网络安全创新大会
Cyber Security Innovation Summit

工业安全脆弱性评测与防护建设

姓名　胡杨

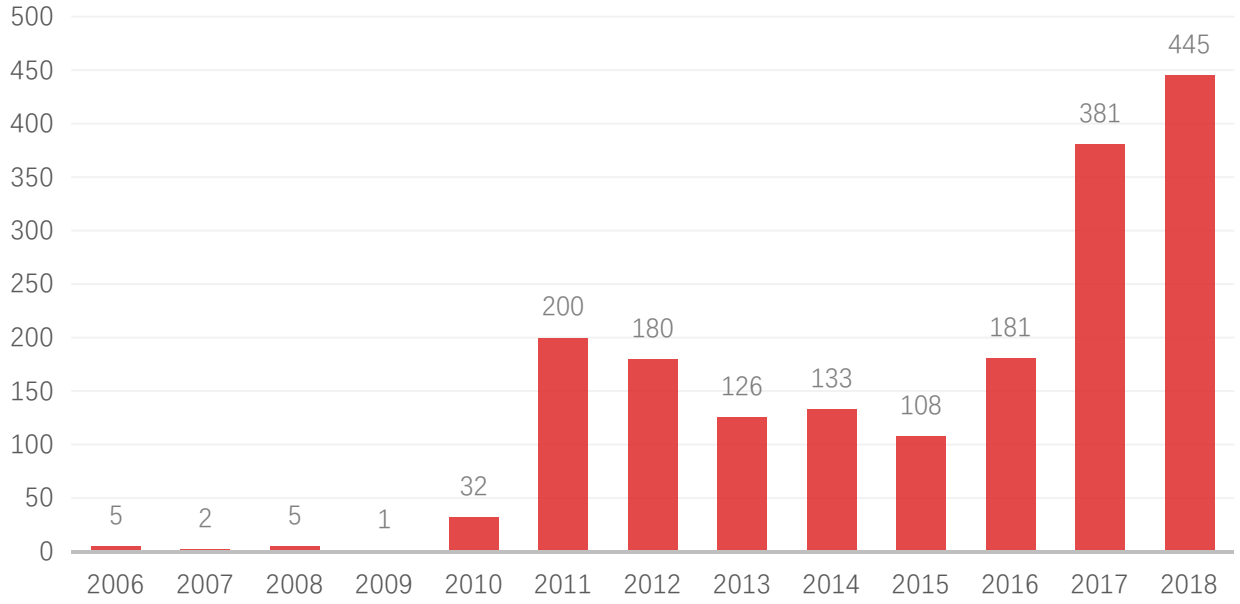
工业安全脆弱性评测与防护建设

胡杨

- Topsec 安全研究员
- IRTeam 团队核心
- Chamd5 IoT组成员
- 主要方向：工业互联网安全建设的实施与脚本小子高效进化的方式

工业互联网安全态势

2006-2018年公开工控漏洞趋势图



2020年	12月1日左右，以色列供水设施ICS遭伊朗黑客入侵
2020年	12月1日，温哥华地铁遭到了Egregor勒索软件的破坏
2020年	11月29日左右，富士康被黑客攻击，索要 2.3 亿元赎金
2020年	11月25日巴西航空工业公司被勒索软件“撕票”
2018年	VPNFilter入侵物联网载体的高级恶意软件攻击
2017年	WannaCry勒索病毒
2016年	乌克兰最大机场遭网络攻击
2016年	德国核电站负责燃料装卸系统遭恶意程序攻击
2015年	乌克兰电网BlackEngery病毒
2010年	伊朗核电站举世闻名的“震网”事件

工业互联网架构介绍

执行机构

机械手臂

计量仪表

伺服电机

… … …

控制器
（下位机）

PLC

DCS

RTU

机柜设备

通信协议

工业通信协议

OPC

S7Comm

Modbus TCP

通过网关等设备
进行工业协议与
以太网协议转换

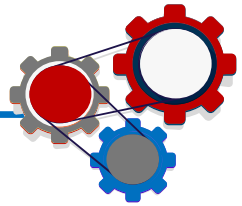
工控主机
（上位机）

操作员站

工程师站

数据库

SCADA



MES\EMS\WMS
系统

生产执行

数据管理

物料管理

信息系统

OT

IT

ERP系统

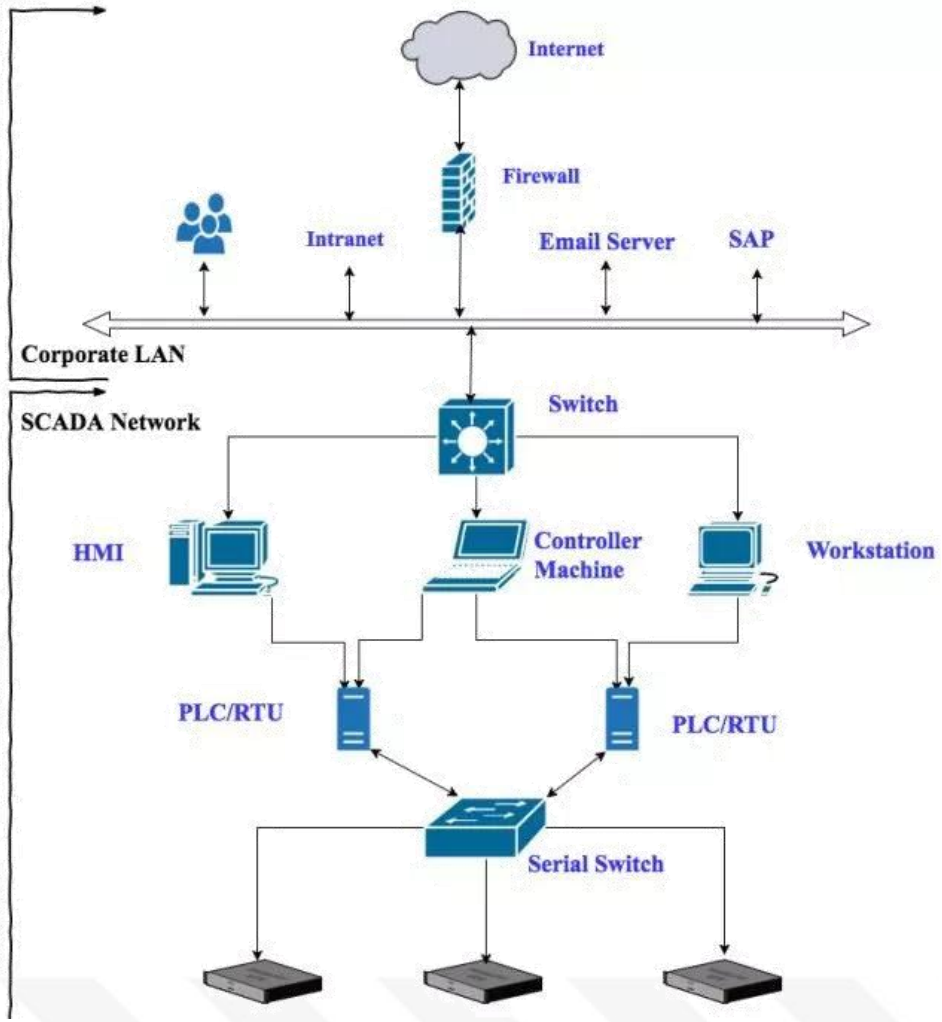
技术管理

材料工时

仓储管理

… … …

工业互联网安全风险点



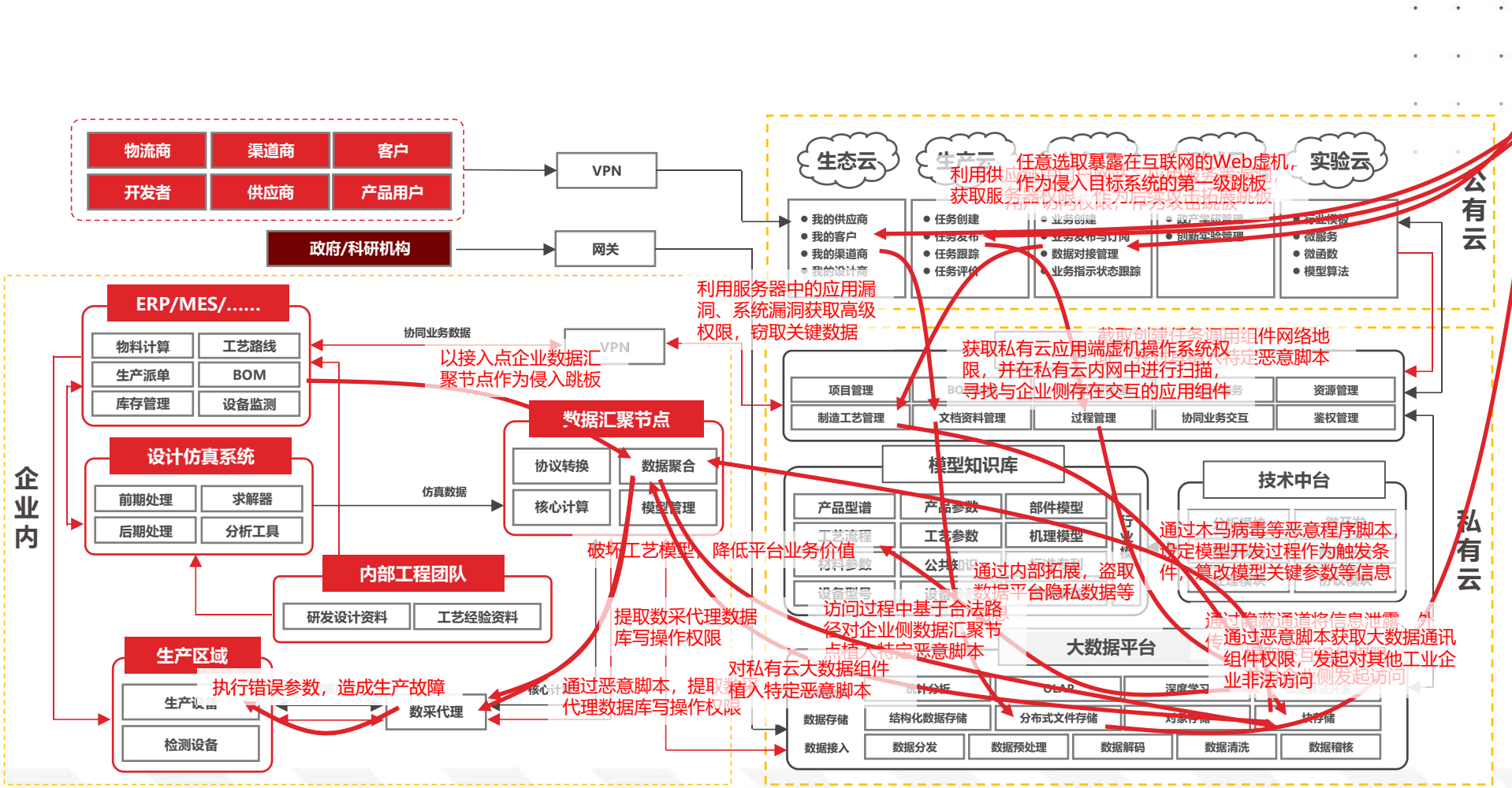
SCADA系统涉及三个主要关键点：

1、人机接口与控制平台：通常使用windows工作站通过软件来管理和控制网络上的PLC。如果工作站被攻击了，那么SCADA网络中的所有内容都可以被访问。

2、PLC（Programmable Logic Controller-可编程逻辑控制器）：可编程逻辑控制器是种专门为在工业环境下应用而设计的数字运算操作电子系统。它采用一种可编程的存储器，在其内部存储执行逻辑运算、顺序控制、定时、计数和算术运算等操作的指令，通过数字式或模拟式的输入输出来控制各种类型的机械设备或生产过程。我们可以通过网路浏览器、Telnet、SSH访问PLC，这样PLC就可能受到各种应用程序和网络层的攻击。一旦遭到攻击，那么攻击者就可以操纵输入与输出设备，并对工业环境造成损害。

3、终端设备（传感器，阀门或泵）：终端设备安装在远程站点。他们可以通过无线电、串型接口、以太网或调制解调器等通信链路向PLC反馈。如果受到攻击可能损害环境的完整性。

工业互联网威胁多样性



攻击者

数据窃取

侵入节点： 公有云Web系统

攻击路径： 公有云web门户-私有云应用-私有云分布式数据库

参数破坏

侵入节点： 公有云Web系统

攻击路径： 公有云web门户-私有云应用-大数据模型开发组件-模型库

生产破坏（纵向）

侵入节点： 公有云Web系统

攻击路径： 公有云web门户-私有云应用-大数据通讯组件-企业侧数据汇聚节点-数采代理-控制

生产破坏（横向）

侵入节点： 企业侧信息化系统

攻击路径： 公有云web门户-私有云应用-大数据通讯组件-企业侧数据汇聚节点-数采代理-控制系统

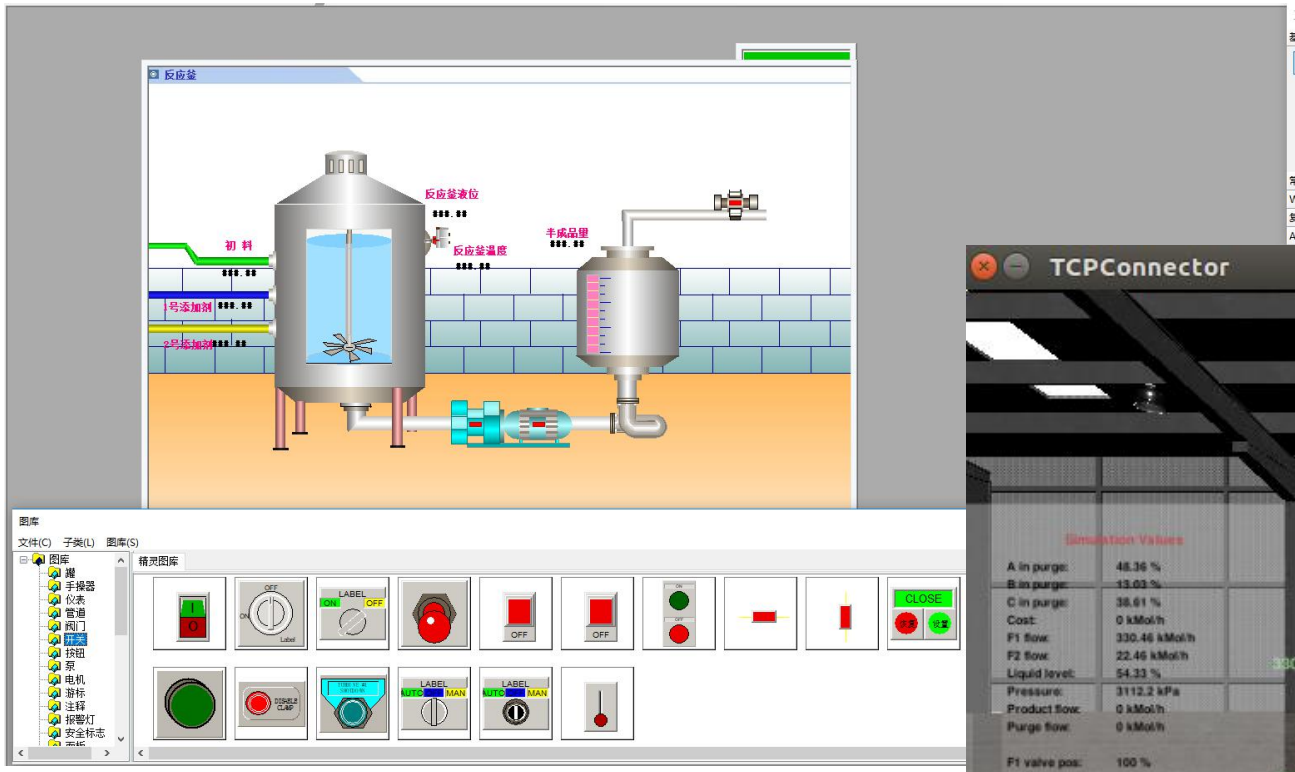
数据隐蔽传输方式

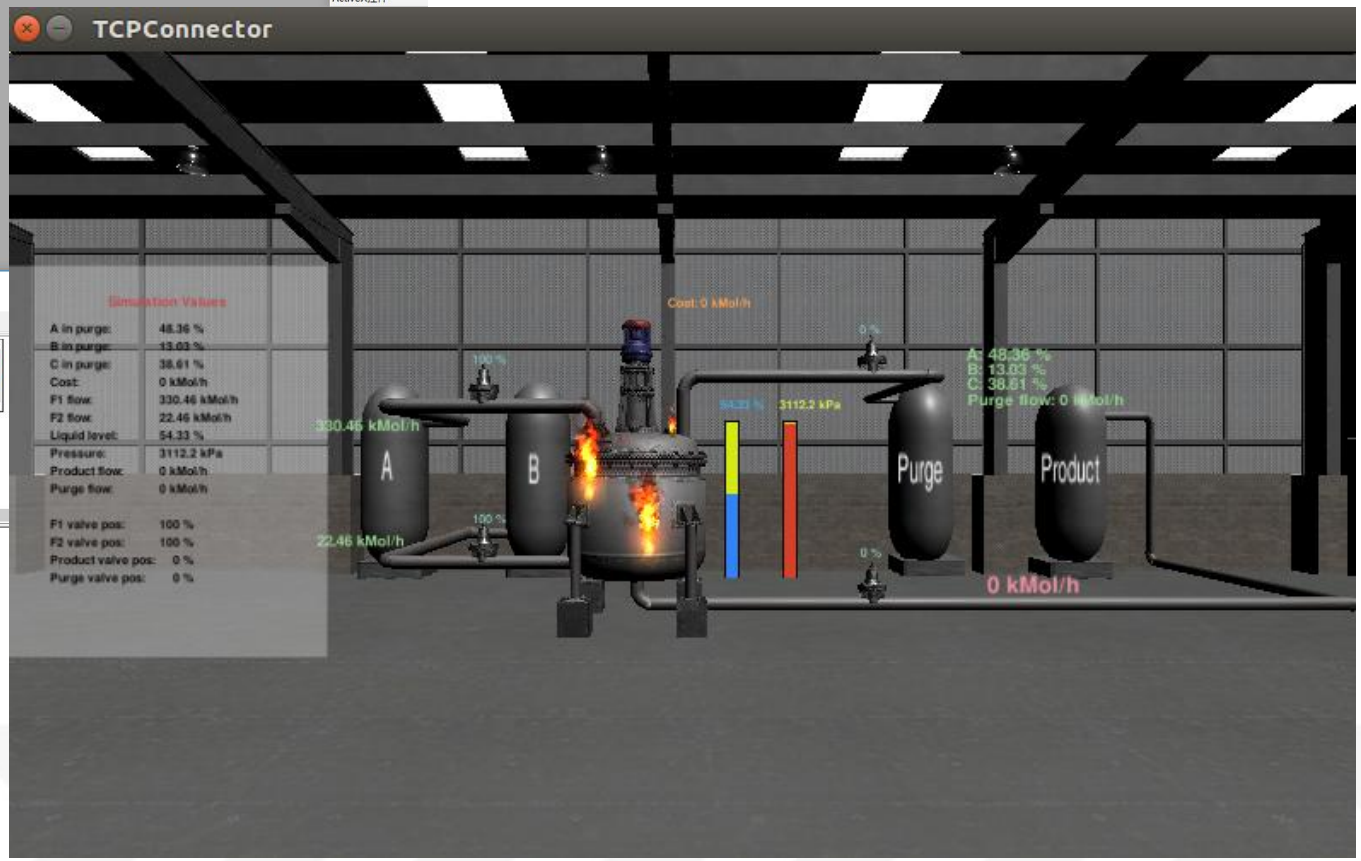
ICMP
DNS
ARP
LDAP
Powershell
WindowsDomWmi

WebDav
WebSocket
Https Proxy
JS混淆请求
Java RMI
图片像素加载
Ngrok内网穿透

DropBox
Office 365
Mail
Message App
OSS云存储
Jira等企业应用服务

工业现场攻击场景模拟


反应釜
反应釜液位
反应釜温度
半成品量
初 料
1号添加剂
2号添加剂
图库
文件(C) 子类(L) 图库(S)
精灵图库
CLOSE


TCPConnector
Simulation Values
A in purge: 48.36 %
B in purge: 13.03 %
C in purge: 38.61 %
Cost: 0 kMol/h
F1 flow: 330.46 kMol/h
F2 flow: 22.46 kMol/h
Liquid level: 54.33 %
Pressure: 3112.2 kPa
Product flow: 0 kMol/h
Purge flow: 0 kMol/h
F1 valve pos: 100 %
F2 valve pos: 100 %
Product valve pos: 0 %
Purge valve pos: 0 %
330.46 kMol/h
22.46 kMol/h
A
B
Purge
Product
0 kMol/h

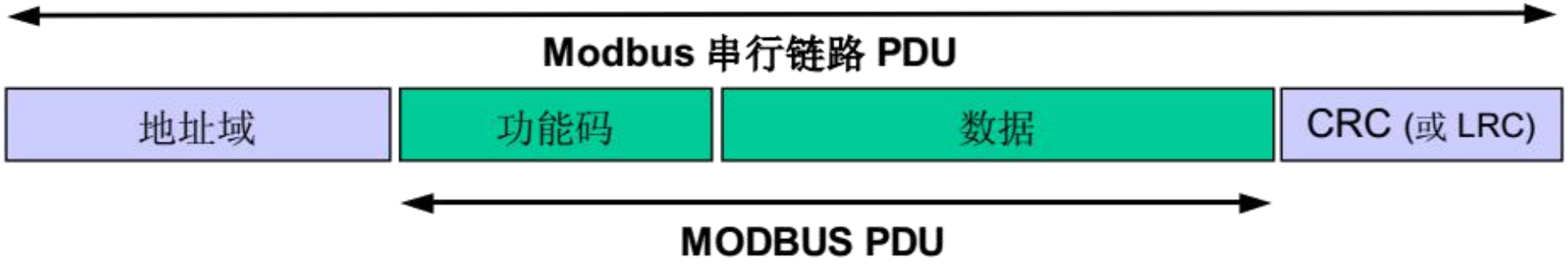
工业控制网络协议分析


文件(F) 编辑(E) 视图(V) 跳转(G) 捕获(C) 分析(A) 统计(S) 电话(Y) 无线(W) 工具(T) 帮助(H)
应用显示过滤器 … <Ctrl-/>
表达式…
数据包过滤器
No. Time Source Destination Protocol Length Info
1 0.000000 10.0.0.57 10.0.0.3 TCP 60 2387 → 502 [FIN, ACK] Seq=1 Ack=1 Win=64099 Len=0
2 0.000122 10.0.0.3 10.0.0.57 TCP 60 502 → 2387 [ACK] Seq=1 Ack=2 Win=65439 Len=0
3 0.000493 10.0.0.3 10.0.0.57 TCP 60 502 → 2387 [FIN, ACK] Seq=1 Ack=2 Win=65439 Len=0
4 0.000536 10.0.0.57 10.0.0.3 TCP 60 2387 → 502 [ACK] Seq=2 Ack=2 Win=64099 Len=0
5 2.751380 10.0.0.57 10.0.0.3 TCP 62 2578 → 502 [SYN] Seq=0 Win=64240 Len=0 MSS=1460 SACK_PERM=1
6 2.751546 10.0.0.3 10.0.0.57 TCP 62 502 → 2578 [SYN, ACK] Seq=0 Ack=1 Win=65535 Len=0 MSS=1460 SACK_PERM=1
7 2.751605 10.0.0.57 10.0.0.3 TCP 60 2578 → 502 [ACK] Seq=1 Ack=1 Win=64240 Len=0
8 15.266493 10.0.0.57 10.0.0.3 Modbus/TCP 66 Query: Trans: 0; Unit: 10, Func: 8/ 1: Force Listen Only Mode
数据包列表
Frame 8: 66 bytes on wire (528 bits), 66 bytes captured (528 bits) 物理层数据
Ethernet II, Src: Runtop_00:62:0d (00:20:78:00:62:0d), Dst: Intel_ce:70:51 (00:02:b3:ce:70:51) 链路层数据
Internet Protocol Version 4, Src: 10.0.0.57, Dst: 10.0.0.3 网络层数据
Transmission Control Protocol, Src Port: 2578, Dst Port: 502, Seq: 1, Ack: 1, Len: 12 应用层数据
Modbus/TCP
Transaction Identifier: 0
Protocol Identifier: 0
Length: 6
Unit Identifier: 10
Modbus
.000 1000 = Function Code: Diagnostics (8)
Diagnostic Code: Force Listen Only Mode (4)
Data: 0000
数据包信息
十六进制数据
0000 00 02 b3 ce 70 51 00 20 78 00 62 0d 08 00 45 00 ····pQ· x·b···E·
0010 00 34 85 83 40 00 80 06 61 05 0a 00 00 39 0a 00 ·4··@··· a····9··
0020 00 03 0a 12 01 f6 61 97 f1 83 70 f1 ad 1b 50 18 ·····a· ··p···P·
0030 fa f0 19 52 00 00 00 00 00 00 00 06 0a 08 00 04 ···R···· ········
0040 00 00 ··
数据包内容

工业控制网络协议Modbus功能码

代码	中文名称	作用
1	读取线圈状态	取得一组逻辑线圈的当前状态（ON/OFF)
2	读取输入状态	取得一组开关输入的当前状态（ON/OFF)
3	读取保持寄存器	在一个或多个保持寄存器中取得当前的二进制值
4	读取输入寄存器	在一个或多个输入寄存器中取得当前的二进制值
5	强置单线圈	强置一个逻辑线圈的通断状态
6	预置单寄存器	把具体二进值装入一个保持寄存器
7	读取异常状态	取得8个内部线圈的通断状态，这8个线圈的地址由控制器决定，用户逻辑可以将这些线圈定义，以说明从机状态，短报文适宜于迅速读取状态
8	回送诊断校验	把诊断校验报文送从机，以对通信处理进行评鉴
9	编程（只用于484）	使主机模拟编程器作用，修改PC从机逻辑
10	控询（只用于484）	可使主机与一台正在执行长程序任务从机通信，探询该从机是否已完成其操作任务，仅在含有功能码9的报文发送后，本功能码才发送
11	读取事件计数	可使主机发出单询问，并随即判定操作是否成功，尤其是该命令或其他应答产生通信错误时
12	读取通信事件记录	可是主机检索每台从机的ModBus事务处理通信事件记录。如果某项事务处理完成，记录会给出有关错误
13	编程（184/384 484 584）	可使主机模拟编程器功能修改PC从机逻辑
14	探询（184/384 484 584）	可使主机与正在执行任务的从机通信，定期控询该从机是否已完成其程序操作，仅在含有功能13的报文发送后，本功能码才得发送
15	强置多线圈	强置一串连续逻辑线圈的通断
16	预置多寄存器	把具体的二进制值装入一串连续的保持寄存器
17	报告从机标识	可使主机判断编址从机的类型及该从机运行指示灯的状态
18	（884和MICRO 84）	可使主机模拟编程功能，修改PC状态逻辑
19	重置通信链路	发生非可修改错误后，是从机复位于已知状态，可重置顺序字节
20	读取通用参数（584L）	显示扩展存储器文件中的数据信息
21	写入通用参数（584L）	把通用参数写入扩展存储文件，或修改之

数据单元部分的开发是最基本的部分，主要是2个方面的内容：一是生成客户端（主站）访问服务器（从站）的命令部分；二是生成服务器（从站）响应客户端（主站）回复部分。



Modbus协议的报文（或帧）的基本格式是：表头 + 功能码 + 数据区 + 校验码

功能码和数据区在不同类型的网络都是固定不变的，表头和校验码则因网络底层的实现方式不同而有所区别。表头包含了从站的地址，功能码告诉从站要执行何种功能，数据区是具体的信息。

工业控制网络协议Modbus指令与响应

从机地址	功能码	起始地址高位	起始地址低位	寄存器数量高位	寄存器数量低位	CRC高位	CRC低位
1	1	0	17	0	26	0D	D4

从机地址	功能码	返回字节数	数据1	数据2	数据3	数据4	数据5	CRC高位	CRC低位
1	1	5	CD	6B	B2	0E	1B	44	EA

1、根据协议控制规范或者捕获工业控制网络协议数据流来构造正常的数据包；
2、分析正常协议的字段及其重要性；
3、根据分析的协议中不同的数据类型，设计有效地变异策略；
4、设计并实现工业控制网络协议数据包发包工具；
5、设计并实现代理器及监视器；
6、采用发包工具，将畸形数据包发送给被测工控目标；
7、通过监视器探测被测工控目标异常记录。

工业互联网安全学习思路

工业互联网安全学习思路

一.工业控制系统组成及其架构概述

- 1）工业控制系统概念及其组成部件
- 2）工业控制系统体系架构
- 3）工业现场、网络环境常见威胁风险与解决方案

二.工业控制系统国家相关政策要求解析及合规建设

- 1）国家工业安全政策解析，包括不限于：
  《工业控制系统信息安全防护指南》
  《等级保护2.0工业控制系统扩展要求》
  《关键信息基础设施网络安全建设要求》
- 2）工业现场、网络环境安全合规建设

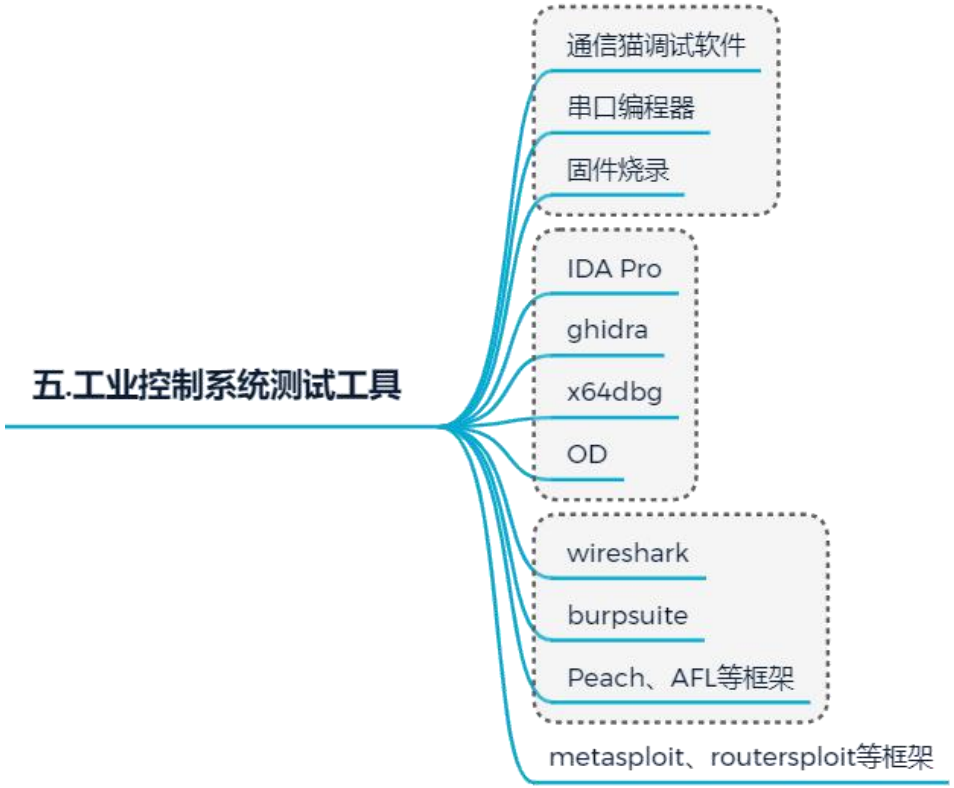
三.工业控制系统协议分析

- 对工业互联网协议、工控总线协议的解析，包括不限于：Modbus-Tcp、Profinet、Iec104、Modbus-Rtu、Profibus
- 工业协议对应报文内容、协议帧、功能码介绍

四.工业控制系统漏洞分析

- 工控设备状态控制
- 工控设备上传数据篡改
- 组态控制指令篡改
- 包括对控制设备、组态软件等设备的漏洞分析

工业互联网安全学习思路



工业互联网安全学习思路

网络安全创新大会
Cyber Security Innovation Summit

THANKS

ChaMD5