西门子 福建省宁德市（中国）授权 一级代理总代理

产品名称	西门子 福建省宁德市（中国）授权 一级代理总代理
公司名称	广东湘恒智能科技有限公司
价格	.00/件
规格参数	西门子变频器:西门子触摸屏 西门子伺服电机:西门子PLC 西门子直流调速器:西门子电缆
公司地址	惠州大亚湾澳头石化大道中480号太东天地花园2栋二单元9层01号房
联系电话	18475208684 18475208684

产品详情

一提起PLC解密的事情，多少还是有点兴奋的！其实，对于S7-300CPU密码的破解有好几种方法，一种是用读卡器加S7ImgWR/RD软件，还有一种是直接用MMC卡解密软件。但是，今天重点来说一说用TIA Portal+S7Client暴力破解西门子S7-300/400密码。

一、

环境介绍

工具名称	工具说明
TIA Portal V13	[illegible]
s7clientdemo.exe	[illegible]查看cpu密码设置状态工具
Wireshark	用来截取PLC和上位机通信的报文

s7clientdemo.exe下载地址可在公众号后台回复：“ s7client ” 获取二、

准备工作

三、

算法加密

```
intmain(){   char opData[8],Pwd[8],pass[8];   int c;    opData[0] = '1';   o
pData[1] = '2';   opData[2] = '3';   opData[3] = '4';   opData[4] = '5';
 opData[5] = '6';   opData[6] = 0x20;   opData[7] = 0x20;    Pwd[0] =
opData[0] ^ 0x55;          Pwd[1] = opData[1] ^ 0x55;   for (c =
2; c < 8; c++) {       Pwd[c] = opData[c] ^ 0x55 ^ Pwd[c - 2];
};
```

```
/*   Pwd[0] = 0x64;   Pwd[1] = 0x67;   Pwd[2] = 0x02;   Pwd[3] =
0x06;   Pwd[4] = 0x62;   Pwd[5] = 0x65;   Pwd[6] = 0x17;   Pwd[7] =
 0x10;   */
```

四、

暴力破解

五、

存储块解密

我们研究S7-300 CPU密码得到以下成果：

经过研究得出以下结论：

```
charopData[8],Pwd[8],pass[8];   int c;    opData[0] = '1';   opData[1] = '2';
  opData[2] = '3';   opData[3] = '4';   opData[4] = '5';   opData[5] =
'6';   opData[6] = 0xaa;      opData[7] = 0xaa;    Pwd[0] = opData[0]
 ^ 0xaa;   Pwd[1] = opData[1] ^ 0xaa;   for (c = 2; c < 8; c++) {
    Pwd[c] = opData[c] ^ 0xaa ^ Pwd[c - 2];   };
```

六、

保护方式及建议