目录

工控安全概览

- 最新版本：`v1.0`
- 更新时间：`20210608`

简介

整理信息安全领域内的工控安全的基本介绍，包括工控协议，比如常见的Modbus、S7等，工控协议测试脚本，工控系统和产品，工控设备扫描检索网站和系统，工控漏洞和攻击，工控相关框架和工具，工控固件的提取和分析，工控无线协议，工控操作系统，工控的各个行业的安全等。

源码+浏览+下载

本书的各种源码、在线浏览地址、多种格式文件下载如下：

Gitbook源码

- crifan/industrial_control_security_overview: 工控安全概览

如何使用此Gitbook源码去生成发布为电子书

详见：crifan/gitbook_template: demo how to use crifan gitbook template and demo

在线浏览

- 工控安全概览 book.crifan.com
- 工控安全概览 crifan.github.io

离线下载阅读

- 工控安全概览 PDF
- 工控安全概览 ePub
- 工控安全概览 Mobi

版权说明

鸣谢

感谢我的老婆**陈雪**的包容理解和悉心照料，才使得我 `crifan` 有更多精力去专注技术专研和整理归纳出这些电子书和技术教程，特此鸣谢。

更多其他电子书

本人 `crifan` 还写了其他 `100+` 本电子书教程，感兴趣可移步至：

crifan/crifan_ebook_readme: Crifan的电子书的使用说明

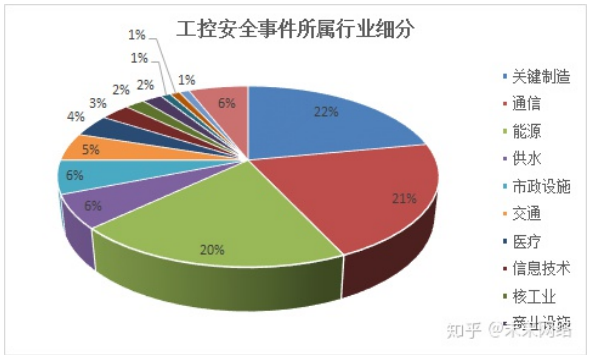
工控安全概览

如信息安全概览所总结，从技术领域分，信息安全大体可以分为：

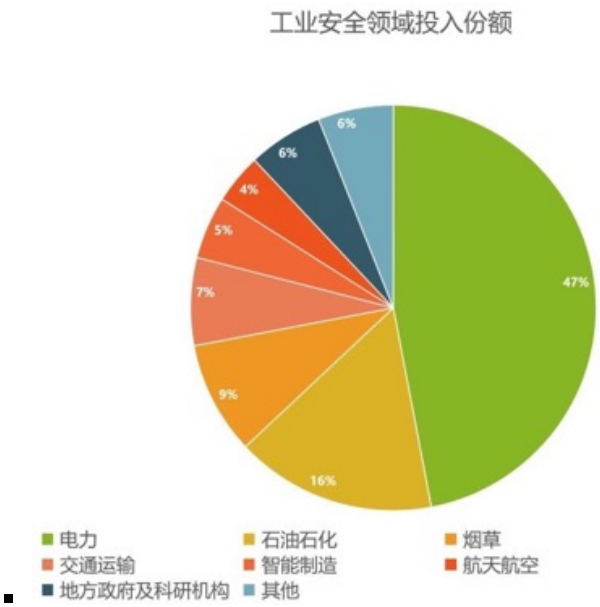
- Web安全
  - =网络安全
- 移动端安全
- 工控安全

此处主要介绍工控领域内的安全：

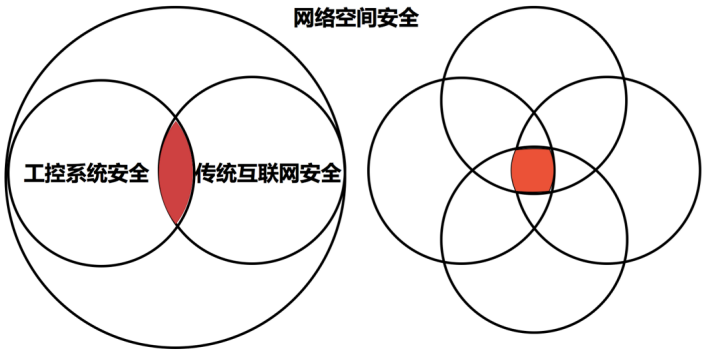
- 工控安全，即在工控领域的安全相关技术的统称
  - 工控，全称**工业控制**
    - 工业，包含很多行业
      - 按照工业4.0
        - 抽象概念
        - 

      - 工业控制的细分领域众多
        - 据调查近年来工控安全事件涉及超过 15 个行业
        - 

        - 但目前工控市场安全只覆盖到了其中部分行业，要实现全面防护还有许多路要走



- 工控安全和传统互联网安全关系



- 工控安全概况

工控安全子方向

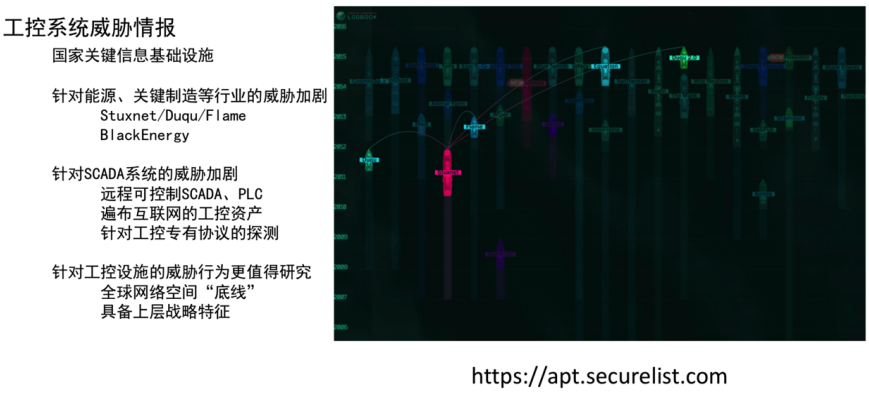
- 工控安全，其实也算是一个大的方向，其常见的具体的子方向包括
  - 工控固件逆向
    - 常涉及
      - Flash
        - 拆焊PCB版上的flash
        - 用编程器读取固件二进制
      - 架构
        - ARM
      - 系统
        - Linux
          - Linux kernel
          - Linux文件系统加密
          - uboot/grub
        - Vxworks
      - 固件
        - （固件）启动/加载地址
          - 魔数定位
          - 指令定位
        - 内存布局
        - 中断表地址
      - 分析工具
        - 反汇编
          - IDA PRO
            - switch 跳转表
          - Capstone
        - binwalk
        - rbasefind
  - 工业网络数据分析
  - 工控安全分析
  - 工业信息安全检测评估

工控威胁和情报

相关机构及关系

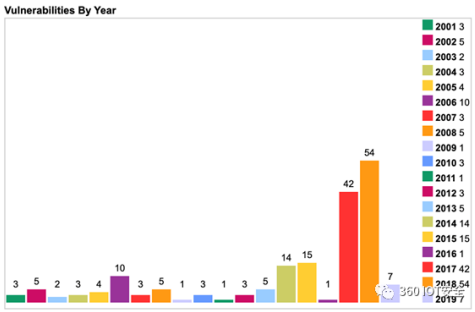
- 基础威胁情报(数据情报)
  - 流量/文件
  - BGP/AS/路由/Whois/指纹
  - Passive DNS/信誉数据
- 战术威胁情报(数据关联&分析)
  - 机读文件(IoC/TTP)
  - 情报落地、协作联动
- 战略威胁情报(价值&决策)
  - 可读报告
  - 意图分析、感知预测、决策支撑

工控系统威胁情报

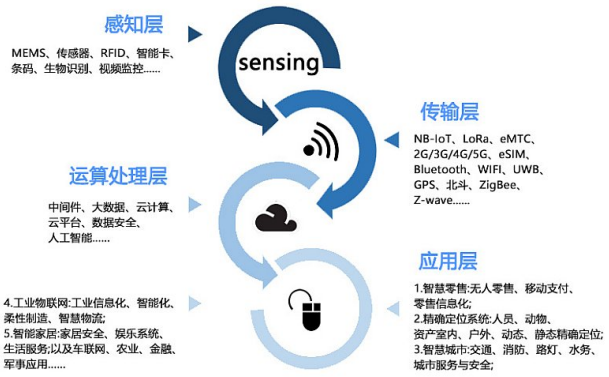


https://apt.securelist.com

物联网安全

- 物联网
  - 名称
    - 传统叫法：工控领域
    - 最新叫法：物联网
      - 万物互联的时代
  - 含义
    - 联网的嵌入式设备
  - 常见设备
    - 包含
      - 摄像头、路由器、无人机、智能家居、工控设备等
    - 特点
      - 大多数安全性都较低
      - 头部厂商
        - D-Link
          - 产品：路由器、摄像头
          - 安全事件频发
            - 被美国联邦贸易委员会（FTC）起诉
            - 统计
            - 

        - Axis
          - 摄像头设备
            - 被曝出过多起安全事件
              - 影响
                - 水电站、原油储备基地等，也被应用于学校、商业会议中心、机场等领域
          - 举例
            - ACE-128401
            - ACV-120444
  - 包含内容
    - 以IOTE2021国际物联网博览会为例来说明，物联网包含了哪些层面的内容
      - 图



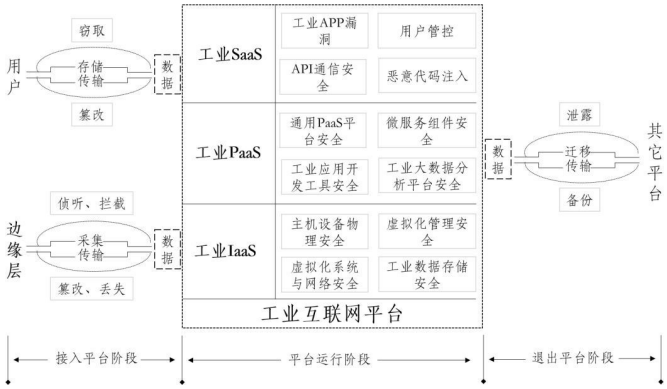
- 文字
  - 物联网感知层
    - MEMS、传感器、RFID、智能卡、条码、生物识别、视频、监控（摄像头）
  - 网络传输层
    - NB-IoT、LoRa、eMTC、2G/3G/4G/5G、eSIM、Bluetooth、WIFI、UWB、GPS、北斗、ZigBee、Z-wave.....
  - 运算处理层：
    - 中间件、大数据、云计算、云平台、数据安全、人工智能
  - 应用层
    - 1.智慧零售：无人零售、移动支付、零售信息化
    - 2.精确定位系统：人员、动物、资产室内、户外、动态、静态精确定位；
    - 3.智慧城市：交通、消防、路灯、水务、城市服务与安全；
    - 4.工业物联网：工业信息化、智能化、柔性制造、智慧物流；
    - 5.智能家居：家居安全、娱乐系统、生活服务；
    - 6.以及车联网、农业、金融、军事应用
  - 简单说，上述物联网内容，或多或少都和 `物联网安全` 、 `工控安全` 有所关联
- 物联网安全
  - 在和工控紧密相关的IoT物联网方面的安全，也被叫做：物联网安全

- 一些最佳实践
  - 关闭任何不必要的开放端口
  - 消除任何不需要的可信接口
  - 在设备基础架构和设计团队中实施最小特权原则
  - 禁用默认密码
  - 正确使用加密
  - 根据情况考虑使用安全硬件

工业互联网安全

- 工业互联网安全
  - 标准体系
    - 设备
    - 控制
    - 网络
      - 含标识解析系统
    - 平台
    - 数据
  - 平台
    - 国家工业互联网安全技术保障平台
    - 基础资源库
    - 安全测试验证环境
  - 重点领域
    - 汽车
    - 电子信息
    - 航空航天
    - 能源
  - 构建
    - 安全管理制度
      - 安全监督检查
      - 风险评估
      - 数据保护
      - 信息共享和通报
      - 应急处置
  - 分层
    - 边缘层
    - IaaS层（云基础设施）
    - 平台层（工业PaaS）
    - 应用层（工业SaaS）
  - 安全
    - 标识解析系统安全
    - 平台安全
    - 工业控制系统安全
    - 数据安全
    - 5G安全
  - 产品研发
    - 攻击防护
    - 漏洞挖掘
    - 态势感知
  - 人才
    - 缺口很大
  - 涉及多学科
    - 工业控制与自动化
    - 电子信息通信

        - 网络安全
    - 内容
        - 工控漏洞挖掘
        - 安全威胁感知
        - 网络攻防对抗与安全防护
    - 平台和工具
        - 工业互联网攻防演练靶场
        - 仿真测试平台
        - 安全资源库、工具集
            - 工业协议库
            - 安全漏洞库
            - 恶意代码病毒库
            - 安全威胁信息库
            - 安全应急处置
            - 安全事件现场取证
    - 安全能力
        - 工业资产探查能力
        - 工业设备漏洞挖掘与检测能力
        - 工业控制协议深度解析能力
        - 攻击发现和阻断能力
        - 高级持续威胁（APT）发现和追踪溯源能力
        - 网络安全攻防对抗能力
        - 源代码安全检测能力
        - 工业云平台防护能力
        - 工业大数据安全防护能力
        - 安全态势感知平台建设能力
        - 大数据建模和分析处理能力
        - 功能安全与信息安全融合能力
    - 针对主机的攻击方式
        - 通过网络攻击取得工业主机管理权限，加密关键文件，进行勒索
        - 通过U盘对工业主机注入病毒篡改控制器上报数据，掩盖控制数据异常
        - 通过鱼叉攻击实现多台工业主机提权，篡改下发控制指令
        - 通过感染双网卡工业主机跨区传播计算机病毒
        - 通过被控制的工业主机向控制器下发网络风暴数据，造成控制器运行周期异常甚至死机
    - 标准
        - 等保2.0
        - 分保
    - 工业互联网平台架构
        - 概述



- 工业互联网平台安全
  - 边缘层安全
  - 工业IaaS安全
  - 工业PaaS安全
  - 工业SaaS安全
  - 平台数据安全
- 现状
  - 重视不足
    - 网络安全投入占IT投入比重
      - 美国：10%
      - 中国：2%

工控协议

常见协议

常见协议总结

工控协议	传输协议	端口	说明
Modbus	TCP	502	工控常用协议，Modbus协议是应用 制器上的一种协议。通过此协议设 信。它已成为一通用工业标准。 详见：Modbus
Siemens S7	TCP	102	西门子PLC支持的通讯协议。属于 议，用于西门子设备之间进行交换 TSAP，可加载MPI,DP,以太网等不 总线或网络上，PLC一般可以通过 讯功能块实现。 s7协议是SIEMENS s7协议族的标 议，使用s7-应用接口的通信不依赖 线系统。 详见：Siemens S7
BACnet	TCP/UDP ?	47808	楼宇自动控制网络数据通讯协议。 制网络数据通讯协议（A Data Cor Protocol for Building Automation a Networks）。BACnet 协议是为计 暖、制冷、空调HVAC系统和其他 系统定义服务和协议。 楼宇自动控制网络数据通讯协议(B 对采暖、通风、空调、制冷控制设 同时也为其他楼宇控制系统（例如 保、消防等系统）的集成提供一个
ATG	TCP	10001	ATG，油罐液位仪，一种储油罐的 ATG（Automated-Tank-Gauge） 仪器的私有通讯协议
`IEC 104`	TCP	2404	输配电通讯协议。`IEC 104` = `IEC` `104` 是国际电工委员会制定的一个 适应和引导电力系统调度自动化的 调度自动化及远动设备的技术性能
`DNP3` = `DNP 3.0`	TCP/UDP	20000	`DNP` = `Distributed Network Protoc` 网络协议 是一种应用于自动化组件 协议，常见于电力、水处理等行业 络协议，主要用于电力行业。SCA 用DNP协议与主站、RTU、及IED 简化OSI模型，只包含了物理层， 用层的体系结构（EPA）
ICCP			电力控制中心通讯协议
OPC			过程控制的OLE （OLE for Proces Control）。OPC包括一整套接口、 法的标准集，用于过程控制和制造 统

工控协议	传输协议	端口	说明
OPC DA	TCP	135	OPC（OLE for Process Control, 用制的OLE）是一个工业标准。OPC 接口、属性和方法的标准集，用于制造业自动化系统。OPC DA基于OLE、COM和DCOM技术
OPC UA	TCP	4840	opc-ua tcp4840 port:4840 OPC-UA（Unified Architecture）是 OPC 标准，通过提供一个完整的、靠的跨平台的架构，以获取实时和时间。OPC UA不再依靠DCOM，向服务的架构 （SOA）
CIP			通用工业协议， 被 `DeviceNet` 、 `ControlNet` 、 `Eth` 种网络所采用
Tridium Niagara Fox	TCP	1911	Fox协议是Tridium公司开发的Niag一部分，广泛应用于楼宇自动化控
Crimson V3	TCP	789	
PCWorx	TCP	1962	PCWorx协议由菲尼克斯电气公司广泛使用于工控系统。PCWORX3克斯电气公司的专用协议
ProConOs	TCP	20547	ProConOS是德国科维公司(KW-S GmbH)开发的用于PLC的实时操作一个高性能的PLC运行时引擎，目于基于嵌入式和PC的工控系统
MELSEC-Q	TCP/UDP	tcp 5007 / UDP 5006	MELSEC-Q系列设备使用专用的网通讯，该系列设备可以提供高速、据处理和机器控制
`IEC-61850` = MMS + goose + SV	TCP	102	输配电通讯协议。IEC 61850标准自动化领域唯一的全球通用标准。的实现，实现了智能变电站的工程化。使得智能变电站的工程实施变一和透明
GE SRTP	TCP	18245	GE-SRTP协议由美国通用电气公司PLC可以通过GE-SRTP进行数据传输
CANopen			控制局域网通讯协定
`ONVIF`	UDP	3702	ONVIF协议的开发目的是通过全球口标准来推进网络视频在安防市场一接口标准将确保不同厂商生产的品具有互通性
工业现场总线			

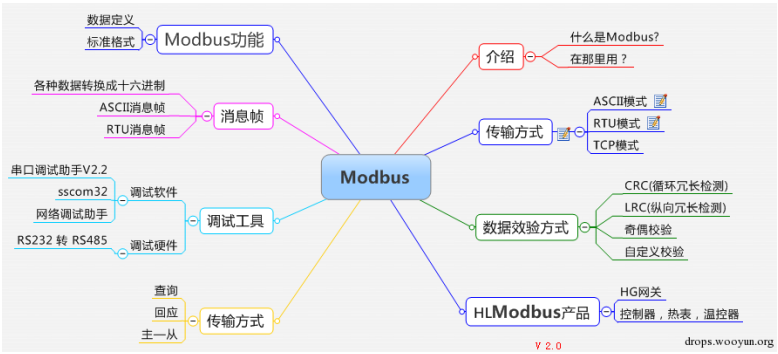
工控协议	传输协议	端口	说明
PROFIBUS			一种用于工厂自动化车间级监控和数据通信与控制的现场总线技术，设备层到车间级监控的分散式数字通信网络
EtherNet/IP	TCP/UDP	44818	Ethernet/IP是一个面向工业自动化应用层协议。它建立在标准UDP/I协议之上，利用固定的以太网硬件配置、访问和控制工业自动化设备应用层协议。 是一种CIP的实现方式，由罗克韦司开发的工业以太网通讯协定。
Profinet			开放式的工业以太网通讯协定
EtherCAT			德国Beckhoff公司推动的开放式实讯协定
HART-IP	TCP/UDP	5094	HART协议是美国Rosement公司于出的一种用于现场智能仪表和控制的通信协议。现已成为全球智能仪准
PLC通信协议			
MELSEC	TCP/UDP	TCP 5007 UDP 5006	三菱Q PLC支持的通讯协议
OMRON FINS	TCP/UDP	9600	欧姆龙PLC支持的通讯协定。欧姆网络协议FINS进行通信，可通过多理网络，如以太网、控制器连接等
EGD			GE Fanuc为PLC开发的通讯协定
Sinec H1			西门子PLC支持的通讯协议
无线协议			
mqtt			
zigbee			开放式的无线通讯协定
主流网络协议			
RTPS	TCP	554	RTSP协议是一种实时流传输协议义了一对多应用程序如何有效地通送多媒体数据
SIP	TCP	5060	SIP协议是由IETF制定的多媒体通SIP的开发目的是用来帮助提供跨高级电话业务

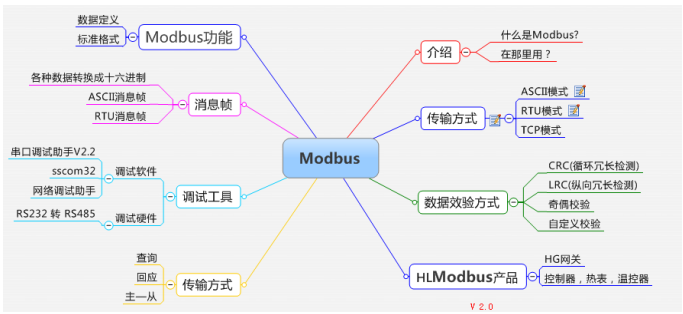
工控协议	传输协议	端口	说明
其他协议			
IEC 103			
Power Link			开放式实时以太网通信
FF HSE			基金会现场总线以太网通信协定
CoAP			轻量应用层协议
openSAFETY			开源安全应用协议
SERCOS III			实时以太网通讯协定
TTEthernet			实时以太网通讯协定
CDT			远动规约
KNXnet/IP			住宅和楼宇控制标准
Lontalk			埃施朗公司的LonWorks技术所使用 议
SAE J1939			一种CAN的变种，适用在农业车辆
USITT DMX512-A			灯光控制数据传输协议
BSSAP/BSAP			由Bristol Babcock Inc发展的通讯协
Gryphon			车用通讯协定
Doip			汽车诊断协议
AUTOSAR			汽车开放系统协议
redlion-crimson3	TCP	789	协议被Crimson桌面软件用于与Red G306工控系统的HMI人机接口
Fox	TCP	1911	Fox协议是Tridium公司开发的Niag 一部分，广泛应用于楼宇自动化控
secure-fox	TCP	4911	Fox协议是Tridium公司开发的Niag 一部分，广泛应用于楼宇自动化控
moxa-nport	UDP	4800	Moxa串口服务器专为工业应用而设 配置组合的串口服务器更能符合不 的需求。NPort系列串口服务器让你 232/422/485设备立即联网，提供您 串口联网解决方案
CoDeSys	TCP	2455	CoDeSys编程接口在全球范围内使 球上百个设备制造商的自动化设备 该编程接口

工控协议	传输协议	端口	说明
ddp	TCP/UDP	5002	DDP协议（DTU DSC Protocol）是 DSC之间的通讯协议，DDP是一种 私有公开性质的通信协议，用于数 DTU管理
lantronix-udp	TCP	30718	Lantronix串口服务器专为工业应用 口服务器是一种具有串口转以太网 备，它能将RS-232/485/422串口转 TCP/IP网络接口，串口服务器广泛 SCADA数据采集环节上，用于解决 太网的通信问题
wdbrpc	TCP	17185	VxWorks是世界上使用最广泛的一 系统中部署的实时操作系统，是由 WindRiver公司于1983年设计开发 VxWorks系统在工业控制领域应用 WDB RPC是VxWorks的远程调试
dahua-dvr	TCP	37777	DAHUA-DVR协议是浙江大华安防 私有通信协议，该协议用于实时视 输
vstarcam-udp	UDP	8600	VSTARCAM-UDP协议是威视达康 备的私有通信协议该协议用于获取 备的网络配置等信息
CSPV4	TCP	2222	CSPV4是可以识别PLC5/SLC 500 务；罗克韦尔的SLC 500功能强大 的指令集、丰富的输入输出模块， 业现场恶劣的工作环境而设计
general-electric-srtp	TCP	18245	GE-SRTP协议由美国通用电气公司 PLC可以通过GE-SRTP进行数据通 传输
私有协议			
bachmann-tcp	TCP	3500	Bachmann是一种私有协议，用于 PLC的通讯，常见于风力发电等行
bachmann-udp	UDP	3003	Bachmann是一种私有协议，用于 PLC的通讯，常见于风力发电等行
beckoff-ads	UDP	48899	Beckoff-ads是一种私有协议，用于 PLC的通讯，常见于风力发电等行
hollysys-lk	UDP	6000	Hollysys-lk协议是一种私有协议， Hollysys PLC的通讯，常见于电力 工等行业
hollysys-macs	UDP	8000	Hollysys-macs协议是一种私有协议 Hollysys DCS的通讯，常见于电力 工等行业

工控协议	传输协议	端口	说明
siemens-license	TCP	4410	Siemens License协议是一种私有 西门子上位机软件的License服务
igss	TCP	12397	IGSS协议是一种私有协议，用于 IGSS（Interactive Graphical SCA System）软件之间的通讯
foxboro	TCP	20476	Foxboro是一种私有协议，用于Fo 的通讯，常见于电力、石油、化工
ilon-smartserver	TCP	1628	ILON-SMARTSERVER协议是ECI 生产的iLon系列产品的私有通信协 列产品可以广泛的应用于工业控制 SmartServer类似于一台服务器， 发，数据存储等作用

Modbus

- `Modbus`
  - MODBUS协议定义了一个与基础通信层无关的简单协议数据单元（PDU）。特定总线或网络上的MODBUS协议映射能够在应用数据单元（ADU）上引入一些附加域。
  - 

  - 安全问题：
    - 缺乏认证：仅需要使用一个合法的Modbus地址和合法的功能码即可以建立一个Modbus会话
    - 缺乏授权：没有基于角色的访问控制机制， 任意用户可以执行任意的功能。
    - 缺乏加密：地址和命令明文传输， 可以很容易地捕获和解析
- Modbus=Modbus协议
  - 历史和背景
    - Modicon公司1979年发行
    - 工业控制已从单机控制走向集中监控、集散控制，如今已进入网络时代，工业控制器连网也为网络管理提供了方便
    - Modbus 就是工业控制器的网络协议中的一种
    - 2004年，中国国家标准委员会正式把Modbus作为了国家标准，开启了Modbus为中国工业通信做贡献的时代
  - 现状
    - 已经被广泛应用于工业控制现场的应用层协议
      - 监控和控制现场设备
  - 协议
    - 概述
    - 

    - 种类

        - 串口上的：Modbus Serial协议
        - TCP/IP 以太网上 上的：Modbus TCP协议=Modbus/TCP协议

Modbus Serial协议

- Modbus Serial协议
  - 解释
    - 在物理层面上选择串口进行简单的串行通信
    - 最初是为了实现串行通信，运用在串口（如RS232、RS485、RS422等）传输上的，分为ModbusRTU、Modbus ASCII两种
    - Modbus协议最初是通过串行数据进行通信的，也就是Modbus Serial协议
  - 包含
    - Modbus ASCII
      - 特点
        - 通讯是普通文本=ASCII？
      - Modbus ASCII 常用的报文格式
        -

起始位	设备地址	功能代码	数据区	LRC 校验	结束符
1 个字节	2 个字节	2 个字节	n 个字节	2 个字节	2 个字节
:					CR LF（回车 换行）

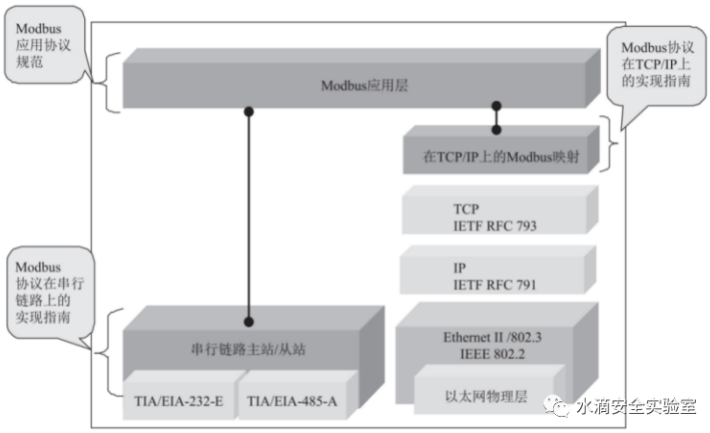
    - Modbus RTU
      - RTU=Remote Terminal Unit
        - RTU通信就是通过模拟远程终端设备读写寄存器
      - 特点
        - 通讯是二进制？
      - Modbus RTU 常用的报文格式
        -

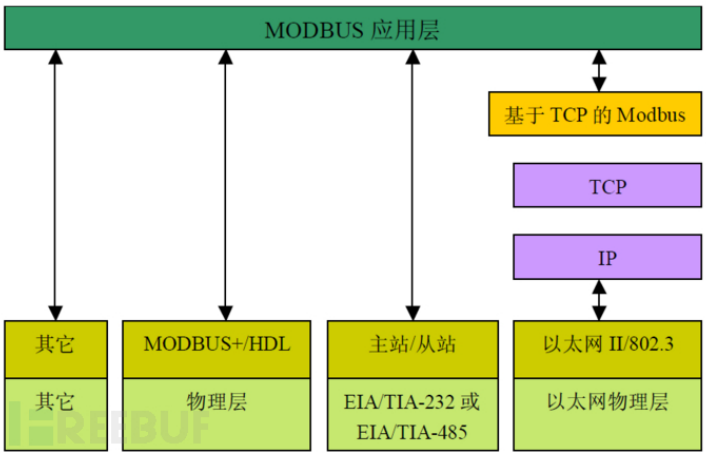
起始位	设备地址	功能代码	数据区	CRC校验
T1T2T3..	1个字节	1个字节	n个字节	2个字节

  - 架构
    - 一主多从架构
      - 主站发起请求，从站负责响应

Modbus TCP协议

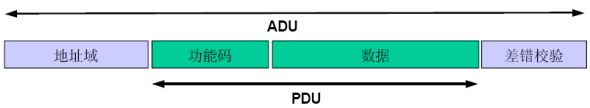
- Modbus TCP协议
  - 协议栈
    - Modbus TCP一种应用层消息传递协议，位于OSI模型的第7级

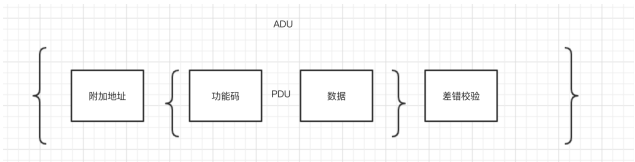


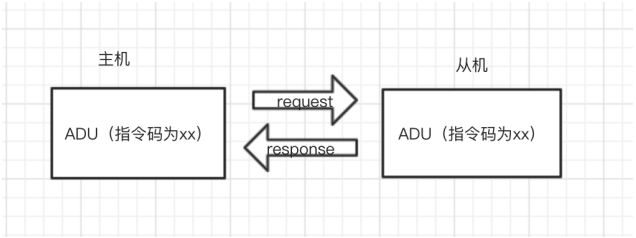


Layer	ISO/OSI Model	
7	Application	MODBUS Application Protocol
6	Presentation	Empty
5	Session	Empty
4	Transport	Empty
3	Network	Empty
2	Data Link	MODBUS Serial Line Protocol
1	Physical	EIA/TIA-485 (or EIA/TIA-232)

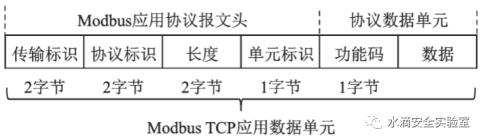
- 协议细节
  - 帧格式
    - 两种帧格式
      - 802.3
      - Ethernet II
    - 数据帧
      - 概述



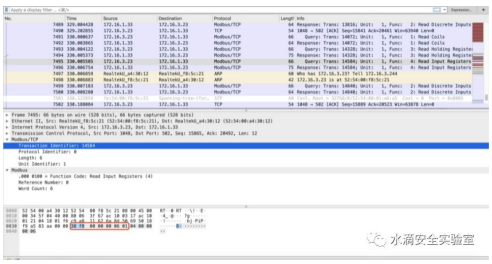




- 包含
  - MBAP 报文头
    - 4 分内容， 7 个字节
    - 报文格式
      - 图



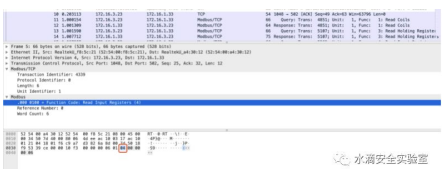
      - 举例
        - Modbus/TCP
          - Transaction Identifier: 89 //数据包序号
          - Protocol Identifier: 0 //数据协议类型
          - Length: 9 //Modbus协议长度
          - Unit Identifier: 1 //目的设备ID
        - Modbus
          - Function Code: Write Multiple Coils (15) //功能码
          - Reference Number: 0 //线圈储存当前地址偏移量
          - Bit Count: 10 //一共10位
          - Byte Count: 2 //以两个字节发送
          - Data: c403 //按位转为16进制的多线圈数据
      - 包含
        - 传输标识
          - 2 个字节
          - 传输中的序列号
          - 生成该序列号的对应的传输形式是 Query
          - 响应是复制该序列号就是 Response
        - 协议标识
          - 2 个字节
          - 采用 Modbus 时为 0 （即 00 00 ）
          - 采用 UNI-TE 时为 1
        - 后续字节长度
          - 2个字节
          - 代表后续字节数
        - 单元标识
          - 1个字节
          - 代表 Modbus RTU 中的地址码
      - 举例



- 上图中 MBAP
  - 传输标识： 38 f8
  - 协议标识：Modbus 协议为 00 00
  - 后续字节长度为 00 06 后续有 6个字节长度
  - 单元表示为 01，代表查询 RTU 的地址码为 01
- 功能码
  - 1个字节
  - 分类
    - 按照用途分3类
      - 概述

				功能码		
				码	子码	（十六进制）
数据访问	比特访问	物理离散量输入	读离散量输入	02	--	02
		内部比特或物理线圈	读线圈	01	--	01
			写单个线圈	05	—	05
			写多个线圈	15	—	0F
	16 比特访问	输入寄存器	读输入寄存器	04	—	04
		内部存储器或物理输出存储器	读多个寄存器	03	-	03
			写单个寄存器	06	—	06
			写多个寄存器	16	—	10
			读/写多个寄存器	23	—	17
			屏蔽写寄存器	22	--	16
			读 FIFO 队列	24	—	18
	文件记录访问		读文件记录	20	6	14
			写文件记录	21	6	15
诊断			读异常状态	07	—	—
			诊断	08	00-18	—
			获得公用事件计数器	11	—	0B
			获得公用事件记录	12	—	0C
			报告从站 ID	17	—	11
			读设备识别码	43	14	2B
其他			封装接口传输			

      - 包含
        - 公共功能码
          - 为已被定义好的一致的、唯一的、公开的功能码
        - 用户自定义功能码
          - 为用户自行定义的功能码，在区间 65-72 和 100-110
        - 保留功能码
          - 留作扩展功能备用 22-64，留作内部作用 120-127，留作异常应答 128-255
      - 举例



        - Modbus 流量中的 04 读输入寄存器功能码
- 数据

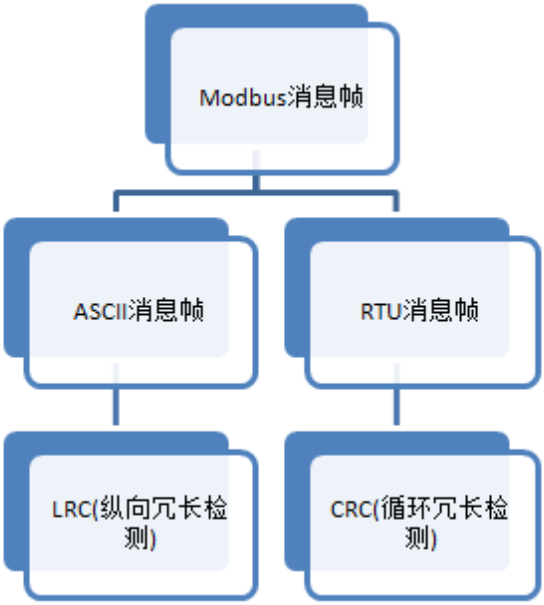
- 解释
  - 使用TCP的方式进行传输
  - 随着工业现代化的发展，产生了Modbus TCP协议，即通过与TCP协议相结合来发送和接收Modbus Serial数据。
  - 后来施耐德电气将该公司收购，并在1997年推出了基于TCP/IP的Modbus TCP。现在使用最多的就是Modbus TCP了
  - Modbus的协议栈仅仅是在传统ISO/OSI模型的基础上对数据链路层和应用层做了定义
- 应用
  - 广泛应用于电力、水力等工业系统
- 漏洞
  - 产生机制
    - 正是因为modbus是应用层的协议，所以它的安全漏洞并不只是它本身，TCP/IP的漏洞也可以利用在modbus上
  - 案例
    - 最典型的就是18年工控比赛的题目，中间人
- 架构
  - 主从架构
    - 举例
      - Master：HMI=人机界面，监控系统等
      - Slave：PLC
    - 或
      - Master：主PLC
      - Slave： PLC 、 HMI 、 I/O设备、传感器、执行器，电表、仪表等
- 部署
  - 典型的部署方式
    - 在 SCADA 区域使用 Modbus TCP 对主 HMI 和主 PLC集中管理
    - 各 PLC 则通过总线拓扑串联多个 PLC 、 HMI 和 RTU 等
- 协议 报文 细节
  - PDU=Protocol Data Unit=协议数据单元
  - ADU=数据单元
    - 与基础网络无关
  - ASCII模式
    - 表1 ASCII帧

开始	地址	功能	数据	纵向冗余检查	结束
1字符	2字符	2字符	n字符	2字符	2字符

  - RTU模式
    - 表2 RTU帧

开始	地址	功能	数据	校验	终止
T1-T2-T3-T4	8B位S	8B位S	N×8B位S	16B位S	T1-T2-T3-T4

  - 通用消息帧



- modbus功能码
  - 概述
    - 通过功能码主设备能够对从设备下达指令
    - 功能码有效范围：1~255
  - 公共功能码分类

表3 公共功能码分类

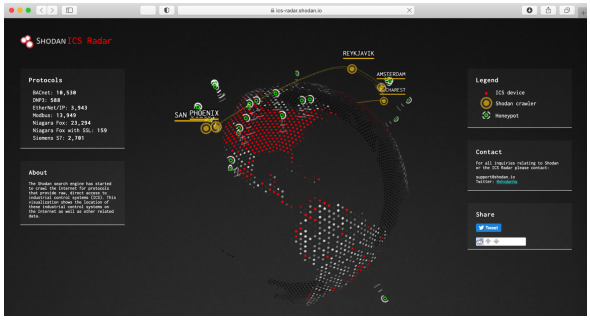
基本表格	对象类型	访问类型	内容
离散量输入	单个比特	只读	I/O系统提供这种类型数据
线圈	单个比特	读写	通过应用程序改变这种类型数据
输入寄存器	16比特字	只读	I/O系统提供这种类型数据
保持寄存器	16比特字	读写	通过应用程序改变这种类型数据

  - 公共功能码定义

表4 公共功能码定义

				功能码			
				码	子码	(十六进制)	页
数据访问	比特访问	物理离散量输入	读输入离散量	02		02	11
		内部比特或物理线圈	读线圈	01		01	10
			写单个线圈	05		05	16
			写多个线圈	15		0F	37
	16比特访问	输入存储器	读输入寄存器	04		04	14
		物理输出存储器	读多个寄存器	03		03	13
			写单个寄存器	06		06	17
			写多个寄存器	16		10	39
			读/写多个寄存器	23		17	47
			屏蔽写寄存器	22		16	46
	文件记录访问		读文件记录	20	6	14	42
			写文件记录	21	6	15	44
封装接口			读设备识别码	43	14	2B	

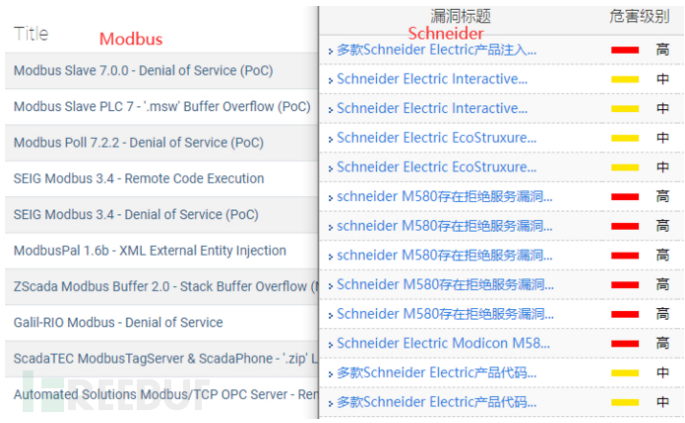
  - 举例
    - 01 读线圈状态
    - 02 读离散输入状态
    - 03 读保持寄存器

        - 04 读输入寄存器
        - 05 写单个线圈
    - 使用分布
        - SHODAN搜集协议使用分布区域的动态立体图
            - Shodan - ICS Radar
                - https://ics-radar.shodan.io
                - 

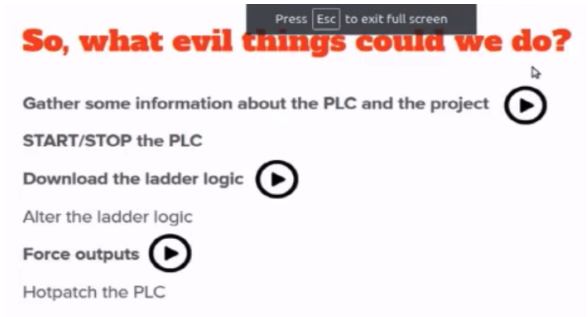
    - 安全方面
        - Modbus的出现是为了使工业现场设备实时地接收和发送相关命令和数据，然后最重要的安全措施在Modbus的设计之初并没有被考虑进去
        - 原因：
            - Modbus TCP 协议设计时，考虑的应用场景是外界隔离的工业以太网，更多的考虑的是 Modbus TCP 协议的可靠性、实时性和传输效率，基本没有考虑协议的安全性
    - Modbus协议缺陷
        - 没有认证机制
            - 缺乏认证导致攻击者容易获取 Modbus TCP 信息，并且攻击者只要使用有效的功能码和地址，就可以冒充主控端操控 Modbus 设备
        - 传输内容没有加密
            - 直接以明文的形式传输命令和地址，能够被攻击者轻易捕获、解析和重放，目前已经有了 N-Modbus TCP 协议基于 SSL 解决这个问题，但是传输效率降低
        - 可编程性
            - Modbus 协议的 salve 端多为可编程逻辑控制单元，攻击者发出的恶意攻击代码可以直接控制 PLC 或者 RTU 等工控设备
    - Modbus攻击面=攻击方式
        - 通过扫描的方式
            - 获取网络中主 / 从设备的地址、开放端口等信息。嗅探网络中的数据包，获取控制指令、设备参数等工业敏感信息。
        - 前期通过公网渗透进入工业网络环境中后，模拟主 / 从设备发送恶意指令，造成设备错误操作，破坏工控流程
            - 例如：在攻击者得到主从设备的网络配置后，仿冒主设备的地址信息，构造功能码令从设备强制重启；构造功能码修改寄存器的值，导致控制器做出错误决策；
        - 模拟从设备给主设备发送错误码，致使主设备判断逻辑发生错误
            - 例如：攻击者模拟某个 PLC 给从设备发送 04 错误码，告诉主设备从设备故障，如果此时主设备的顶层逻辑是启用备份设备，对于某些压力工厂风险是巨大的。
                - 错误码

代码	名称	含义
01	非法功能	对于服务器（或从站）来说，询问中接收到的功能码是不可允许的操作，可能是因为功能码仅适用于新设备而被选单元中不可实现同时，还指出服务器（或从站）在错误状态中处理这种请求，例如：它是未配置的，且要求返回寄存器值。
02	非法数据地址	对于服务器（或从站）来说，询问中接收的数据地址是不可允许的地址，特别是参考号和传输长度的组合是无效的。对于带有100个寄存器的控制器来说，偏移量96和长度4的请求会成功，而偏移量96和长度5的请求将产生异常码02。
03	非法数据值	对于服务器（或从站）来说，询问中包括的值是不可允许的值。该值指示了组合请求剩余结构中的故障。例如：隐含长度是不正确的。modbus协议不知道任何特殊寄存器的任何特殊值的重要意义，寄存器中被提交存储的数据项有一个应用程序期望之外的值。
04	从站设备故障	当服务器（或从站）正在设法执行请求的操作时，产生不可重新获得的差错。
05	确认	与编程命令一起使用，服务器（或从站）已经接受请求，并且正在处理这个请求，但是需要长持续时间进行这些操作，返回这个响应防止在客户机（或主站）中发生超时错误，客户机（或主机）可以继续发送轮询程序完成报文来确认是否完成处理。
07	从属设备忙	与编程命令一起使用，服务器（或从站）正在处理长持续时间的程序命令，当服务器（或从站）空闲时，客户机（或主站）应该稍后重新传输报文。
08	存储奇偶性差错	与功能码20和21以及参考类型6一起使用，指示扩展文件区不能通过一致性校验。服务器（或从站）设备读取记录文件，但在存储器中发现一个奇偶校验错误。客户机（或主机）可重新发送请求，但可以在服务器（或从站）设备上要求服务。
0A	不可用网关路径	与网关一起使用，指示网关不能为处理请求分配输入端口值输出端口的内部通信路径，通常意味着网关是错误配置的或过载的。
0B	网关目标设备响应失败	与网关一起使用，指示没有从目标设备中获得响应，通常意味着设备未在网络中。

- 安全问题=漏洞
  - 包含
    - 拒绝服务Dos攻击
    - 远程代码执行
    - 堆栈缓冲区溢出
    - 中间人攻击
      - 传统TCP/IP存在的问题
        - 举例
          - 18年的中间人攻击
    - 其他操作
      - 读写线圈和寄存器
  - 举例



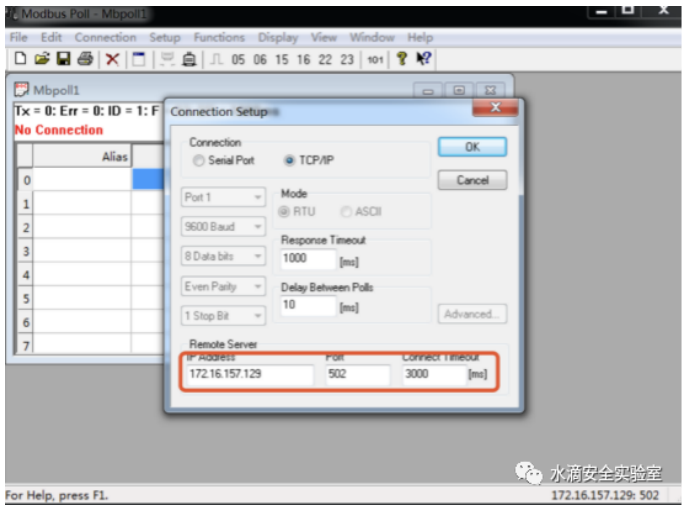
  - 具体案例
    - 工控安全入门（一）—— Modbus协议 - 安全客，安全资讯平台
      - https://www.anquanke.com/post/id/185513
        - 2019工控安全比赛 线上赛第一场 Modbus题目（第一版）
          - 19年的第一版，施耐德的高危功能码，这是非常难的
            - 从之前的分析可以看到这些保留的功能码在厂商自定义后对于我们普通的参赛选手来说是很难真正读懂流量包的，需要配合相应的正向使用知识，和正向使用的流量包来进行学习
        - 2019工控安全比赛 线上赛第一场 Modbus题目（第二版）
      - Modbus在施耐德设备上的一个重要漏洞
        - defcon上展示过的fun with 0x5a

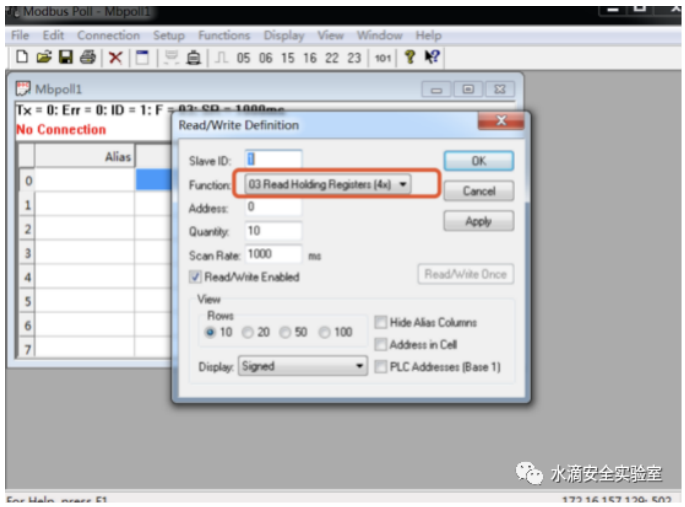


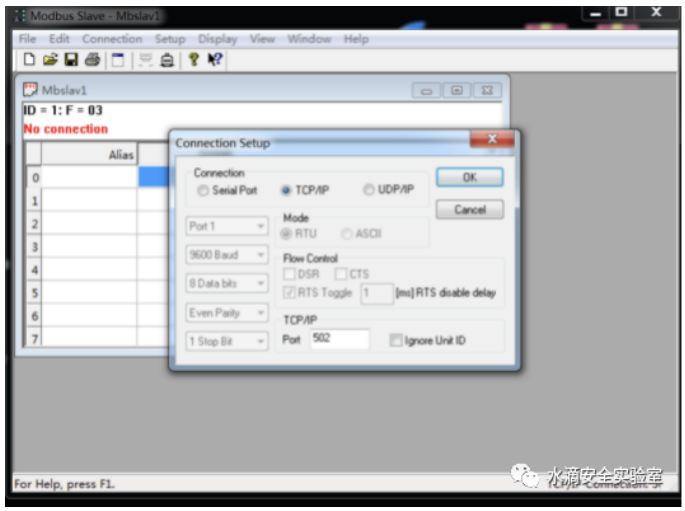
        - Modbus题目解析
            - Modbus协议与S7Comm协议浅析 - Sec' Hotspot
                - https://sec.thief.one/article_content?a_id=186aecd7d905fd606076bc50e51919db
                    - 黑客通过外网进入一家工厂的控制网络，之后对工控网络中的操作员站系统进行了攻击，最终通过工控协议破坏了正常的业务。我们得到了操作员站在攻击前后的网络流量数据包，我们需要分析流量中的蛛丝马迹，找到FLAG

Modbus工具

- Smod
    - 简介
        - 一个模块化的Modbus渗透测试框架，可以用来测试Modbus协议所需的各种诊断和攻击功能。这是一个使用Python和Scapy的完整的Modbus协议实现。
    - 支持系统： Linux / OSX
    - 版本：python 2.7.x
    - 模块
        - modbus-discover.nse（nmap自带）识别并发现Modbus PLCS设备及版本
        - modicon-info.nse（需添加）识别并列举Schneider Electric Modicon PLC
        - modbus-enum.nse （需添加）识别并枚举使用Modbus的设备
    - 功能
        - 暴力破解PLC的UID
        - 网络嗅探进行ARP地址欺骗
        - 枚举Modbus PLC的功能
        - 模糊读写单一或多个线圈功能
        - 模糊读写单一或多个输入寄存器功能
        - 测试读写单一或多个保持寄存器功能
        - 测试单个PLC 所有功能
        - 对单个或多个线圈写值进行Dos攻击
        - 对单个或多个寄存器写值进行Dos攻击
        - 对ARP地址欺骗进行Dos攻击
    - 命令
        - show modules
            - 查看有哪些功能模块

        - use /modbus/scanner/uid
        - /modbus/scanner/getfunc
- Modbus Poll/Salve模拟器
    - 包含组件
        - 服务端模拟器Modbus Poll(可设置虚拟IP 地址，常用请求功能码，任意大小的内存)
            - 

            - 

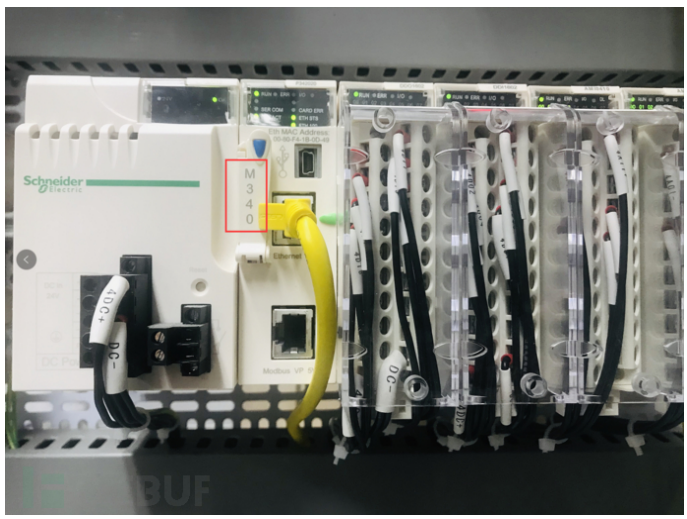
        - 客户端模拟器Modbus Slave
            - 

        - Modbus_RSsim(可读取协议数据段数据)

- ISF
  - 相关
    - 【整理】工控系统渗透方法和工具
  - 其中就有
    - plc相关的扫描
      - ### 三、Modules

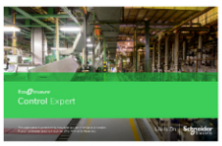
Name	Desc
Schneider_CPU_Command	Control Schneider PLC CPU start or stop
Siemens_300_400_CPU_Control	Control Siemens PLC-300 and PLC-400 CPU start or stop
Siemens_1200_CPU_Control	Control Siemens PLC-1200 CPU start or stop
Modbus_PLC_Injecter	Modbus PLC injecter tools
plcscan	Modbus and S7 PLC scanner tools
lantronix_telnet_password	Recover lantronix telnet password
Siemens_1200_Control	Control Siemens PLC

相关

- SummerySCADA
  - 过程控制网络
- 常见PLC
  - Schneider（施耐德）PLC M340
    - 简介
      - Modicon M340是全球能效管理专家施耐德电气于2007年推出的高性能中型PLC平台，拥有“精巧、可靠、创新、易用、高性价比”等诸多新亮点，适用于中小型项目、复杂机械及过程装备
    - 图
      - 
    - 上位机编程软件：EcoStruxure Control Expert

Product data sheet
Characteristics

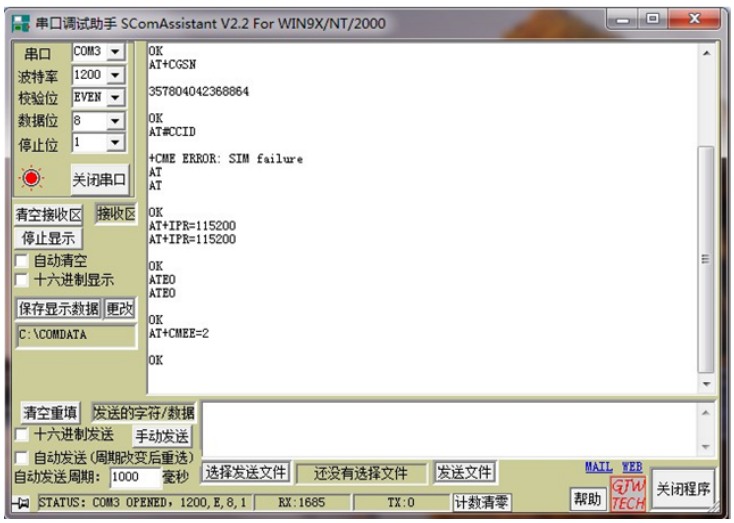
CEXPACKAGEV14
Software package, EcoStruxure Control Expert, for all sizes : S, L, XL and safety



Main

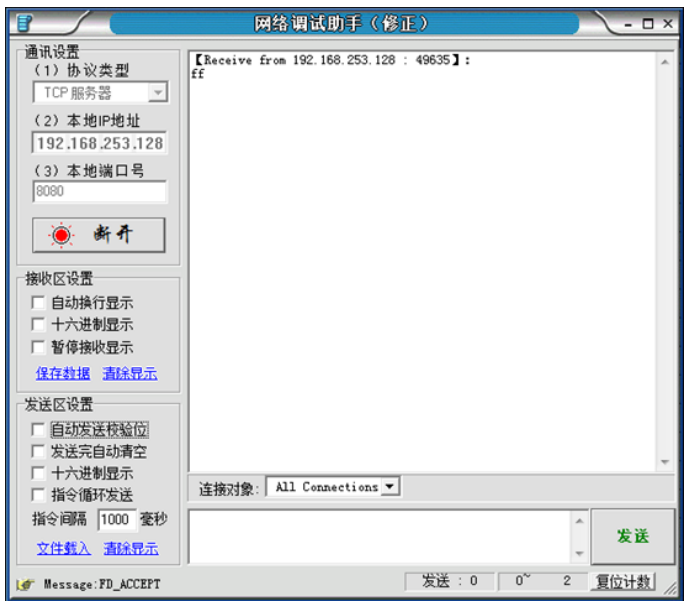
Range of product	EcoStruxure Control Expert
Product or component type	Software package
Language	Italian Chinese Spanish English German French
Format	DVD-ROM

- 主站
  - 
- 从站
  - 
- 西门子 S7系列
  - 上位机编程软件：博途

- 串口工具
  - 虚拟串口工具
    - VSPD=Virtual Serial Port Driver
      - 9.0 by Eltima Software
  - 串口调试工具的使用
    - 

    - 串口调试工具 + RS485

- 网络调试助手



- Python
  - Python的modbus_tk库
- 防御
  - 建议：一个Modbus协议系统里需要多层次的安全防御手段
  - 手段
    - 流量异常行为检测
    - 身份认证和授权
      - 只有可信任的设备，才能接入工控系统网络，且需要进行身份认证，确保登陆者也是可信任者
        - 背景
          - modbus根本没有认证方面的定义，攻击者需要的仅仅是一个合适的ip地址而已，至于授权更是无从谈起，加

密方面也是漏洞百出

    - 日志记录和安全审计
        - 记录操作的时间、地点、操作者和操作行为等关键信息从而提供安全事件爆发后的追查能力
    - （企业）要定期对工控系统进行漏洞扫描
        - 及时修补漏洞更新软硬件
    - 安全设计
        - 需要注意 功能码滥用
- 由Modbus从设备提供给Modbus主设备的对象类型

Object type	Access	Size	Address Space
线圈Coil	Read-write	1 bit	00001 - 09999
离散输入Discrete input	Read-only	1 bit	10001 - 19999
输入寄存器Input register	Read-only	16 bit	30001 - 39999
保持寄存器Holding register	Read-write	16 bit	40001 - 49999

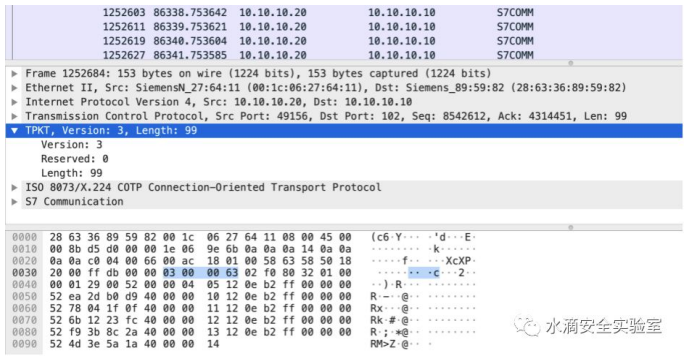
Siemens S7

- `Siemens S7` = `S7Comm` = `西门子S7` (协议)
  - 介绍
    - 德国西门子公司生产的 `PLC` 与 `SCADA` 系统进行通信的私有协议
    - `S7` 被封装在 `TPKT` 和 `ISO-COTP` 协议中，基于 TCP 协议， S7 的协议传输单元能够通过 TCP 传送
  - 协议栈

OSI layer Protocol	OSI layer Protocol
7 Application Layer S7 communication	7 Application Layer S7 communication
6 Presentation Layer S7 communication (COTP)	6 Presentation Layer S7 communication (COTP)
5 Session Layer S7 communication (TPKT)	5 Session Layer S7 communication (TPKT)
4 Transport Layer ISO-on-TCP (RFC 1006)	4 Transport Layer ISO-on-TCP (RFC 1006)
3 Network Layer IP	3 Network Layer IP
2 Data Link Layer Ethernet	2 Data Link Layer Ethernet
1 Physical Layer Ethernet	1 Physical Layer Ethernet

基于OSI模型的S7Comm协议

  - `TPKT` 协议层
    - 会话层的 TPKT 协议是应用程序数据传输协议，介于 TCP 协议和 COTP 协议之间， windows 常用的远程桌面协议 RDP 也是基于 TPKT ， S7 协议的会话层 TPKT 协议默认 TCP 端口是 102
    - PKTP协议wireshark协议栈

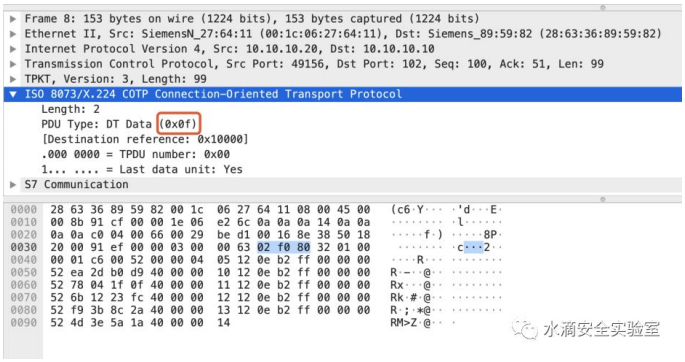


      - 一共四个字节：
        - Version ， 一个字节，版本信息
        - Reserved ， 一个字节，保留字段
        - Length ， 两个字节，包括当前 4 个字节在内的后续 TCP payload 的字节长度
  - `COPT` 协议层
    - COPT 协议（面向连接的传输协议），在传输数据前需要进行握手确立连接，所以 COPT 协议有两种包， COPT 连接包（握手包）和 COPT 功能包。
    - COPT 协议栈里面 PDU 类型为连接请求（ 0x0e ），表示该数据包是一个连接请求包， PDU 类型为连接请求（ 0x0 d ），表示该数据包是一个连接响应包
    - COPT 协议栈 PDU 类型码表

0x1	ED Expedited Data，加急数据
0x2	EA Expedited Data Acknowledgement，加急数据确认
0x4	UD，用户数据
0x5	RJ Reject，拒绝
0x6	AK Data Acknowledgement，数据确认
0x7	ER TPDU Error，TPDU错误
0x8	DR Disconnect Request，断开请求
0xc	DC Disconnect Confirm，断开确认
0xd	CC Connect Confirm，连接确认
0xe	CR Connect Request，连接请求
0xf	DT Data，数据传输

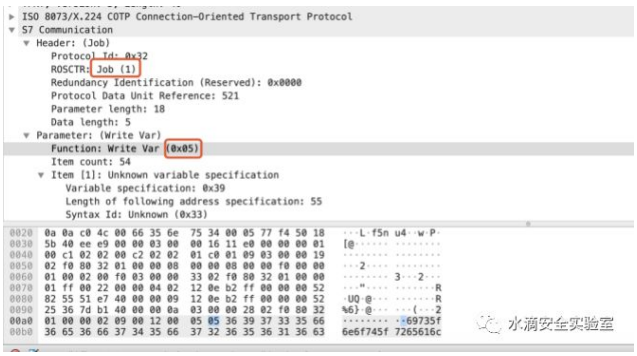
COPT 协议栈 PDU 类型码表

- S7Comm 数据传输数据包



  - 上图的 PDU Type 为 0x0f，表明是数据传输的数据包

- `S7Comm` 协议层
  - `S7Comm` 协议包括三个部分：
    - Header
      - ROSCTR
        - 常见值
          - 0x01： JOB 即作业请求，如，读 / 写存储器，读 / 写块，启动 / 停止设备，设置通信
          - 0x02： ACK 即确认相应，这是一个没有数据的简单确认
          - 0x03： ACK_DATA 即确认数据相应，一般是响应 JOB 的请求
          - 0x07： USERDATA 即扩展协议，其参数分段包含请求 / 响应 ID，一般用于编程 / 调试，读取 SZL 等
    - Parameter
    - Data
  - 举例
    - 功能码为 0x05 的 S7Comm 数据包



    - 含义解析
      - Header：
        - 第一个字节是协议标识符 0x32
        - ROSCTR：1
          - ROSCTR 这个字段的取值决定后面 PDU 的结构，这里我们只分析取值为 0x01-JOB，作业请求
            - 由主设备发送的请求（例如，读 / 写存储器，读 / 写块，启动 / 停止设备，设置通

信）。

- Parameter
  - S7Comm 当 ROSCTR 取值为 0x01 时，协议栈中的 Parameter 项的第一个字段是 function （功能码），大小为 1 字节
  - 功能码为 0x05 的 S7Comm 数据包查询功能码表可以确定这个数据包是写入值
    - 整理常见的 JOB 和 Ack_data 的功能码表

整理常见的 JOB 和 Ack_data 的功能码如下表：

十六进制	值	描述
0x00	CPU服务	CPU服务
0xf0	设置通讯	建立通讯
0x04	读取Var	读取值
0x05	写变量	写入值
0x1a	请求下载	请求下载
0x1b	下载区	下载块
0x1c	下载结束	下载结束
0x1d	开始上传	开始上传
0x1e	上载	发布
0x1f	结束上传	发布结束
0x28	PI服务	程序调用服务
0x29	PLC停止	关闭PLC

常见的功能码

- data
  - 因此 Write Var 中Parameter 的结构后面要添加写入值的内容，多了一个 data 项
  - data 的结构
    - 0 (Unsigned integer, 1 byte): Return code，返回代码
    - 1 (unsigned integer, 1 byte): Transport size，确定变量的类型和长度
    - 2-3 (unsigned integer, 2 bytes): Length，写入值的数据长度
    - 4 (1 byte): Data，写入的值
    - 5 (unsigned integer, 1 byte): Fill byte，填充字节，如果数据的长度不足 Length 的话，则填充

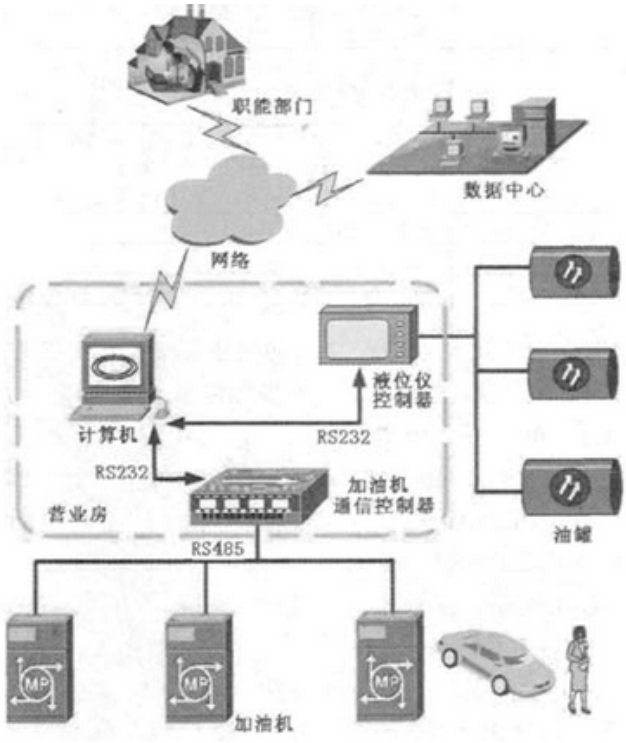
DNP3

- `DNP3 = DNP 3.0`
  - `DNP = Distributed Network Protocol = 分布式网络协议`
  - 是什么：是一种应用于自动化组件之间的通讯协议
    - SCADA可以使用DNP协议与主站、RTU、及IED进行通讯
  - 用途
    - 常见于 `电力` 、 `水处理` 等行业
  - 特点
    - 简化OSI模型，只包含了物理层，数据层与应用层的体系结构

OPC

- `OPC = 过程控制的OLE = OLE for Process Control`
  - OPC包括一整套接口、属性和方法的标准集，用于过程控制和制造业自动化系统
  -

ATG

- ATG
  - =油罐液位仪=加油站液位仪
  - 是什么：一种储油罐的监测设备
  - 现状
    - 全球有高达5800多站点的设备接入了互联网
    - 其中5300多位于美国
    - 仪表主要供应商为维德路特（Vedeer-Root）
    - 仪表设备经由串转网（串口转以太网）的方式接入互联网（主要用于运营商远程监控数据）
      - 因为设备协议上没有认证
        - 攻击者可以轻易通过网络更改仪表的门限和阀值、产生警报等引起安全事故
  - 加油站监测的系统结构图
    - 

工控安全组织和机构

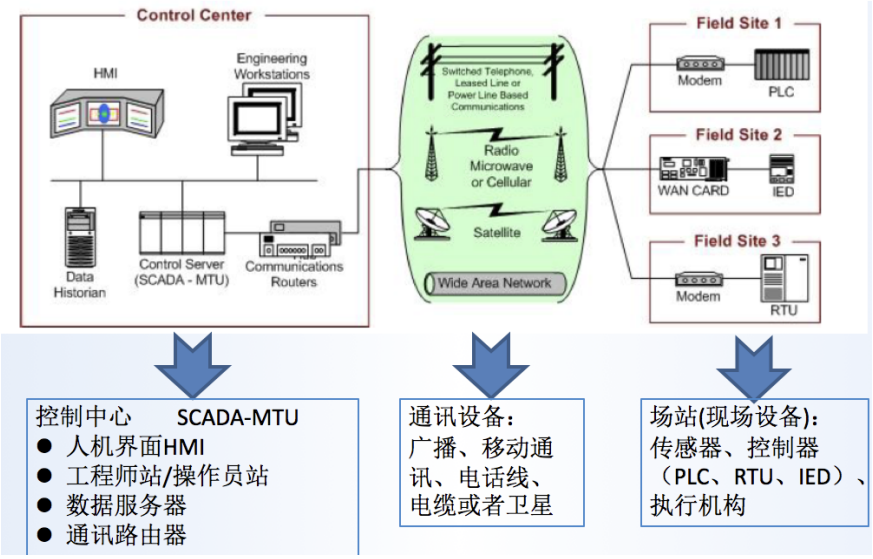
- 工控安全相关组织和机构
  - 工业互联网安全应急响应中心
    - 

  - 工业互联网产业联盟
    - http://www.aii-alliance.org/index.php

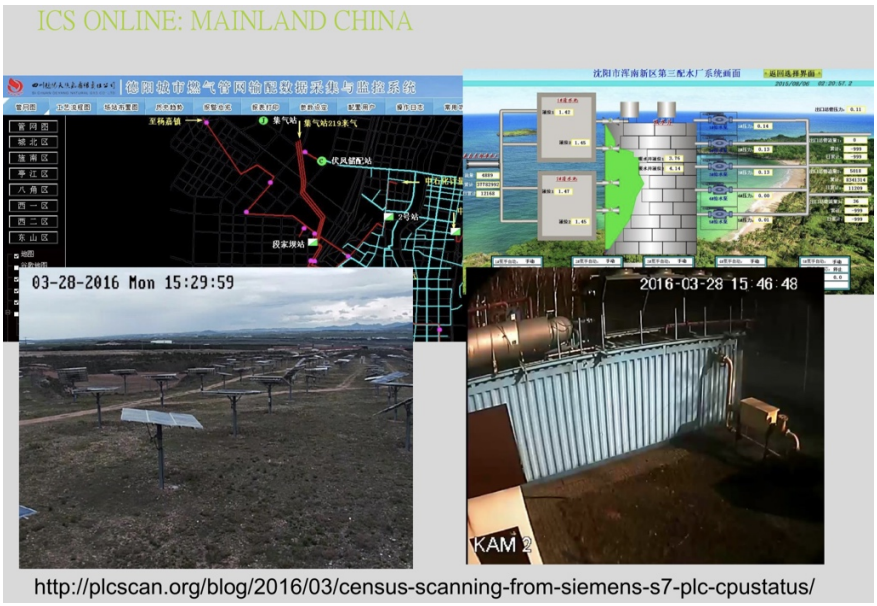
工控系统和产品

工控系统

典型工控系统架构



真实的工控系统举例



工控资产

参考这里，可以把工控资产，进行如下分类：

- `PLC = 可编程逻辑控制器`
- `SCADA / HMI` ： 监控组态类软件以及人机交互软硬件
- `RTDB / HISDB` ： 实时/历史 数据库
- `RTU / 传感器 / DTU`
- IOServer：数据通信组件
- 各种工控协议的通信接口： `Modbus / IEC104 / DNP3 / DLT 698 / OPCUA`
- 工业企业内网向外映射发布的视频监控设备
- 工业企业内网向外映射发布的Web生产管理系统

工控设备扫描

概述

各类漏洞引擎内容不同，采取配置、部署节点等存在较大的差异，目前针对工控这块的搜索引擎以 `shodan` 和 `ditecting` 更为专业，但是从针对端口来看，各个引擎宣称的公布检索方式不尽相同。

开放的互联网设备搜索平台

Shodan	shodan.io
Censys	censys.io
ZoomEye	zoomeye.org
ICSfind	icsfind.org
IVRE	ivre.rocks
Rapid7	scan.io

基于指纹识别平台的工控设备信息收集方式

《ICS/SCADA/PLC Google/Shodanhq Cheat Sheet》

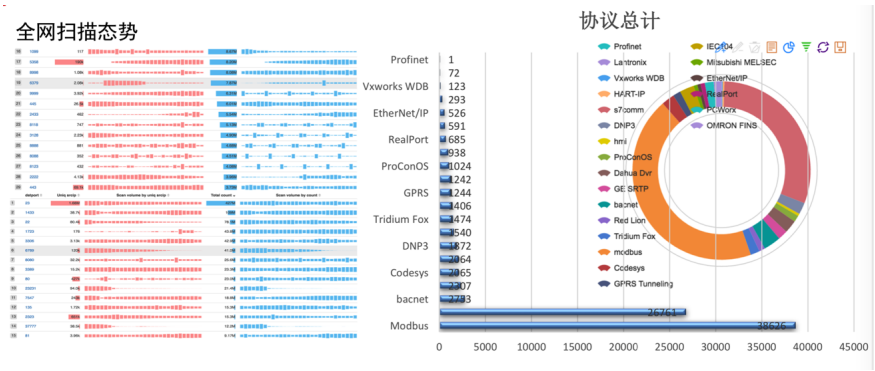
http://scadastrangelove.org/

《Internet connected ICS/SCADA/PLC Cheat Sheet》

http://www.scadaexposure.com/

举例：

全网扫描和相关工控协议



国外针对网络空间的情报收集计划

- SHINE计划——Project Shodan Intelligence Extraction

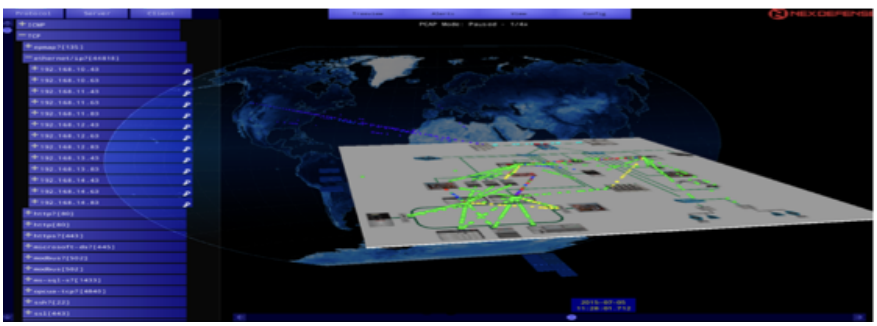
- X-Plane

- Treasure Map
- NCR

扫描后

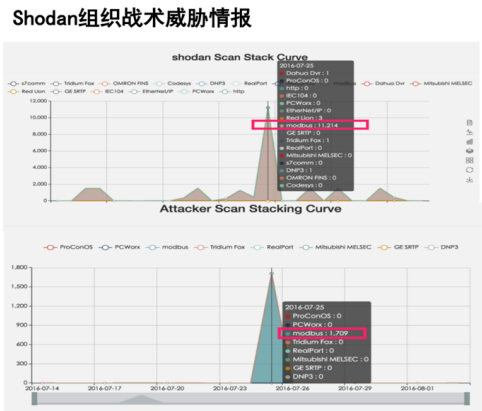
绘制网络空间地图，构建上帝视角感知能力

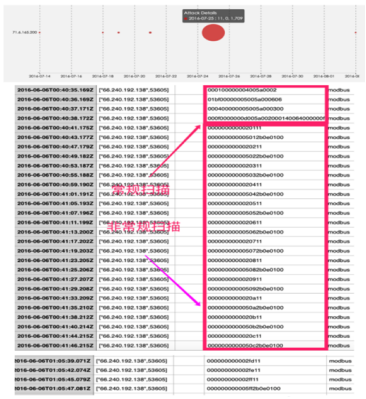
一般扫描出设备和风险、漏洞、威胁后，为了便于直观理解，往往会去绘制空间图。



出情报

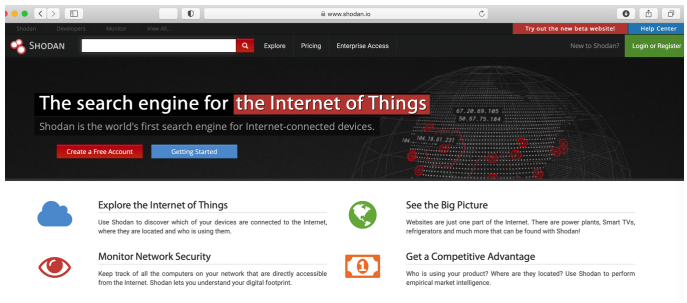
扫描后，就可以给出总结报告，情报了：



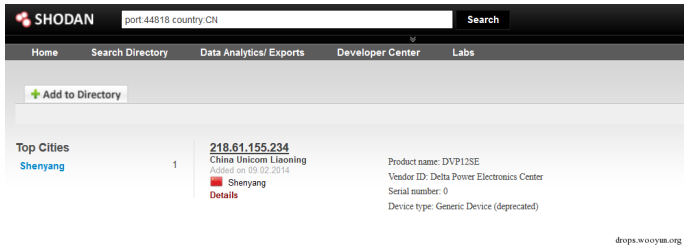


工控设备扫描系统

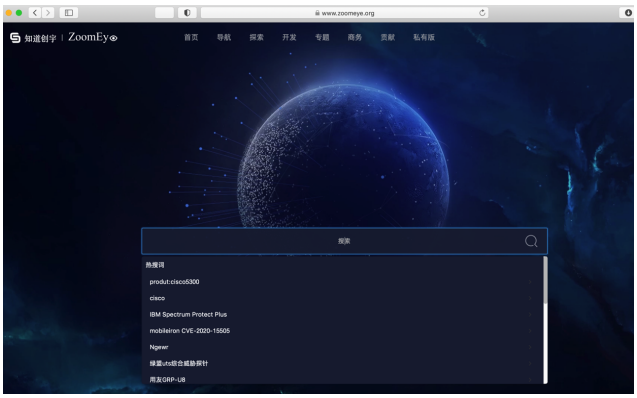
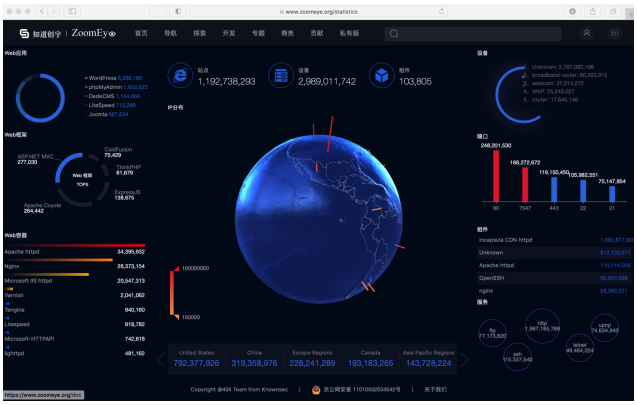
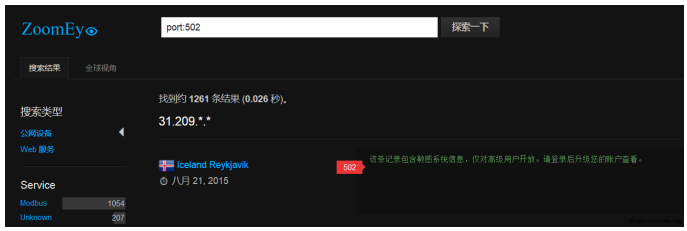
- 常见的 工控设备扫描系统 = 开放式网络空间搜索引擎
  - ICS-Radar
    - http://radar.winicssec.com/html/search/search_topic.html
    - 

  - Shodan搜索
    - https://www.shodan.io
    - 

    - 

    - 举例
    - 

  - Censys 全网引擎
    - 概述
      - Censys 是一款搜索引擎，它允许计算机科学家了解组成互联网的设备和网络。
      - Censys 由因特网范围扫描驱动，它使得研究人员能够找到特定的主机，并能够针将设备、网站和证书的配置和部署信息创建到一个总体报告中
  - Zoomeye搜索
    - 概述
      - 知道创宇打造的面向网络空间的搜索引擎

        - ZoomEye 于 2015 年 3 月上线了工控专题 (http://ics.zoomeye.org)，ZoomEye 支持 12 种工控协议的数据检索，使用者也可以使用工控协议的端口和特征 Dork 关键字发现暴露在互联网的工控软硬件
        - 对于工控协议类型的数据，ZoomEye 启用了保护策略，一般用户无法直接查看
    - ZoomEye - Cyberspace Search Engine
        - https://www.zoomeye.org
        - 
    - ZoomEye - Cyberspace Search Engine
        - https://www.zoomeye.org/statistics
        - 
    - 举例
        - 

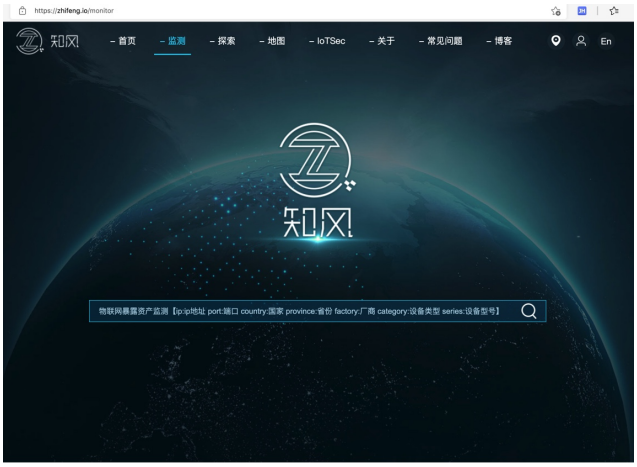
- FOFA 引擎
    - 概述
        - FOFA 是白帽汇推出的一款网络空间资产搜索引擎。它能够帮助用户迅速进行网络资产匹配、加快后续工作进程。
            - 例如进行漏洞影响范围分析、应用分布统计、应用流行度排名统计等
- Diting 全网引擎
    - 概述
        - 谛听 (ditecting) 网络空间工控设备搜索引擎，取谛听辨识万物之意，意在搜寻暴露在互联网上的工业控制系统联网设备， 帮助安

全厂家维护工控系统安全、循迹恶意企图人士

- 主页
  - 谛听 - 专注工控安全的搜索引擎
    - http://www.ditecting.com
    - 

- iotsec
  - 灯塔实验室 - 物联网安全威胁情报搜索引擎
    - https://www.iotsec.io
      - IoTSec.io-开放式物联网安全威胁情报搜索引擎
        - IoTSec.io是由灯塔实验室研发与运营的开放式物联网安全威胁情报搜索引擎，IoTSec.io由一个分布式互联网背景流量分析引擎组成，IoTSec.io可以实时收集与分析互联网海量网络流量行为，并且能够对网络流量行为、互联网传播的流量载荷、攻击事件进行自动化分析
        - IoTSec.io目前是一个完全开放式的数据搜索引擎，任何人都可以使用IoTSec.io来了解当前网络安全态势，通过使用IoTSec.io可以：
          - 1、掌握与监控各类网络扫描组织和网络空间测绘引擎行为
          - 2、掌握与监控各类网络扫描组织与扫描IP节点运行情况、扫描节点扫描的通信协议行为
          - 3、掌握与监控当前互联网扫描端口动态趋势
          - 4、掌握与监控当前互联网应用层载荷传播与排行情况
          - 5、掌握与监控当前互联网各类自动化漏洞利用情况
          - 6、掌握与监控当前物联网、工控系统相关被扫描、被攻击安全情况
      - 截图
        - 

- 知风
  - 知风-互联网联网工控资产与企业分析系统
    - https://zhifeng.io/monitor
      - 是什么：互联网联网工控资产与企业的关联分析系统
      - 用途：您可搜索任何企业名称来了解该企业是否存在接入互联网的工控系统和资产类型，您也可以搜索特定的系统名称来了解该系统是否接入过互联网
      - 背景
        - 随着网络化和信息化的普及，越来越多工业企业为满足运营、数据通信和运维需求，将工控网络与信息网络相连接，某些特殊情况下甚至直接将工业控制系统接入互联网中。经工业信息安全权威机构统计，我国存在大量工业控制相关软硬件资产直接接入互联网的情况，随着网络空间搜索引擎的出现和工控协议、设备识别方法的公开，使得人们可以利用Shodan、Censys、ZoomEye等开放式网络空间搜索引擎直接检索和访问联网的工业控制设备和系统，同样间接的暴露针对企业和相关系统的攻击面
        - 目前大量工业企业可能由于企业规模、建设规划、系统集成、管理运维、生产运营等多种原因可能将工控系统接入互联网，而其中原因可能是企业网络运维人员自身也不了解的，而“知风”积累的海量数据将可以告诉用户，自己的系统和企业是否曾经接入互联网，以便评估是否是由未授权导致的系统接入互联网
      - 概述
        - “知风”提出了一种互联网联网工控资产自动化分析方式，基于分析结果将可真正帮助用户了解目前接入互联网的工控资产是何企业所属，接入时间，系统名称等。利用“知风”积累的企业和系统数据，您使用“知风”时只需输入企业简称或系统简称，即可了解目标系统企业和系统是否有工控资产联网情况，借助“知风”您也可以了解您的企业、系统是否存在遭受互联网攻击的可能。
      - 系统工作方式
        - “知风”数据跨度长达3年，其系统分析的最原始联网工控资产数据来源渠道主要来自于各种网络空间搜索引擎如Shodan、Censys、ZoomEye、FOFA等公开平台，我们通过独有的IP核查与关联分析技术来鉴定联网工控资产、系统的所属，对系统和企业进行标识。“知风”系统本身是一个“被动”，“非接触式”的综合分析数据管理系统，整体依托开放平台提供的原始数据展开关联分析
      - 截图

- 

扫描工具

常见的工控设备扫描工具有：

- nmap

nmap

nmap是网络领域常用的端口扫描工具。

此处对于工控领域来说，也可以用于互联网上的公开的端口扫描，以发现相关工控设备。

nmap的nse脚本

- NSE脚本
  - 是什么：nmap的扫描测试脚本
  - 作用
    - 用于扫码相关协议的设备
  - 意义
    - 定位工控系统及协议模块
    - 收集目标工控的信息，如版本、内网IP、模块、硬件信息等
    - 结合对应的NSE脚本进一步拓展，例如自定义空间搜素引擎
  - 资源
    - Github测试脚本
      - https://github.com/atimorin/scada-tools
      - https://github.com/atimorin/PoC2013
      - https://github.com/drainware/scada-tools
      - https://github.com/drainware/nmap-scada
    - Exploit-db测试脚本
      - https://www.exploit-db.com/exploits/19833/
      - https://www.exploit-db.com/exploits/19832/
      - https://www.exploit-db.com/exploits/19831/
      - https://www.exploit-db.com/search/?action=search&description=scada&e_author=

Nmap NSE脚本

Nmap NSE脚本	端口	插件信息
mms-identify.nse	102	iec-61850-8-1 (mms) ics protocol
s7-enumerate.nse	102	numerates Siemens S7 PLC Devices and collects their device information
modbus-discover.nse	502	Enumerates SCADA Modbus slave ids (sids) and collects their device information
modicon-info.nse	502	use Modbus to communicate to the PLC via Normal queries that are performed via engineering software
cr3-fingerprint.nse	789	Fingerprints Red Lion HMI devices
moxa-enum.nse	4800	MoxaNPort
melsecq-discover.nse	5007	MELSEC-Q Series PLC CPUINFO
melsecq-discover-udp.nse	5006	MELSEC-Q Series PLC CPUINFO
BACnet-discover-enumerate.nse	47808	BACnet
atg-info.nse	10001	Guardian AST I20100
codesys-v2-discover.nse	1200/2455	received then the output will show that the port as CoDeSyS
cspv4-info.nse	2222	cspv4-info
dnp3-info.nse	20000	DNP3
enip-enumerate.nse	44818	CIP = Information that is parsed includes Vendor ID, Device Type, Product name, Serial Number, Product code,Revision Number, as well as the Device IP
fox-info.nse	1911	collect information from A Tridium Niagara system
omrontcp-info.nse	9600	Controller Data Read Command and once a response is received
omronudp-info.nse	9600	Controller Data Read Command and once a response is received
pcworx-info.nse	1962	PCWorx info

Nmap NSE脚本	端口	插件信息
proconos-info.nse	20547	ProConOs
Siemens-CommunicationsProcessor.nse	80	Checks for SCADA Siemens S7 Communications Processor devices
Siemens-HMI-miniweb.nse	80	Checks for SCADA Siemens SIMATIC S7-devices
Siemens-SIMATIC-PLC-S7.nse	80	Checks for SCADA Siemens Simatic S7 devices
Siemens-Scalance-module.nse	161	Checks for SCADA Siemens SCALANCE modules
Siemens-WINCC.nse	137	Checks for SCADA Siemens WINCC server
bradford-networks-nac.nse	8080	Attempts to detect Bradford Networks Network Sentry appliance admin web interface
iec-identify.nse	2404	Attemts to check tcp/2404 port supporting IEC 60870-5-104 ICS protocol
minecraft.nse	25565	Checks for Minecraft Servers using the 0x02 "Handshake" protocol
mop-discover.nse	null	Detect the Maintenance Operation Protocol (MOP) by sending layer 2 DEC DNA Remote Console hello/test messages
stuxnet-detect.nse	445	Detects whether a host is infected with the Stuxnet worm

脚本测试使用举例

Ethernet/IP 44818

```
nmap -p 44818 --script enip-enumerate.nse 85.132.179.*
```

```
D:\Tools\nmap-6.47>nmap -p 44818 --script enip-enumerate.nse  85.132.179.[redacted]

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-06 14:23 中国标准时间
Nmap scan report for 85.132.179.138
Host is up (0.38s latency).
PORT      STATE SERVICE
44818/tcp open  EtherNet/IP
| enip-enumerate:
|   Vendor: Rockwell Automation/Allen-Bradley (1)
|   Product Name: 1766-L32BWA A/5.00
|   Serial Number: 0x404fa80e
|   Device Type: Programmable Logic Controller (14)
|   Product Code: 90
|   Revision: 1.5
|_  Device IP: 192.168.3.50

Nmap done: 1 IP address (1 host up) scanned in 10.12 seconds
```

Modbus 502

```
nmap --script modicon-info.nse -Pn -p 502 -sV 91.83.43.*
```

```
D:\Tools\nmap-6.47>nmap --script modicon-info.nse -Pn -p 502 -sU 91.83.43.[redacted]

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-06 14:03 中国标准时间
Nmap scan report for 91.83.43.181
Host is up (0.34s latency).
PORT    STATE SERVICE VERSION
502/tcp open  Modbus
| modicon-info:
|   Vendor Name: Schneider Electric
|   Network Module: BMX P34 2020
|   CPU Module: BMX P34 2020
|   Firmware: v2.2
|   Memory Card: BMXRMS008MP
|   Project Information: Project - V4.0   FAYCSABA-PC D:\Fay Automation\projektek\Gombos_ifj\Gombos_m340\gombos_140726.stu
|   Project Revision: 0.8.40
|_  Project Last Modified: 8/29/2015 8:53:49

Service detection performed. Please report any incorrect results at http://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 50.80 seconds
```

IEC 61870-5-101/104 2404

```
nmap -Pn -n -d --script iec-identify.nse --script-args=iec-identify -p 2404 80
```

```
D:\Tools\nmap-6.47>nmap -Pn -n -d --script iec-identify.nse  --script-args=iec-identify -p 2404 80.34.253.[redacted]

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-06 14:33 中国标准时间
Winpcap present, dynamic linked to: WinPcap version 4.1.3 (packet.dll version 4.1.0.2980), based on libpcap version 1.0 branch 1_0_rel0b (20091008)
--------------- Timing report ---------------
  hostgroups: min 1, max 100000
  rtt-timeouts: init 1000, min 100, max 10000
  max-scan-delay: TCP 1000, UDP 1000, SCTP 1000
  parallelism: min 0, max 0
  max-retries: 10, host-timeout: 0
  min-rate: 0, max-rate: 0
---------------------------------------------
NSE: Using Lua 5.2.
NSE: Script Arguments seen from CLI: iec-identify
NSE: Loaded 1 scripts for scanning.
NSE: Script Pre-scanning.
NSE: Starting runlevel 1 (of 1) scan.
Initiating SYN Stealth Scan at 14:34
Scanning 80.34.253.26 [1 port]
Packet capture filter (device eth4): dst host 192.168.[redacted] and (icmp or icmp6 or ((tcp or udp or sctp) and (src host 80.34.253.[redacted])))
Discovered open port 2404/tcp on 80.34.253.26
Completed SYN Stealth Scan at 14:34, 0.92s elapsed (1 total ports)
Overall sending rates: 1.09 packets / s, 48.09 bytes / s.
NSE: Script scanning 80.34.253.26.
NSE: Starting runlevel 1 (of 1) scan.
NSE: Starting iec-identify against 80.34.253.26:2404.
Initiating NSE at 14:34
NSE: try to connect to port 2404
NSE: testfr status true
NSE: testfr recv: 680483000000
NSE: startd recv_len: 6
NSE: startdt recv: 68040b000000
NSE: c_ic_na_1 status true
NSE: c_ic_na_1 recv len: 7
NSE: c_ic_na_1 recv: 54494d4545554
NSE: Finished iec-identify against 80.34.253.26:2404.
Completed NSE at 14:34, 1.58s elapsed
Nmap scan report for 80.34.253.26
Host is up, received user-set (0.31s latency).
```

Siemens S7 102

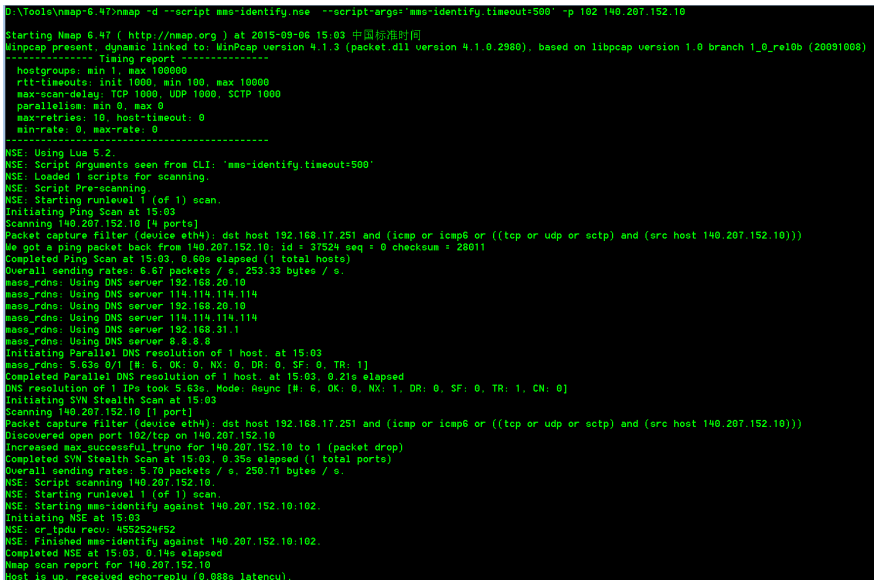
```
nmap -p 102 --script s7-enumerate -sV 140.207.152.*
```

```
D:\Tools\nmap-6.47>nmap -p 102 --script s7-enumerate -sV 140.207.152.[redacted]

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-06 14:59 中国标准时间
Nmap scan report for 140.207.152.10
Host is up (0.048s latency).
PORT    STATE SERVICE  VERSION
102/tcp open  iso-tsap Siemens S7 PLC
| s7-enumerate:
|   Module: 6ES7 314-1AG14-0AB0
|   Basic Hardware: 6ES7 314-1AG14-0AB0
|   Version: 3.3.2
|   System Name: SIMATIC 300 Station
|   Module Type: CPU 314
|   Serial Number: S C-BDU433522011
|_  Copyright: Original Siemens Equipment
Service Info: Device: specialized
```

和：

```
nmap -d --script mms-identify.nse --script-args='mms-identify.timeout=500' -p
```



Tridium Niagara Fox 1911

```
nmap -p 1911 --script fox-info 99.55.238.*
```

```
D:\Tools\nmap-6.47>nmap -p 1911 --script fox-info 99.55.238.[redacted]

Starting Nmap 6.47 ( http://nmap.org ) at 2015-09-06 15:08 中国标准时间
Nmap scan report for adsl-99-55-238-41.dsl.irvnca.sbcglobal.net (99.55.238.41)
Host is up (0.18s latency).
PORT     STATE SERVICE
1911/tcp open  Niagara Fox
| fox-info:
|   Fox Version: 1.0.1
|   Host Name: 99.55.238.41
|   Host Address: 99.55.238.41
|   Application Name: Station
|   Application Version: 3.7.106.1
|   VM Name: Java HotSpot(TM) Client VM
|   VM Version: 1.5.0_34-b28
|   OS Name: QNX
|   Host ID: Qnx-NPM6-0000-11E0-F82F
|   VM UUID: 11e49da1-6be2-f6d6-0000-00000000bb2d
|_  Brand ID: Webs
```

工控攻击

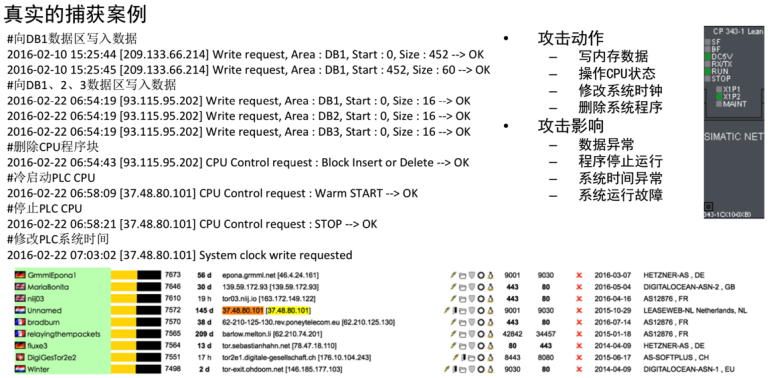
- 工控风险的增加
  -
    1. 整个工控设备更新慢、较封闭
    2. 随着网络智能制造提出新的需求，以前隐蔽的内网环境被暴露出来
  -
    1. 传统工业企业的数字化改造
    2. 也会导致暴露的漏洞越来越多
- 工控受到的网络攻击
  - 方式
    - IT侧攻击
      - IT侧作为跳板
    - OT侧攻击
      - 控制工业现场设备
        - 目的：以达到真正攻击工业设备目的
        - 手段：
          - `组态利用`
          - `通信劫持`
          - `Web渗透`
  - 结果
    - 各种安全威胁
      - 敏感信息的泄露
      - 内网横向渗透
      - 蠕虫病毒传播
      - 权限维持
  - 对策
    - IT侧
      - 技术
        - 搭建防火墙
          - 进行身份访问控制
        - 主机及时更新
        - 关闭敏感端口
        - 尽可能关闭远程服务
          - 启用远程服务时使用隧道加密，保护通信数据
        - 蜜罐/蜜网=Honeypot
          - 含义：高仿真、高交互的专用工业入侵诱捕系统
            - 可以理解为：网络攻防领域的钓鱼执法
          - 作用：专指用来侦测或抵御未经授权操作或者是黑客攻击的陷阱，因原理类似诱捕昆虫的蜜罐因而得名
          - 特点：发现未知攻击的有效工具
      - 人 = 社工
        - 加强人员安全意识
    - OT测
      - 要对工控系统采取全面安全评估，对关键资产节点，制定重点保护策略，实现单点阻断。

攻击事件

- BlackEnergy
  - 2015年12月乌克兰国家电网系统遭到BlackEnergy的攻击，并引起了乌克兰大规模的停电事故
  - 涉及协议：ProfiNET？
  - 

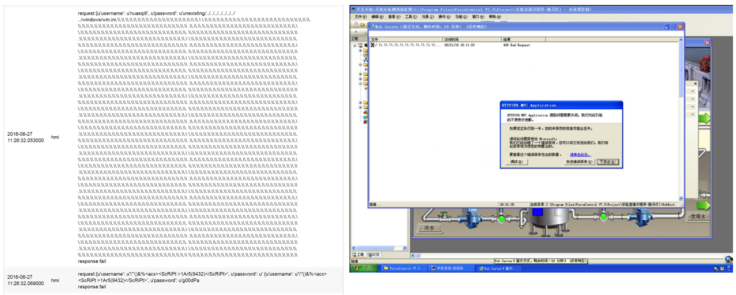
- PLC攻击

  真实的捕获案例

  - 

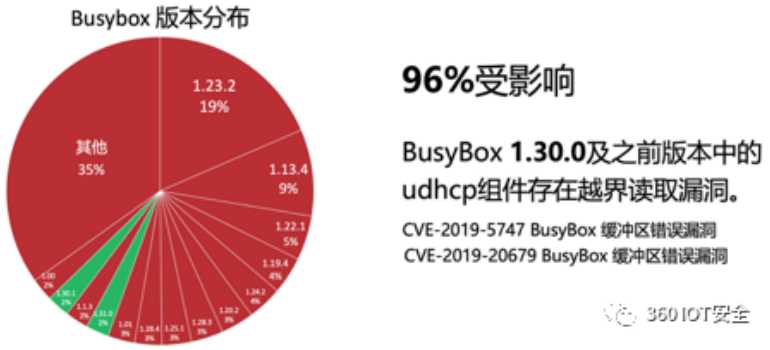
- HMI溢出

  针对HMI的溢出攻击

  - 

工控漏洞

- Busybox1.30.0
  - 2019 年Busybox1.30.0及之前版本存在的漏洞，包括CVE-2019-5747和CVE-2019-20679等。有非常多的固件使用了Busybox组件，并且大部分使用的都是1.30.0之前的版本。经过360安全研究院团队从数万个固件样本中统计，96%的固件都使用了1.30.0之前的版本
  - 这会导致各种类型的设备都受其影响，包括与GE医疗心电图分析系统密切相关的串口设备服务器、智能楼宇的自动化控制系统设备、工控系统中的RTU控制器以及工业安全路由器等



- D-Link
  - 2019年9月，集成自动化网络安全解决方案商Fortinet的FortiGuard Labs发现并向官方反馈了D-Link产品中存在的一个未授权命令注入漏洞（FG-VD-19-117/CVE-2019-16920）。攻击者可以利用该漏洞在设备上实现远程代码执行（RCE），且无需通过身份认证。该漏洞被标记为高危级别漏洞

- 数控机床

漏洞分析

乌云工控漏洞的分析

针对乌云主站的漏洞进行关键字搜索：工控(31)、SCADA(15)、Modbus(9)、PLC并进一步整合得到如下列表。

缺陷编号	漏洞起因	漏洞标题
wooyun-2015-132010	弱口令	工控安全之华润燃气敏感环境竟然未走专线可导致内网渗透（监控/配置/阀门可控未测）
wooyun-2015-129388	注入	华润化工控股有限公司信息门户设置缺陷/sql 注入
wooyun-2015-125651	弱口令	某地有线电视内网沦陷可能修改推送广告内容等
wooyun-2015-125399	注入	中华工控网SQL注入导致全网数据沦陷90W会员数据#打包
wooyun-2015-122677	弱口令	某工控系统配置不当危及船只安全
wooyun-2015-117227	弱口令	某水库工控系统存在弱口令(成功渗透)
wooyun-2015-116558	配置不当	某电厂监管系统缺陷可导致整个工控网络沦陷（DCS/PLC 可被操控执行任何命令）
wooyun-2015-107326	注入	某油田开发公司工控系统 sql 注入
wooyun-2015-96729	配置错误	VA 弱密码致华北工控内网远程桌面服务器/内网穿透/涉及敏感信息
wooyun-2014-87708	弱口令	温州市管道燃气公司 SCADA 系统弱口令
wooyun-2014-86726	逻辑漏洞	中国工控网任意用户密码重置漏洞
wooyun-2014-83839	弱口令	大量外网 web 监控系统后台存在弱口令(涉及两款监控产品，涵盖宾馆、车间、仓库、企业内部等)
wooyun-2014-71890	弱口令	某财政信息网系统管理系统密码泄露
wooyun-2014-58681	配置不当	对电厂生产控制网络的一次漫游（针对工控网络的小型APT 攻击）
wooyun-2013-42212	目录遍历	北京市一工控系统多处漏洞可内网渗透（已经发现 webshell）
wooyun-2013-22961	网络未授权访问	301 基础设施系列-国外基础设施 1（鲍里斯波尔国际机场地面照明控制和监测系统）暴漏
wooyun-2013-21848	弱口令	从对某电厂 DCS 控制系统的实体控制谈工控安全（可控制电厂实体设备）
wooyun-2013-21314	弱口令	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透 第二份案例ops.wooyun.org

wooyun-2013-21250	弱口令	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透
wooyun-2012-16328	未授权访问	美国一工业操作系统越权访问,可控制能源基础设施
wooyun-2012-10818	弱口令	武汉市某工控系统弱口令导致信息泄漏，企业各种记录在内
wooyun-2012-09565	命令执行	旅统计代码，站长一秒钟变 APT 攻击专家（wooyun-2012-09025 续）
wooyun-2012-09025	设计缺陷	UC 云端加速引擎存在非正常泄露referer问题
wooyun-2012-07340	账户体系控制不严	某省级能源集团旗下XX 存在安全隐患
wooyun-2012-07172	配置错误	某环境集成平台存在严重问题！获得客户端控制实权！
wooyun-2012-07084	弱口令	中国电信某 GPS 监控平台存在严重问题
wooyun-2012-06997	SQL注入	天津鑫然智能 DCS 监控平台
wooyun-2012-06196	配置不当	国内某大型风电工控系统应用配置失误
wooyun-2012-04702	信息泄露	南京国电自动化股份有限公司厂站监控系统源代码及配置文件泄露漏洞
wooyun-2014-84258	未授权访问	荥堰市自来水公司 SCADA 管网综合监测系统漏洞
wooyun-2014-80994	注入	哈药集团分公司 sql 注入(影响大量同服网站数据库)
wooyun-2014-58654	命令执行	CenturyStar9.0 SCADA 组态软件存在远程命令执行漏洞
wooyun-2014-58130	上传漏洞	某电厂 SCADA 测试文件未清理存在任意上传漏洞(可导致服务器沦陷)
wooyun-2013-34711	弱口令	天能集团某 SCADA 系统弱口令登陆
wooyun-2013-21086	SQL注入	某煤矿 SCADA 系统存在严重缺陷可导致服务器沦陷
wooyun-2012-07334	未授权访问	某市燃气管道 SCADA 系统登录绕过
wooyun-2012-06952	设计缺陷	某 SCADA 电力监控系统漏洞

以上的漏洞列表中，可以得出如下结论：

- 乌云工控漏洞的案例中，绝大多起因是弱口令(弱口令最多的是123456，其次是admin)、注入类漏洞
- 能够挖出工控的精华漏洞的人也是特定的那几位，且在Kcon2015也有过演讲
- 挖掘此类漏洞主要解决两个问题
  - 如何找到工控相关的系统和地址
  - Getshell后，基于工控知识如何操控系统
- 根据漏洞中的细节可以进一步的复测和拓展，进而为工控系统的漏洞挖掘提供非线性思路
  - 结合GHDB关键字的搜素：例如 `inurl:SCADA` 等
  - 链接地址含SCADA、Modbus等协议的关键字等
  - 其他KEY：MIS、SIS、DCS、PLC、ICS、监控系统等
  - 相关公司：南京科远、金风科技、天能集团、国电南瑞、华润燃气、积成电子、重庆三峰、东方电子等

工控精华漏洞分析

乌云工控相关的精华漏洞如下7个，在思路亮点中分析了漏洞的核心，同样也可能是获得打雷精华的理由。几乎共同点均是操控了对应的工控系统

缺陷编号	漏洞标题	思路亮点	作者
wooyun-2015-132010	工控安全之华润燃气敏感环境竟然未走专线可导致内网渗透（监控/配置/阀门可控未测）	燃气系统 Getshell+内网渗透+敏感信息	jianFen
wooyun-2015-125651	某地有线电视内网沦陷可能修改推送广告内容等	Getshell+集群指令下达+敏感信息	scanf
wooyun-2015-116558	某电厂监管系统缺陷可导致整个工控网络沦陷（DCS/PLC可被操控执行任何命令）	发电厂 getshell+内网 DB+操控 DCS+拓扑分析	zph
wooyun-2014-58681	对电厂生产控制网络的一次漫游（针对工控网络的小型 APT 攻击）	MIS&SIS 分析+Getshell+内网	Z-0ne
wooyun-2013-21314	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透 第二份案例	在线 DCS 采集系统操控	Z-0ne
wooyun-2013-21250	从某知名厂商 MIS 软件逻辑缺陷谈对某工控网络的渗透	软件厂商+未授权敏感信息+Getshell+操控 Syncmb	Z-0ne
wooyun-2015-127849	某大型 SCADA 系统缺陷导致多地多个工控基础设施被沦陷（影响电力、自来水、运营商等）	-	zph

drops.wooyun.org

工控漏洞库

- 工控系统行业漏洞
  - 工控漏洞子库 - CNVD
    - https://ics.cnvd.org.cn/
    - 

    - 相关名词
      - `CVND` = `China Natinal Vulnerability Database` = 国家信息安全漏洞共享平台
- 工控漏洞库 - 信息安全漏洞门户 VULHUB
  - http://vulhub.org.cn/view/ics
  - 

社工手段

- 人的漏洞
  - 社工手段
    - 背景
      - 人的因素是网络安全中最重要的因素之一
        - 在工业互联网安全中也是如此
    - 方式
      - 内部人员监守自盗及外部人员腐蚀内部工作人员，鱼叉式钓鱼找准目标人物性格、猎奇心理、兴趣点或物理渗透通过伪装进入现场进行操作
  - 举例
    - 水坑攻击
      - 攻击目标常浏览的网站，留下恶意脚本，等待触发
    - 钓鱼邮件攻击
    - 特斯拉工厂遭黑客攻击
      - 一名俄罗斯黑客联系上特斯拉工厂的一名员工，并承诺给他100万美元，要求其安装恶意软件到特斯拉内部网络，以使内部网络遭受攻击，以便在安全团队忙于应对攻击时，利用恶意软件，窃取商业机密，换取赎金
      - 这是一起靠社工手段非法入侵计算机系统的失败事件

工控渗透

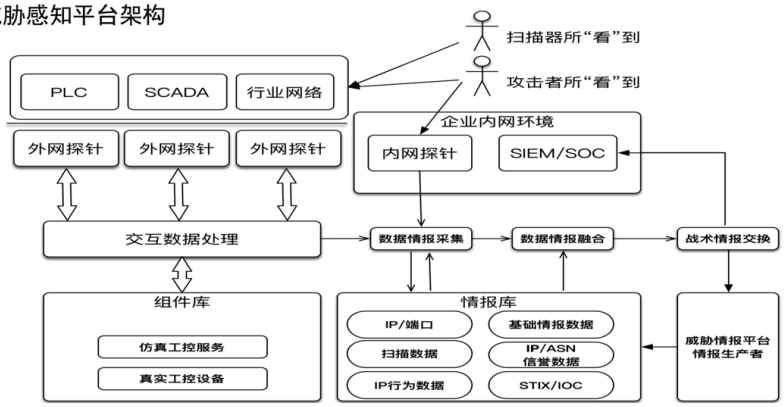
工具和框架

相关领域名词

被动威胁感知

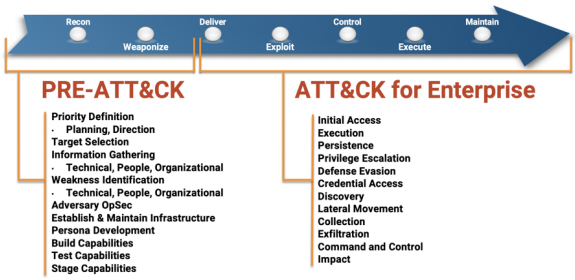
被动威胁感知平台架构

被动威胁感知平台架构

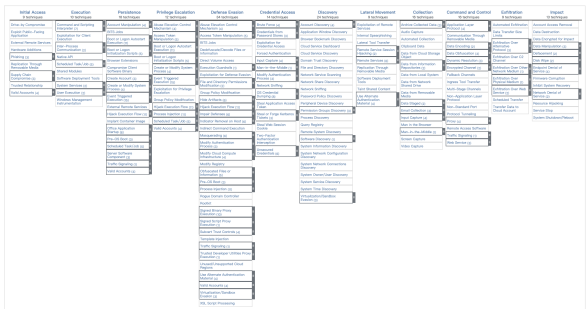


ATT & CK

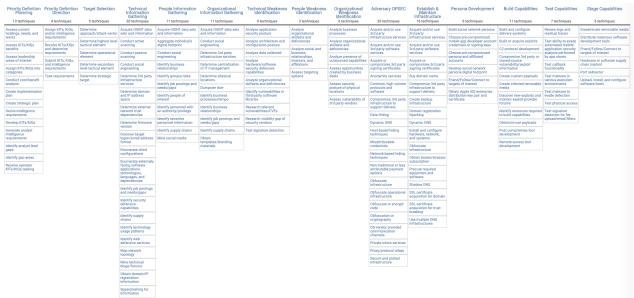
- ATT&CK
  - ATT&CK=Adversarial Tactics, Techniques & Common Knowledge
  - 一句话简介：MITRE ATT&CK 框架是打造检测与响应项目的流行框架
  - 是什么：一个模型
    - 总结概括了你的敌方可能尝试的战术和技术
  - 所属公司：MITRE
    - 所以全称是：MITRE ATT&CK Matrix
  - 呈现形式：一个大列表
  - 时间：2013年提出此概念
  - 细节介绍
    - 总体战术tactics
      - Initial Access
      - Execution
      - Persistence
      - Privilege Escalation
      - Defense Evasion
      - Credential Access
      - Discovery
      - Lateral Movement
      - Collection
      - Exfiltration
      - Impact
  - 分类
    - Enterprise ATT&CK = MITRE ATT&CK® Matrix for Enterprise
      - 介绍：ATT&CK for Enterprise is an adversary model and framework for describing the actions an adversary may take to compromise and operate within an enterprise network
      - 支持平台：
        - Windows
        - macOS
        - Linux
        - Cloud
          - AWS
          - GCP
          - Azure
          - Azure AD
          - Office 365
          - SaaS
      - 矩阵
        - 概述



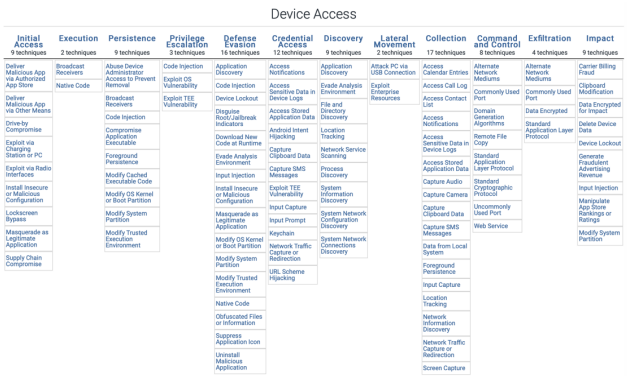
- 细节



- PRE-ATT&CK
  - 概述

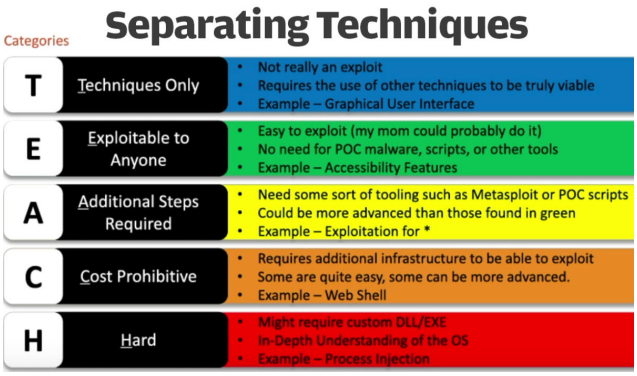


- Mobile ATT&CK
  - 概述



  - 支持平台
    - Android
    - iOS

- 如何理解和使用
  - How to implement and use the MITRE ATT&CK framework | CSO Online
    - https://www.csoonline.com/article/3396139/how-to-implement-and-use-the-mitre-attandck-framework.html
      - 中文版

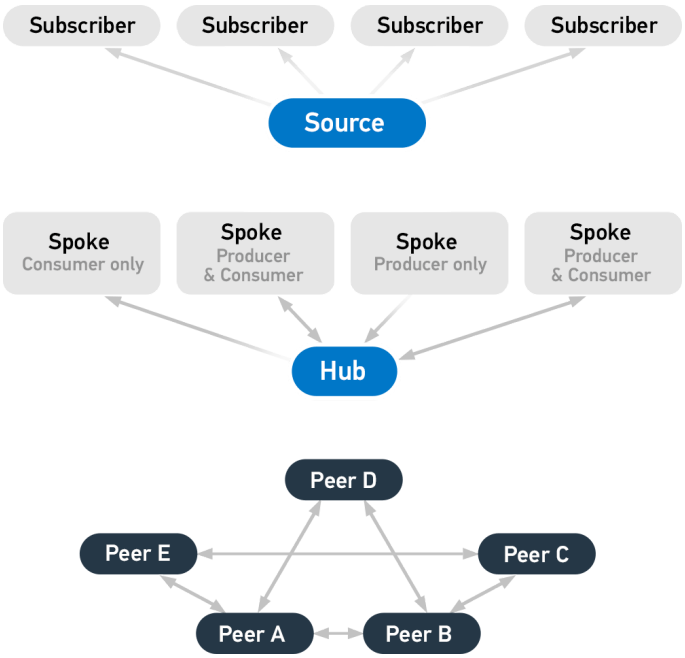
        - MITRE ATT&CK 框架“入坑”指南 - 安全牛
            - https://www.aqniu.com/learn/61125.html
        - ATT&CK - 信息安全漏洞门户 VULHUB
            - http://vulhub.org.cn/attack
    - 按照难度分
        - 

    - 加上难度颜色后，ATT&CK变成
        - 

STIX and TAXII

- STIX and TAXII
  - 是什么：标准standards
  - 目的：降低网络攻击和增强预防
    - STIX：描述了威胁情报有哪些
    - TAXII：介绍如何转发情报信息
  - 概述
    - 

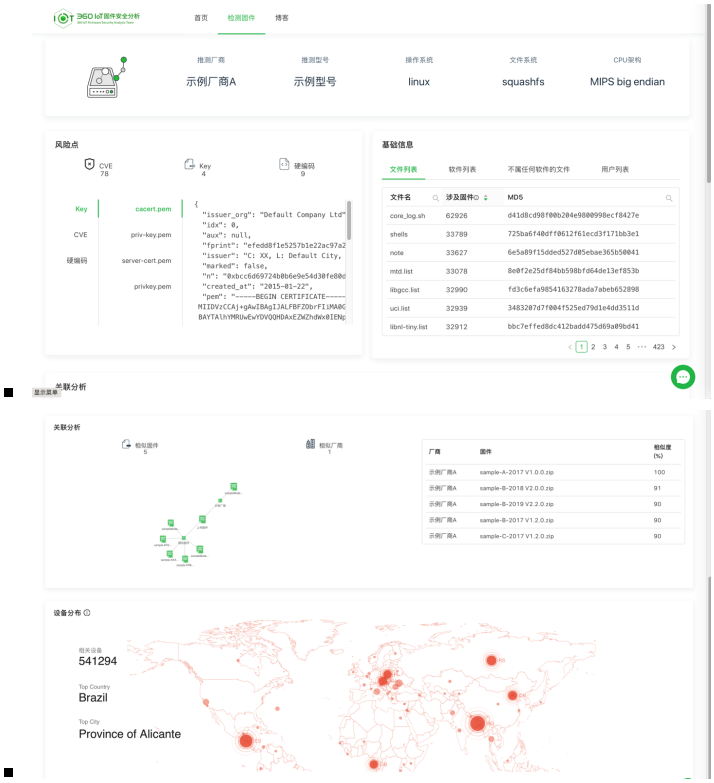
  - 特点
    - machine-readable机器能识别
      - 容易自动化处理
  - STIX= Structured Threat Information eXpression
    - 一句话介绍：STIX, short for Structured Threat Information eXpression, is a standardized language developed by MITRE and the OASIS Cyber Threat Intelligence (CTI) Technical Committee for describing cyber threat information.
    - 应用现状：It has been adopted as an international standard by various intelligence sharing communities and organizations.
    - 使用方式：It is designed to be shared via TAXII, but can be shared by other means
    - 用途
      - STIX is structured in such a fashion that users can describe threat
        - Motivations
        - Abilities
        - Capabilities
        - Response
  - TAXII=Trusted Automated eXchange of Intelligence Information
    - 一句话描述：defines how cyber threat information can be shared via services and message exchanges
    - 作用：It is designed specifically to support STIX information, which it does by defining an API that aligns with common sharing models
    - 3种主要模型
      - Hub and spoke – one repository of information
      - Source/subscriber – one single source of information
      - Peer-to-peer – multiple groups share information

- 4种服务
  - Discovery – a way to learn what services an entity supports and how to interact with them
  - Collection Management – a way to learn about and request subscriptions to data collections
  - Inbox – a way to recieve content (push messaging)
  - Poll – a way to request content (pull messaging)
- 概述
  - 

FirmwareTotal

- FirmwareTotal
  - 是什么
    - 360安全研究院的多维数据关联分析平台
      - IoT固件自动化安全分析解决方案
  - 作用
    - 了解您的IoT固件是否存在安全问题
    - 支撑了追踪分析多起IoT 0-day 在野攻击事件，输出高级威胁情报
    - 支撑了对多起IoT/IIoT供应链漏洞传播安全事件的影响范围评估
  - 用途
    - What can Firmware Total do for you
      - 360安全大脑赋能
        - 基于360安全大脑的安全能力
      - 基于多攻击面的安全分析
        - 固件检测聚焦于与安全相关的指标
      - IoT漏洞特征库
        - 基于不断更新的IoT漏洞特征库
      - 软件供应链分析
        - 基于软件供应链的安全分析
      - 动态分析
        - 动态模拟IoT服务进行安全分析
      - 关联分析
        - 基于多维度的数据关联比对
  - 其他功能
    - IoT安全数据搜索引擎
      - 强大的IoT安全数据搜索引擎，发现更多隐藏的缺陷设备
    - IoT安全可视化关联分析
      - 基于IoT安全数据的可视化关联分析
    - IoT蜜罐模拟平台
      - 通过模拟IoT设备固件，可作为靶场或感知蜜罐
  - 用途举例
    - 对缺陷设备之一的Q6035-E的网络资产探测结果
      - 

    - https://ft.iotsec.360.cn/#/result?id=sample



工控固件

- 固件
  - 工控产品和设备往往是对应的物理硬件，其中有对应的软件，实现相关功能
  - 而想要分析，破解工控产品，往往需要从提取其中的软件入手
  - 所以就会涉及到 `固件逆向`
- `固件逆向` = `固件提取` + `固件分析`
  - `固件提取`
    - 把firmware固件从硬件中，通过各种软硬件方法提取出来
      - 提取出来后往往是一个二进制文件
        - 举例
          - iot初体验 摄像头固件提取 看雪论坛
  - `固件分析` =
    - 提取出固件后，就需要借助于各种工具去分析固件的信息和逻辑，用于安全相关研究
- `固件逆向工具` = `固件破解工具`
  - 对于固件的提取和分析，属于逆向和破解，所以相关工具也叫：`固件逆向工具` = `固件破解工具`
- 取证
  - 公安破案，有时候会涉及到取证
    - 在对电子类设备的取证，往往涉及到 固件提取和固件分析
      - 所以固件提取和固件分析类的工具和软件也被叫做：`取证工具`

举例

- 固件分析举例
  - 施耐德NOE 771固件逆向分析

工控固件逆向

常见的固件逆向分析工具和系统有：

- 主流
  - `binwalk`
  - `BAT = Binary Analysis Toolkit`
- 其他
  - `FAT = Firmware-Analysis-Toolkit`
  - `AttifyOS`
  - `eimgfs`
    - nlitsme/eimgfs: Tool for editting Windows CE/Mobile firmware images.
      - https://github.com/nlitsme/eimgfs

binwalk

- `binwalk`
  - 是什么：固件分析工具
    - Firmware Analysis Tool
  - 一句话描述
    - 固件分析利器
      - 从固件中查找文件
    - a fast, easy to use tool for analyzing, reverse engineering, and extracting firmware images
  - 背景
    - 传统的固件分析：`file`
      - file缺点：占用了太多的磁盘来读写`I/O`，效率太低
    - `libmagic`动态库
      - 文件扫描的更好的解决方案
        - 核心4个函数
          - `magic_open`
          - `magic_close`
          - `magic_buffer`
          - `magic_load`
  - 基本功能
    - 图

    - 文字
      - 提取文件
      - 过滤功能
      - 比较功能
      - 字符串分析
      - 插件功能
  - 用途：
    - 路由器固件分析
    - 分析获取嵌入式设备的文件系统
  - 支持平台
    - `Linux`
    - `macOS`
    - `Cygwin`
    - `FreeBSD`
    - `Windows`
  - 资料

- Github
  - ReFirmLabs/binwalk: Firmware Analysis Tool
    - https://github.com/ReFirmLabs/binwalk
- 快速上手
  - Quick Start Guide · ReFirmLabs/binwalk Wiki
    - https://github.com/ReFirmLabs/binwalk/wiki/Quick-Start-Guide
- 用法
  - Usage · ReFirmLabs/binwalk Wiki
    - https://github.com/ReFirmLabs/binwalk/wiki/Usage

举例

```
root@kali:~# binwalk -B ddwrt-linksys-wrt1200ac-webflash.bin

DECIMAL       HEXADECIMAL     DESCRIPTION
--------------------------------------------------------------------------------
0             0x0             TRX firmware header, little endian, image size:
28            0x1C            uImage header, header size: 64 bytes, header CRC
92            0x5C            Linux kernel ARM boot executable zImage (little-
2460          0x99C           device tree image (dtb)
23432         0x5B88          xz compressed data
23776         0x5CE0          xz compressed data
2117484       0x204F6C        device tree image (dtb)
3145756       0x30001C        UBI erase count header, version: 1, EC: 0x0, VID
```

help语法帮助信息

```
root@kali:~# binwalk -h

Binwalk v2.1.2
Craig Heffner, ReFirmLabs
https://github.com/ReFirmLabs/binwalk

Usage: binwalk [OPTIONS] [FILE1] [FILE2] [FILE3] ...

Signature Scan Options:
    -B, --signature             Scan target file(s) for common file signature
    -R, --raw=<str>             Scan target file(s) for the specified sequenc
    -A, --opcodes               Scan target file(s) for common executable opc
    -m, --magic=<file>          Specify a custom magic file to use
    -b, --dumb                  Disable smart signature keywords
    -I, --invalid               Show results marked as invalid
    -x, --exclude=<str>         Exclude results that match <str>
    -y, --include=<str>         Only show results that match <str>

Extraction Options:
    -e, --extract               Automatically extract known file types
    -D, --dd=<type:ext:cmd>     Extract <type> signatures, give the files an
    -M, --matryoshka            Recursively scan extracted files
    -d, --depth=<int>           Limit matryoshka recursion depth (default: 8
    -C, --directory=<str>       Extract files/folders to a custom directory (
    -j, --size=<int>            Limit the size of each extracted file
    -n, --count=<int>           Limit the number of extracted files
    -r, --rm                    Delete carved files after extraction
    -z, --carve                 Carve data from files, but don't execute extr
    -V, --subdirs               Extract into sub-directories named by the off

Entropy Options:
    -E, --entropy               Calculate file entropy
    -F, --fast                  Use faster, but less detailed, entropy analys
    -J, --save                  Save plot as a PNG
    -Q, --nlegend               Omit the legend from the entropy plot graph
    -N, --nplot                 Do not generate an entropy plot graph
    -H, --high=<float>          Set the rising edge entropy trigger threshold
    -L, --low=<float>           Set the falling edge entropy trigger threshol

Binary Diffing Options:
    -W, --hexdump               Perform a hexdump / diff of a file or files
    -G, --green                 Only show lines containing bytes that are the
    -i, --red                   Only show lines containing bytes that are dif
    -U, --blue                  Only show lines containing bytes that are dif
    -w, --terse                 Diff all files, but only display a hex dump o

Raw Compression Options:
    -X, --deflate               Scan for raw deflate compression streams
    -Z, --lzma                  Scan for raw LZMA compression streams
    -P, --partial               Perform a superficial, but faster, scan
    -S, --stop                  Stop after the first result

General Options:
    -l, --length=<int>          Number of bytes to scan
    -o, --offset=<int>          Start scan at this file offset
    -O, --base=<int>            Add a base address to all printed offsets
    -K, --block=<int>           Set file block size
    -g, --swap=<int>            Reverse every n bytes before scanning
    -f, --log=<file>            Log results to file
    -c, --csv                   Log results to file in CSV format
    -t, --term                  Format output to fit the terminal window
    -q, --quiet                 Suppress output to stdout
    -v, --verbose               Enable verbose output
    -h, --help                  Show help output
    -a, --finclude=<str>        Only scan files whose names match this regex
    -p, --fexclude=<str>        Do not scan files whose names match this rege
    -s, --status=<int>          Enable the status server on the specified por
```

rbasefind

- `rbasefind` ： 查找固件基地址
  - 概述：暴力查找固件在内存中的基地址的工具
  - 背景：在拿到固件的第一步，最重要的就是确定基地址，这样才能让 `IDA` 识别更多的函数和字符串
  - Github
    - https://github.com/sgayou/rbasefind
  - 用法举例

```
lys@ubuntu:~/Documents/test$ rbasefind u-boot.bin
Located 10 strings
Located 72155 pointers
Scanning with 8 threads...
0x80700000: 8
0xff22d000: 1
0xfe3a6000: 1
0xfdb83000: 1
0xfca84000: 1
0xfbf1d000: 1
0xfb632000: 1
0xf965e000: 1
0xf7bae000: 1
0xf777a000: 1
```

addelfinfo

- `addelfinfo`：为原始固件增加ELF头或节表，方便IDA反编译
  - 概述：为原始的二进制添加ELF头和节表，自研小工具
  - GitHub
    - https://github.com/liyansong2018/Tools2Firmware

sibyl

- `sibyl`：还原标准库中的符号表
  - 是什么：an enhanced API bruteforcing tool
  - 概述：sibyl 可以将一些原始的二进制文件中的标准库函数还原，识别库函数的符号表
  - Github
    - GitHub - cea-sec/Sibyl: A Miasm2 based function divination.
      - https://github.com/cea-sec/Sibyl
  - 其他类似/竞品工具
    - Bindiff
      - 基于 `CFG` 签名
        - `CFG` = `Control Flow Graph`
    - FindCrypt
      - 基于魔术常量 `magic constants`
    - FLIRT
      - 基于增强的模式匹配enhanced pattern matching
  - 语法

```
lys@ubuntu:~/Tools/miasm-0.1.1$ sibyl
Usage: /usr/local/bin/sibyl [action]

Actions:
  config   Configuration management
  find     Function guesser
  func     Function discovering
  learn    Learn a new function
```

  - 举例
    - 打印函数

```
sibyl func -a arml u-boot.bin.elf > funcs.txt
```

    - 转换函数

```
sibyl find -a arml -b ABI_ARM u-boot.bin.elf funcs.txt
```

    - 效果

```
Python>
Launch identification on 3085 function(s)
Found memcpy at 0x8057120
Found memmove at 0x805714c
Found memset at 0x8057174
Found strcat at 0x80571a8
Found strchr at 0x80571cc
Found strcmp at 0x8057208
Found strcpy at 0x8057228
Found strlen at 0x8057244
Found strncmp at 0x8057258
Found strncpy at 0x8057280
Found strnlen at 0x80572a8
Found strrchr at 0x80572c0
Found memcmp at 0x80572ff
Found strsep at 0x80576ac
Found strspn at 0x8057704
Found stricmp at 0x805799c
Found strpbrk at 0x8057ab8
Found strtok at 0x8057b30
Found strcmp at 0x8057b48
Found atoi at 0x805df1c
Current: 64.83% (sub_0x80b4ab3)| Estimated time remaining: 14.4
Found atoi at 0x80f1cf3
Current: 100.00% (sub_0x80f7a93)| Estimated time remaining: 0.0
Finished ! Found 21 candidates in 42.70s
Results are also available in 'sibyl_res'
```

miasm2

- `miasm2` ： 逆向分析
  - 概述：Miasm 是一个免费和开源（GPLv2）逆向工程框架。Miasm 旨在分析/修改/生成二进制程序，例如符号执行、沙盒模拟
  - GitHub
    - https://github.com/cea-sec/miasm

embedded-toolkit

- `embedded-toolkit`：跨平台的嵌入式程序
  - 概述：严格意义上来说，这并不是一个工具，而是一个编译好的工具集
  - 包括工具
    - `tcpdump` (statically linked
    - `gawk` (statically linked)
    - `lsof` (statically linked)
    - `gdbserv` (statically linked)
    - `tshd` (statically linked)
    - `mawk` (statically linked)
    - `libpcap` (static library, used for linking into tcpdump so not present in this repo)
  - 说明
    - 这些已经编译好的二进制，包含了多个平台，如 x86、arm、mips，如果不想花时间在交叉编译上，可以使用它们，但不保证二进制有没有安全问题
  - GitHub
    - https://github.com/akpotter/embedded-toolkit

BusyBox

- `BusyBox`：Linux基础工具集
  - 概述：BusyBox 是一个集成了三百多个最常用Linux命令和工具的软件
    - BusyBox 包含了一些简单的工具，例如ls、cat和echo等等，还包含了一些更大、更复杂的工具，例grep、find、mount以及telnet
  - 别称：Linux工具中的瑞士军刀
  - 主页
    - https://busybox.net/
  - 下载
    - https://busybox.net/downloads/binaries/

工控无线协议

从无线协议来说，工业领域中常会用到的无线协议有：

- WiFi
- 蓝牙
- Zigbee
- NFC
- 其他

WiFi

蓝牙

Zigbee

NFC

- NFC=近场通信
  - 工作模式：被动式
  - 工作频率：13.56MHz
  - 应用举例
    - 文字
      - 地铁一卡通
      - 门禁卡
      - 护照
      - Tesla Model 3的钥匙系统：Pektorn PKE
    - 图
    - 

  - NFC 攻击
    - Mifare Classic 的破解
      - 其他类型
        - iClass：某公司的门禁卡
        - Ultralight：某地铁的一次性车票
    - 破解工具=逆向工具
      - PM3=PROXMARK3
        - 号称：研究RFID的瑞士军刀
        - 用途：读取Tesla车卡或物理钥匙
      - NFCGate
        - https://github.com/nfcgate
      - Proxmark3

其他

工控操作系统

工业领域中有各种各样的设备，其中设备中用到的嵌入式操作系统有多种类型，常见的有下面这些：

- NoOS
- 有OS
  - 非实时操作系统
    - 嵌入式linux
    - WinCE
  - 实时操作系统RTOS
    - FreeRTOS
    - VxWorks
  - 其他

NoOS

Linux

WinCE

FreeRTOS

VxWorks

其他

工控各行业安全

工控相关领域很多，包含多个行业。

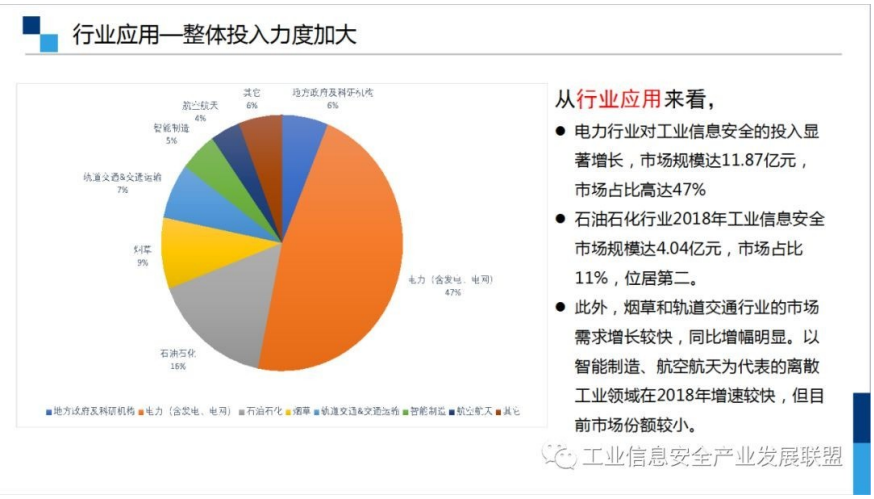
和安全有关的，常见的大的工业分类有：

- 先进制造
- 电力行业
- 轨道交通
- 石油石化
- 烟草行业
- 金属钢铁行业
- 其他行业

工控安全在各行业中的应用

总体概述：

总体投入力度加大：



先进制造

电力

轨道交通

石油石化

烟草

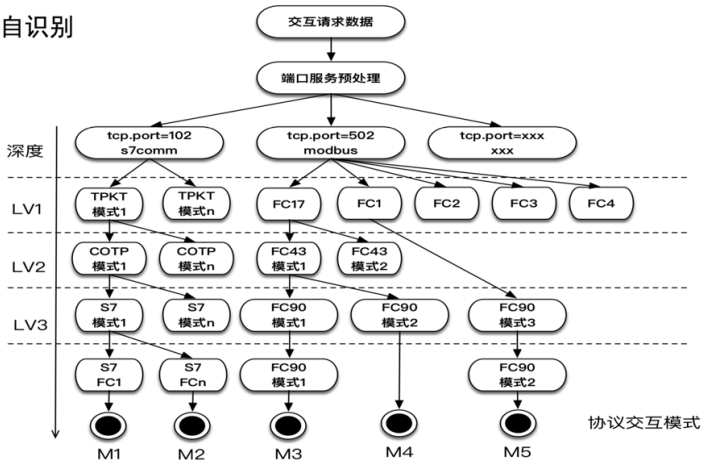
金属钢铁

其他行业

工控安全相关

交互行为模式

交互行为模式自识别



附录

下面列出相关参考资料。

名词术语

- 专业术语
  - `DCS = 分布式控制系统 = 集散控制系统`
  - `PCS = 过程控制系统`
  - `ESD = 应急停车系统`
  - `PLC = Programmable Logic Controller = 可编程序控制器`
  - `RTU = 远程终端控制系统`
  - `IED = 智能监测单元`
  - `HMI = Human Machine Interface = 人机界面`
  - `MIS = Management Information System = 管理信息系统`
  - `SIS = Supervisory Information System = 生产过程自动化监控和管理系统`
  - `MES = 制造执行管理系统`
  - Nday漏洞问题

参考资料

- 全国首个工业互联网安全研究院落户园区-名城苏州新闻中心
- 160077346356.mp4
- 2015年1月 – 灯塔实验室
- 加油站实时监测设备的一次全球统计报告（Tank Gauges Vulnerability Global Census Report） – 灯塔实验室
- 【工控网络协议专题
- 【工控网络协议专题-汇总】工控协议整理集合（更新ing）_qq_29864185的博客-CSDN博客
- ICS-Radar
- ZoomEye - Cyberspace Search Engine
- 【工控协议专题01】Modbus协议原理与安全性分析_qq_29864185的博客-CSDN博客
- 工控安全入门分析 - 路人甲
- 罗克韦尔自动化主页-罗克韦尔自动化（中国）有限公司
- 工控CTF技能点学习总结 - 知乎
- 安全态势 - 工业互联网安全应急响应中心
- OWASP中国苏州移动安全论坛 — OWASP-CHINA
- 网络空间工控系统威胁情报
- 对西门子PLC CPU运行状态的一次全球监测统计 – 灯塔实验室
- 工控行业全省工业系统威胁态势监测场景下的威胁态势感知平台应用 - FreeBuf网络安全行业门户
- 工控系统网络安全，一场没有硝烟的战争 - 知乎
- 浅析工控安全行业 - 知乎
- IOTE 2019第十一届国际物联网展--苏州站-在线订票-互动吧
- IOTE2021国际物联网博览会*苏州物联网展*会物联网展*物联网大会_RFID展*会NBIoT展会_ LORA展会
- 0315E11245SergeyGordeychik.pdf
- 车联网安全系列——特斯拉 NFC 中继攻击（CVE-2020-15912）
- 青藤云安全：ATT&CK框架迎来重大变革，“子技_苏州造型培训学校|苏州化妆|美容|摄影|美发|美甲|纹绣
- 一文看懂ATT&CK框架以及使用场景实例 - 安全客，安全资讯平台
- MITRE ATT&CK 框架“入坑”指南 - 安全牛
- Matrix - Enterprise | MITRE ATT&CK®
- Matrix - Mobile | MITRE ATT&CK®
- Matrix - PRE-ATT&CK | MITRE ATT&CK®
- mitre-attack/attack-navigator: Web app that provides basic navigation and annotation of ATT&CK matrices
- 一文看懂ATT&CK框架以及使用场景实例 - 安全客，安全资讯平台
- What Is MITRE ATT&CK and How Is It Useful? | From Anomali
- What are STIX/TAXII? | Anomali
- 特斯拉工厂遭黑客攻击暴露工控危机 360加码政企安全织密防护网|工业互联网*新浪财经*新浪网
- 360政企安全
- FirmwareTotal-360固件自动化安全分析平台 - 云+社区 - 腾讯云

- Firmware Total
- 这个D-Link不愿修复的高危漏洞，影响面被严重低估了！
- 启明星辰-先进制造业的工控安全解决方案_宇之成信息技术（苏州）有限公司
- 基于Modbus协议认证漏洞的数据包伪造方法研究
- FirmwareTotal-360固件自动化安全分析平台 - 云+社区 - 腾讯云
- Nmap NSE脚本
- Modbus PLC攻击分析：Smod渗透框架研究 - FreeBuf网络安全行业门户
- Modbus PLC攻击分析：从Modbus PollSlave到M340 - FreeBuf网络安全行业门户
- Modbus PLC攻击分析:Python和Mbtget读写PLC - Sec' Hotspot
- 工控安全入门（一）—— Modbus协议 - 安全客，安全资讯平台
- 基于Modbus协议认证漏洞的数据包伪造方法研究—控制网
- 基于Modbus协议认证漏洞的数据包伪造方法研究
- Modbus协议与S7Comm协议浅析 - Sec' Hotspot
- Modbus通讯协议学习 - 认识篇 - 失踪人口 - 博客园
- 十部门关于印发加强工业互联网安全工作的指导意见的通知*部门政务*中国政府网
- 工业互联网安全应急响应中心
- 专家：风险分析是工业互联网安全的基础-新华网
- 深入研究IcedID银行木马的最新版本 - 工业互联网安全应急响应中心
- 中国工业互联网安全态势报告（2018） - 白皮书 - 工业互联网产业联盟
- 孙利民：我国工业互联网安全现状令人堪忧 - 通信产业网 - 中国通信第一产经门户
- 国家顶层设计出台工业互联网安全产业注入“强心剂”-中共中央网络安全和信息化委员会办公室
- 政策解读《工业互联网企业网络安全分类分级指南（试行）》 - 知乎
- 工业互联网平台安全的思考 - 安全内参 | 决策者的网络安全知识库
- 工业互联网安全“三大痛点”如何破解———周鸿祎委员开出一剂药方 - 中国日报网
- 嵌入式设备漏洞研究员
- ReFirmLabs/binwalk: Firmware Analysis Tool
- Binwalk工具的详细使用说明*运维*子曰小玖的博客-CSDN博客
- binwalk windows安装和使用方法 - pcat - 博客园
- 自动提取文件系统---binwalk(一） - blacksunny - 博客园
- Binwalk：固件分析利器 – ArkTeam
- Binwalk | Penetration Testing Tools
- BinWalk安装和命令参数详解 - 云+社区 - 腾讯云
- 灯塔实验室 - 团队出品
- 知风-互联网联网工控资产与企业分析系统
- 【关注】2018年工业信息安全技能大赛西部赛区十强诞生！
- 安全设备的漏洞挖掘-智能设备-看雪论坛-安全社区|安全招聘|bbs.pediy.com
- [原创]固件安全之加载地址分析-智能设备-看雪论坛-安全社区|安全招聘|bbs.pediy.com
- 固件逆向中常用的小工具_MagicSong-CSDN博客
- 工控漏洞挖掘方法之固件逆向分析
- iot初体验 摄像头固件提取 看雪论坛
- 个人经验泛谈之工控安全入门 - panda | 热爱安全的理想少年
-