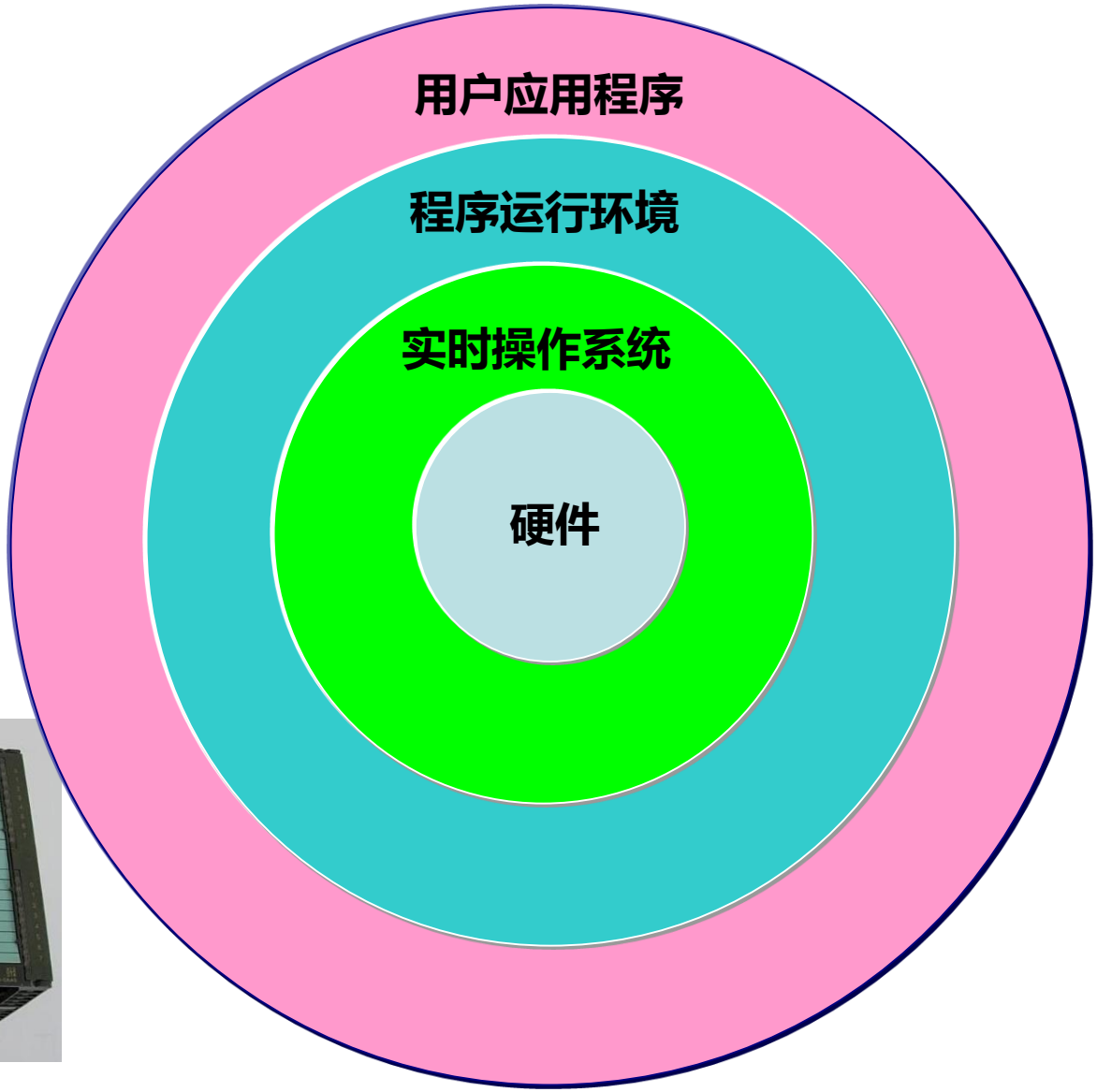
针对PLC攻击的一种新方式研究

工业和信息化部电子科学技术情报研究所
工业信息安全保障技术实验室
李俊　博士

2016/7/20

PLC简介

- CPU
- 电源
- 存储
- I/O
- 网络模块



PLC通讯方式

- **通信介质：双绞线、同轴电缆、光纤**
- **非以太网通信协议（RS232/RS485等串行或总线接口）：**
  - Modbus/Profibus/MPI/DeviceNet/ControlNet
- **以太网通信协议：**
  - Modbus TCP/Profinet/Ethernet IP/IEC104/DNP3

PLC可能存在的安全缺陷

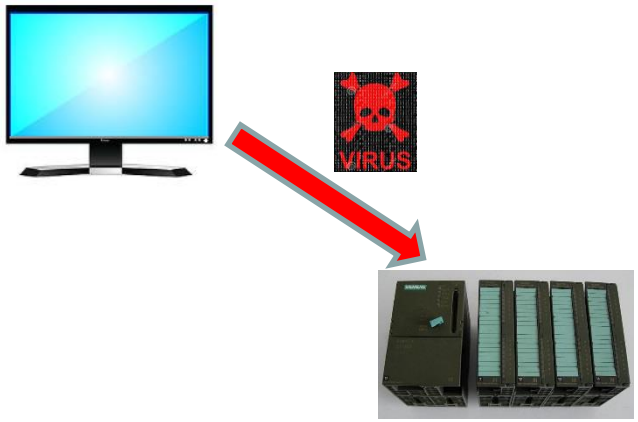
- **通讯协议脆弱性**
  - 无加密
  - 无认证
- **设备无安全策略**
  - 无访问控制
  - 无用户保护

可利用PLC安全缺陷进行攻击

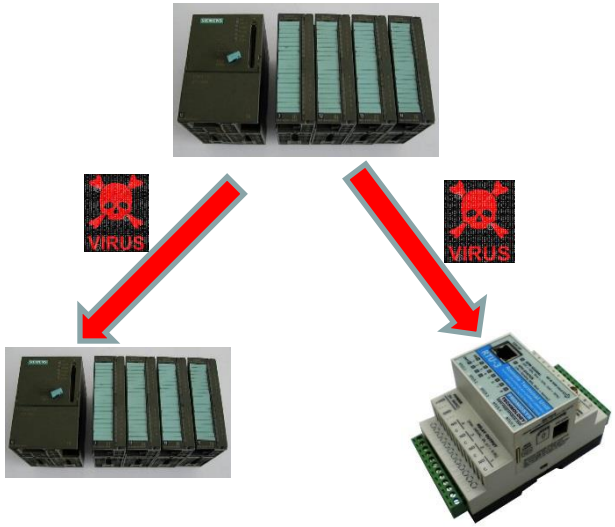
- **修改PLC内存数据**
  - Tag/Address/Var
- **修改PLC运行状态**
  - Stop
  - Run
  - Reset
  - Reboot
- **修改PLC逻辑**
  - Delete
  - Download

对PLC的攻击方式

- **通过PC攻击PLC**
  - 通过渗透等方式获得上位机、工业主机等PC终端权限，再通过PC端向PLC发起攻击
  - 案例：震网、Irongate



- **通过PLC攻击PLC** NEW
  - 利用PLC的通讯功能，攻击其它PLC（或其它工业资产）
  - 案例：PLC-blaster



国外研究动向

- **BlackHat 2015 (2015.8)**
  - SCADACS Internet-Facing PLCs - A New Back Orifice
- **32C3 (2015.12)**
  - OpenSource Security PLC-Blaster - A PLC only worm
- **BlackHat Asia 2016 (2016.3)**
  - OpenSource Security PLC-Blaster: A Worm Living Solely in the PLC
- **BlackHat 2016 (2016.8)**
  - OpenSource Security PLC-Blaster: A Worm Living Solely in the PLC

针对PLC攻击的一种新方式研究

- **以西门子S7系列PLC为研究对象**
  - 掌握S7协议，实现了S7协议功能测试工具
  - 通过西门子S7-1200 PLC实现内网扫描
  - 通过西门子S7-1200 PLC实现Socks代理
  - 实现对不同型号、不同品牌PLC的攻击

研究实验环境

国家工业控制系统与产品安全质量监督检验中心

- **S7-1200 PLC 2台**
  - 6ES7-211-1HE40-0XB0
- **S7-300 PLC 1台**
  - 6ES7-313C-5BE01-0AB0
  - CP 343-1（6GK7-343-1EX30-0XE0）
- **天然气管道输送SCADA系统测试床一套**
  - 阿尔泰Modbus RTU2个
  - 被控对象: 比例阀

研究实验环境

S7-300

S7-1200

阿尔泰RTU

工控系统与产品综合检测平台

天然气管道SCADA系统

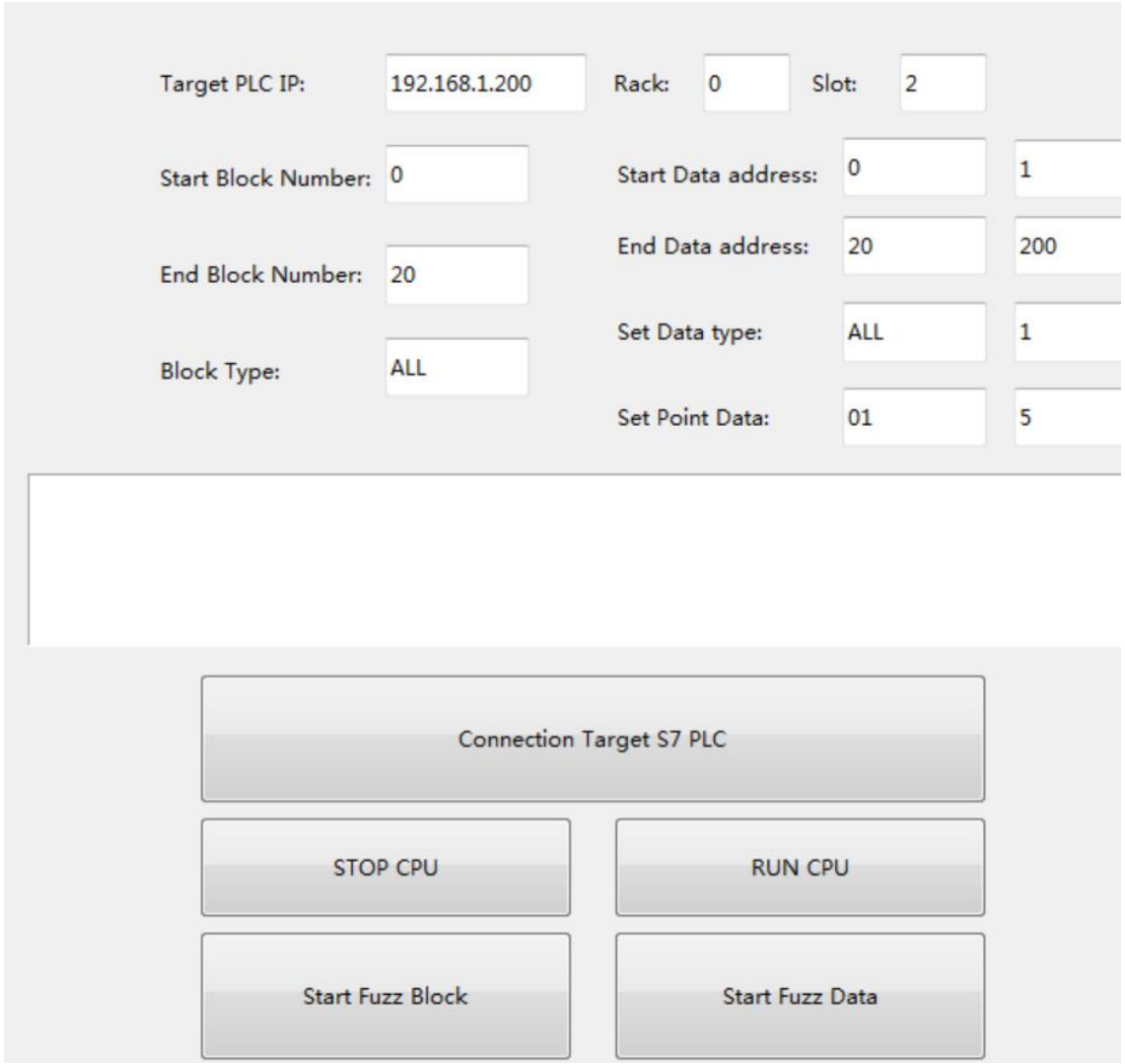
针对PLC攻击的一种新方式研究

- **以西门子S7系列PLC为研究对象**
  - 掌握S7协议，实现了S7协议功能测试工具
  - 通过西门子S7-1200 PLC实现内网扫描
  - 通过西门子S7-1200 PLC实现Socks代理
  - 实现对不同型号、不同品牌PLC的攻击

S7协议功能测试工具

数据测试

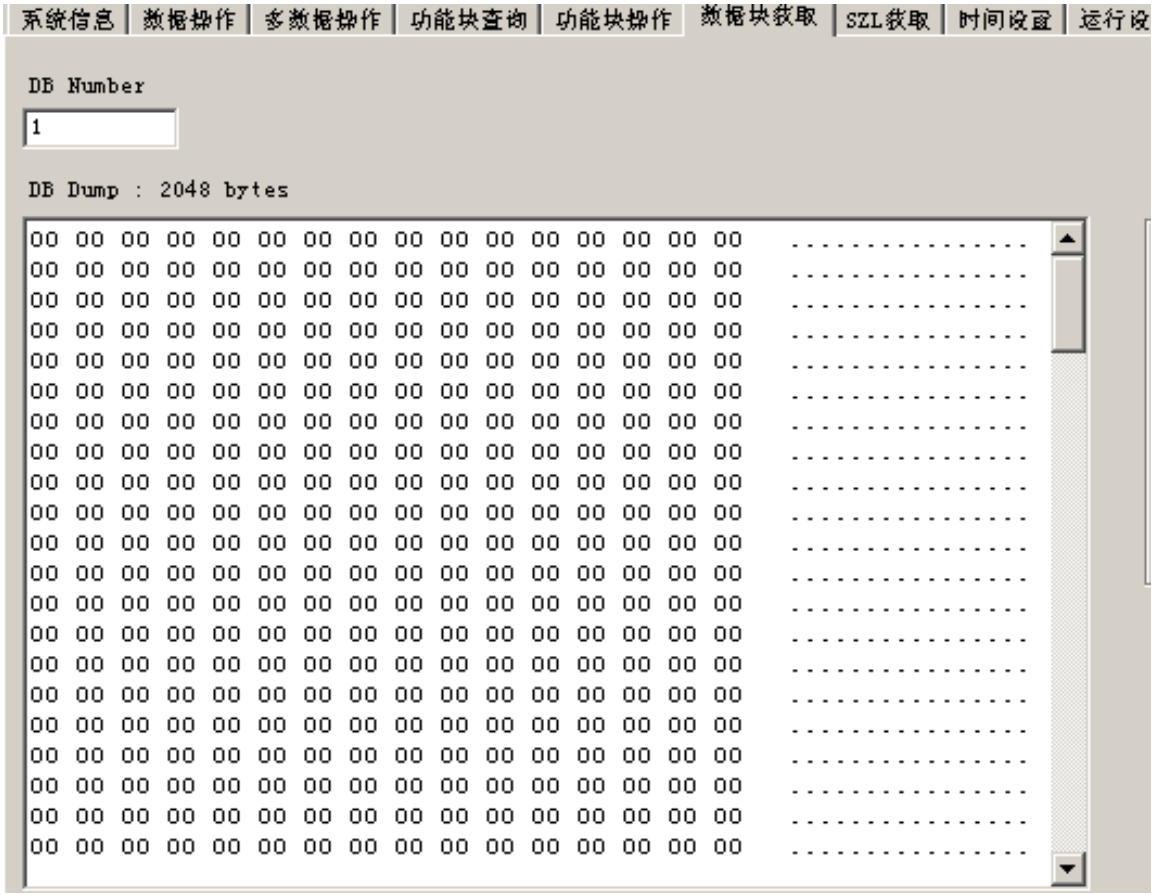
- PLC Tester
  - Get Module Info
  - Set CPU Run/Stop
  - Fuzz Set Value
  - Fuzz DB Data
  - Fuzz Block



S7协议功能测试工具

程序测试

- PLC Tester
  - Block Download
  - Block Upload
  - Block Delete
  - DB Upload
  - Data Change
  - Time Setting
  - ……



针对PLC攻击的一种新方式研究

- **以西门子S7系列PLC为研究对象**
  - 掌握S7协议，实现了S7协议功能测试工具
  - 通过西门子S7-1200 PLC实现内网扫描
  - 通过西门子S7-1200 PLC实现Socks代理
  - 实现对不同型号、不同品牌PLC的攻击

PLC自带通讯功能

- **S7-300**
  - FB65 "TCON"
  - FB63 "TSEND"
  - FB64 "TRCV"
- **S7-1200**
  - TCON
  - TSEND/TUSEND
  - TRCV/TURCV
- **CP**
  - AG_SEND
  - AG_RECV

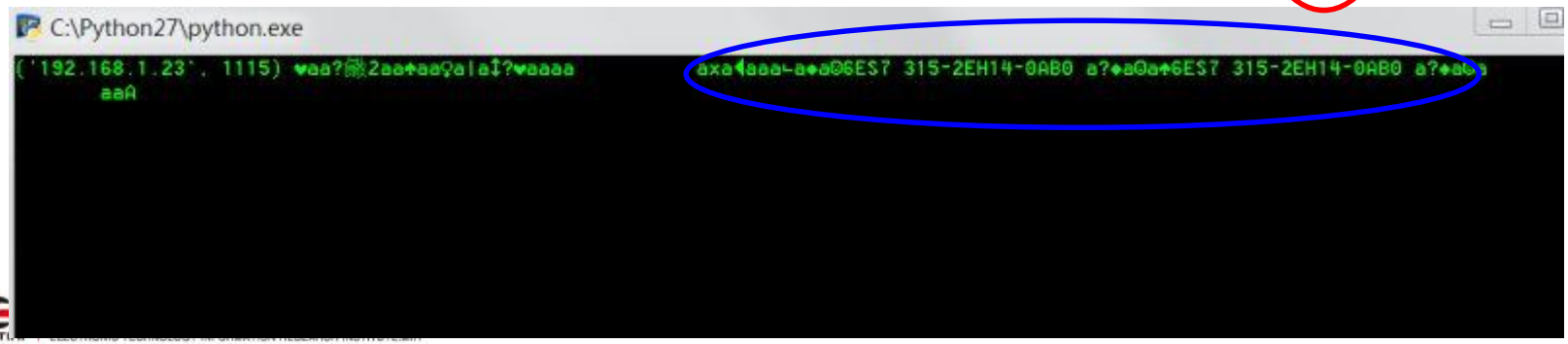
通过西门子S7-1200 PLC实现内网扫描

利用TCON/TSEND(TUSEND)/TRCV(TURCV)在PLC中实现：

- **SNMP扫描**
  - Get OID Description for 1.3.6.1.2.1.1.1
- **ISO-TSAP扫描**
  - COTP（初始化连接）
  - TPKT（确认连接）
  - Read SZL（读系统状态信息）

通过西门子S7-1200 PLC实现内网扫描

	名称	数据类型	偏移里	启动值	监视值
	Static				
	Static_1	Array[0..1024] of Byte	0.0		
	Static_1[0]	Byte	0.0	16#0	16#03
	Static_1[1]	Byte	1.0	16#0	16#00
	Static_1[2]	Byte	2.0	16#0	16#00
	Static_1[3]	Byte	3.0	16#0	16#99
	Static_1[4]	Byte	4.0	16#0	16#02
	Static_1[5]	Byte	5.0	16#0	16#F0
	Static_1[6]	Byte	6.0	16#0	16#80
	Static_1[7]	Byte	7.0	16#0	16#32
	Static_1[8]	Byte	8.0	16#0	16#07
	Static_1[9]	Byte	9.0	16#0	16#00
	Static_1[10]	Byte	10.0	16#0	16#00
	Static_1[11]	Byte	11.0	16#0	16#00
	Static_1[12]	Byte	12.0	16#0	16#00
	Static_1[13]	Byte	13.0	16#0	16#00
	Static_1[14]	Byte	14.0	16#0	16#0C
	Static_1[15]	Byte	15.0	16#0	16#00
	Static_1[16]	Byte	16.0	16#0	16#7C
	Static_1[17]	Byte	17.0	16#0	16#00
	Static_1[18]	Byte	18.0	16#0	16#01
	Static_1[19]	Byte	19.0	16#0	16#12
	Static_1[20]	Byte	20.0	16#0	16#08
	Static_1[21]	Byte	21.0	16#0	16#12
	Static_1[22]	Byte	22.0	16#0	16#84
	Static_1[23]	Byte	23.0	16#0	16#01
	Static_1[24]	Byte	24.0	16#0	16#00

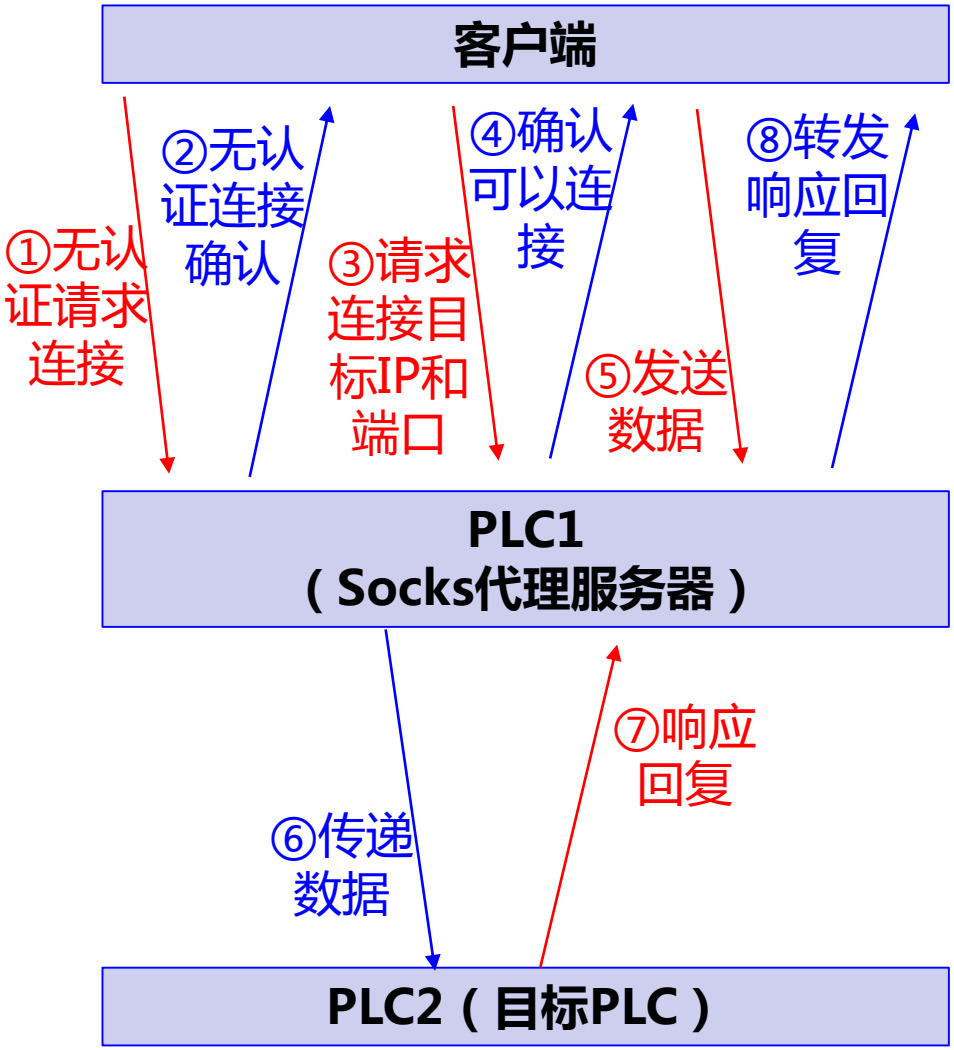


针对PLC攻击的一种新方式研究

- **以西门子S7系列PLC为研究对象**
  - 掌握S7协议，实现了S7协议功能测试工具
  - 通过西门子S7-1200 PLC实现内网扫描
  - 通过西门子S7-1200 PLC实现Socks代理
  - 实现对不同型号、不同品牌PLC的攻击

Socks代理交互流程

流程



在S7-1200 PLC上实现Socks后门

client —> PLC1（Socks server）
- 无认证请求连接

PLC1 —> client
- 无认证连接确认

client —> PLC1
- 请求连接IP和端口

PLC1 —> client
- 确认可以连接

client —> PLC1
- Data

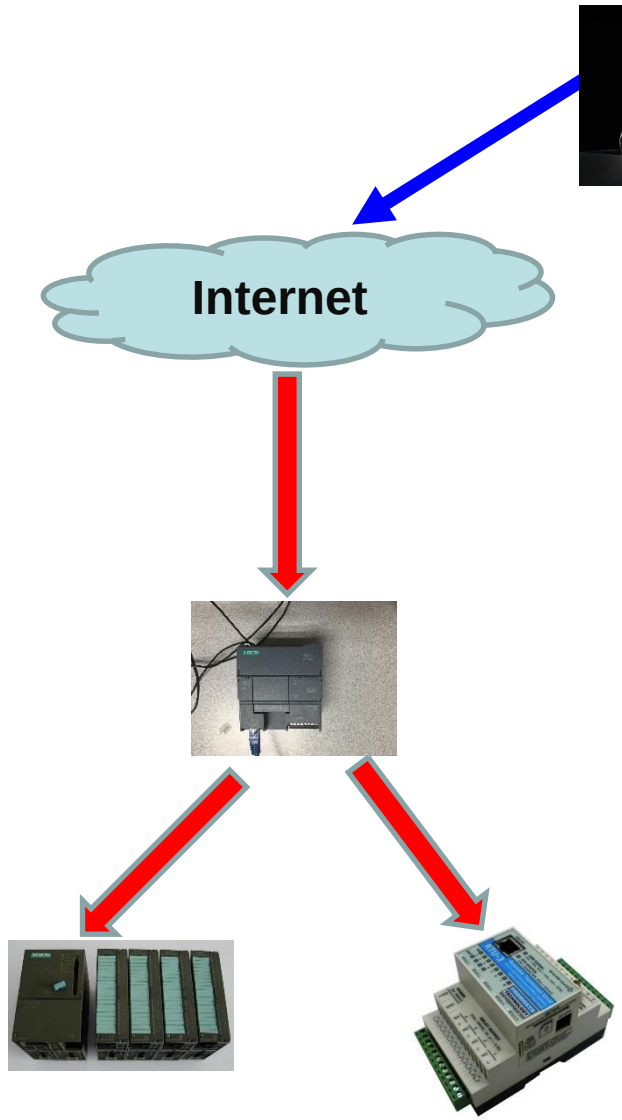
PLC1 —> PLC2
- Forward Data

PLC2—>PLC1
- Response Data

PLC1—>client
- Forward Response Data

危害分析

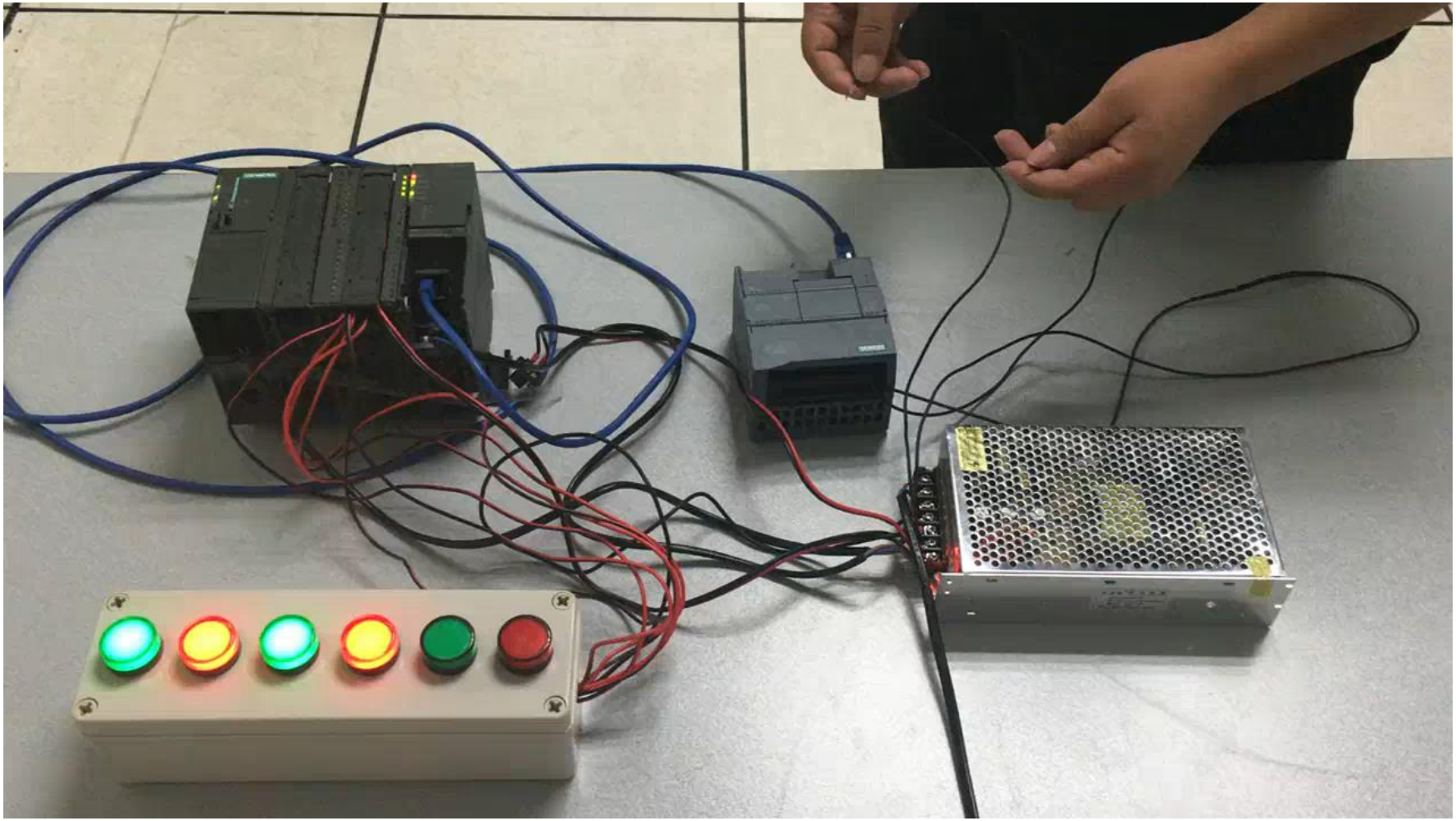
- 访问生产网络其他可达资源
- 突破网络边界
- 绕过白名单等安全防护机制



针对PLC攻击的一种新方式研究

- **以西门子S7系列PLC为研究对象**
  - 掌握S7协议，实现了S7协议功能测试工具
  - 通过西门子S7-1200 PLC实现内网扫描
  - 通过西门子S7-1200 PLC实现Socks代理
  - 实现对不同型号、不同品牌PLC的攻击

攻击演示视频1



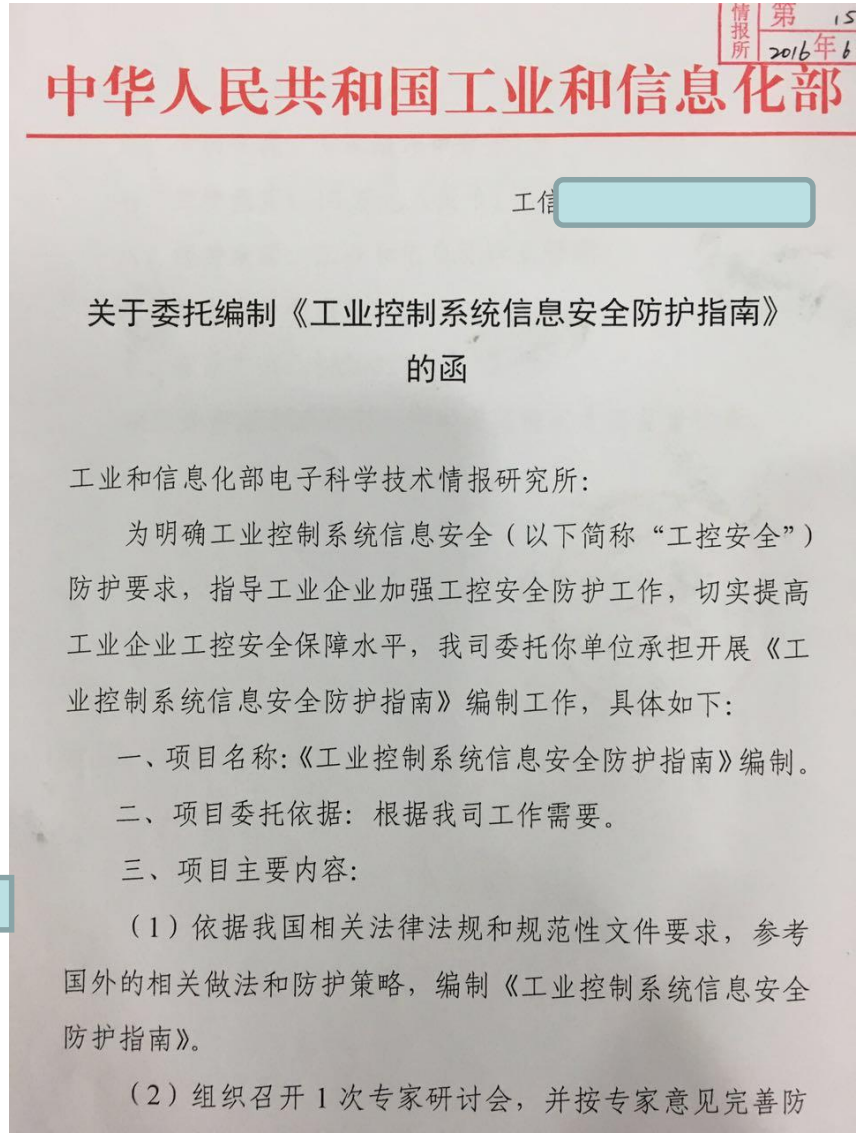
攻击演示视频2


主管道
ETIRI
天然气管道输送SCADA系统
Natural Gas pipeline Transportation SCADA System
工业和信息化部电子科学技术情报研究所
ELECTRONIC TECHNOLOGY INFORMATION RESEARCH INSTITUTE, MIIT

如何加强防护

- 断开不必要的公网连接
- 开启PLC自带的安全防护配置
- 部署网络安全监测设备，发现异常流量

提出了边界防护、安全配置、安全监测等防护措施，可有效避免PLC遭受此类攻击



情报所 第 15 2016年6

中华人民共和国工业和信息化部

工信

关于委托编制《工业控制系统信息安全防护指南》的函

工业和信息化部电子科学技术情报研究所：

为明确工业控制系统信息安全（以下简称“工控安全”）防护要求，指导工业企业加强工控安全防护工作，切实提高工业企业工控安全保障水平，我司委托你单位承担开展《工业控制系统信息安全防护指南》编制工作，具体如下：

一、项目名称：《工业控制系统信息安全防护指南》编制。

二、项目委托依据：根据我司工作需要。

三、项目主要内容：

（1）依据我国相关法律法规和规范性文件要求，参考国外的相关做法和防护策略，编制《工业控制系统信息安全防护指南》。

（2）组织召开1次专家研讨会，并按专家意见完善防

谢谢！

工信部电子一所 工业信息安全保障技术实验室
国家工业控制系统与产品安全质量监督检验中心
李 俊
010-88687835