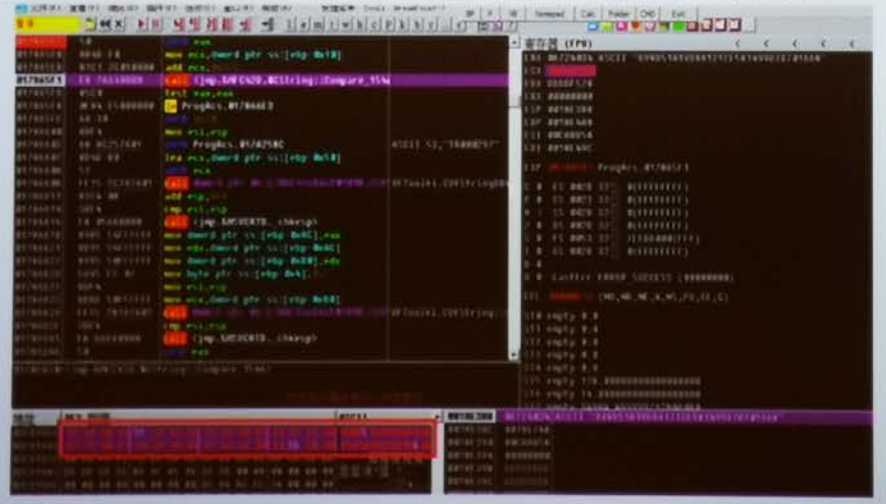
继续研究发现对于已加密的程序可以 进行密码修改，如下图所示



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

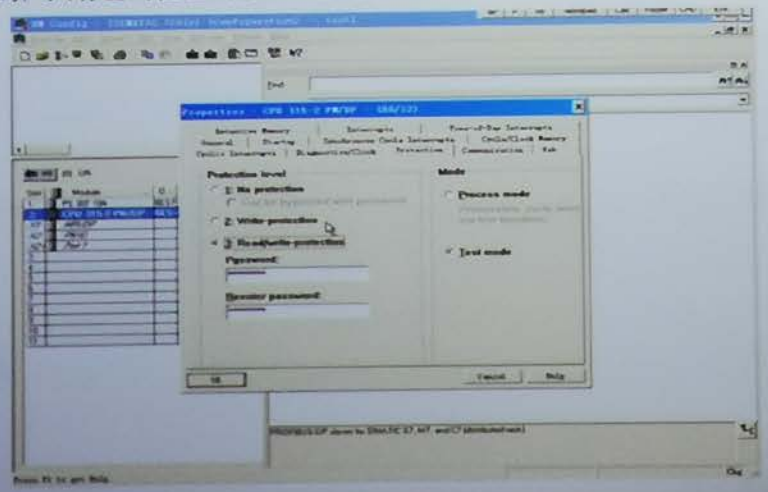
随便输入一个错误的密码，并输入一个新的密码后开始调试，在密码比对的函数中，将自己输入错误密码的密文改成与正确密码密文一致，如下图所示



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



泰坦之剑属性四之获取控制权

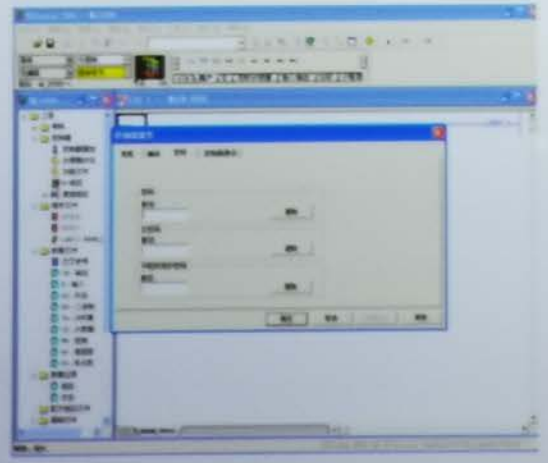
西门子PLC通信密码破解

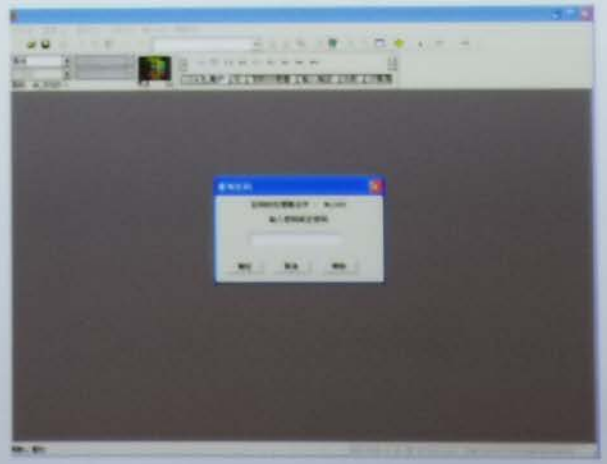
计算完成后，该密码存储于
工程文件夹中\hOmSave7\S7HK31AX\HATTRME1.DBT文件中，如下图所示

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。

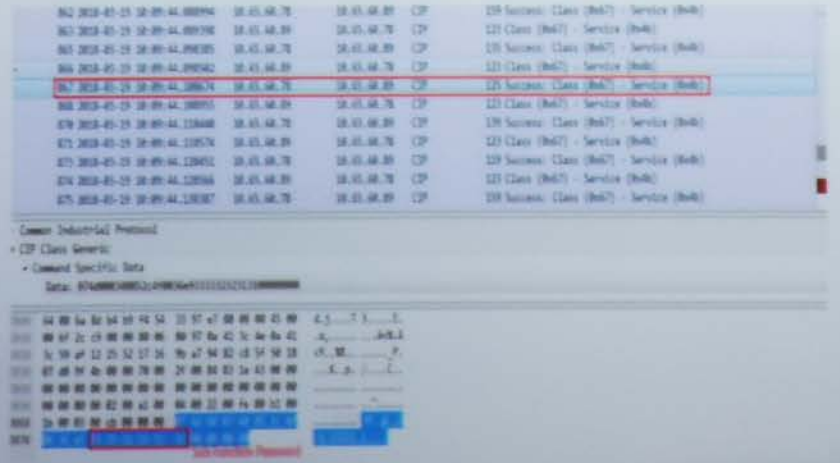




泰坦之剑属性四之获取控制权

罗克韦尔AB PLC通信密码破解

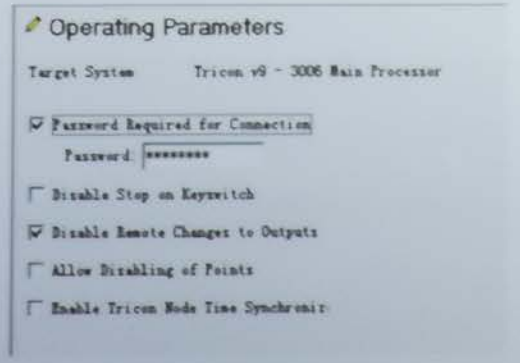
向目标PLC设备发送特定的CIP请求服务数据包，获取到PLC的响应数据包中包含了控制器的子密码



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。



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，解密密码密文的函数如下所示。

```
void __cdecl UTL_PasswordDecrypt(const char *Source, struct CString *A2)
{
  signed int v2; // eax
  char Dest[8]; // [esp+0h] [ebp-Ch]
  char v4; // [esp+8h] [ebp-4h]

  if ( Source && strlen(Source) != 0 )
  {
    Dest[0] = 0;
    strncat(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

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、子关掩码。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

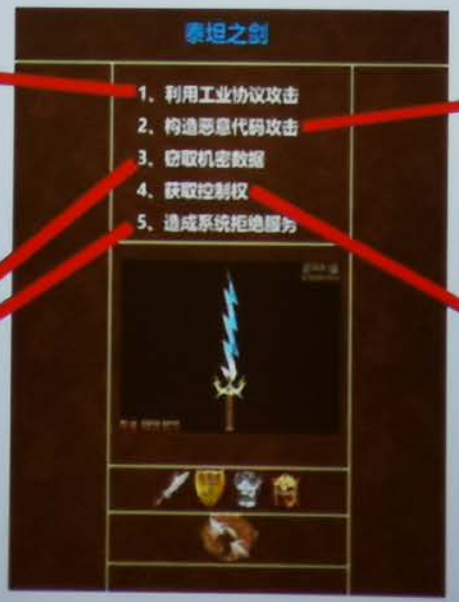
西门子PLC系统

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。

```
}
if ( v11 == 1 )
{
  v17 = operator new(0x58ui64);
  memset(v17, 0, 0x58ui64);                     // 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(v33) = 1;
    v24 = v32;
    sub_14002CA40(v32, &v39, v33);
    if ( (unsigned __int64)v39 <= 0x58A )
    {
```

总结

工业控制系统协议缺乏足够的安全性考虑



面对新型的APT攻击，缺乏有效的应对措施

严重漏洞难以及时处理

缺乏违规操作、越权访问行为审计能力

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