

目录

前言	1.1
工控安全概览	1.2
工控协议	1.3
常见协议	1.3.1
ATG	1.3.1.1
Modbus	1.3.1.2
Siemens S7	1.3.1.3
测试脚本	1.3.2
工控系统和产品	1.4
工控设备扫描	1.5
工控攻击	1.6
工控渗透	1.6.1
工控安全工具和框架	1.7
ATT & CK	1.7.1
STIX and TAXII	1.7.1.1
工控固件	1.8
工控固件提取	1.8.1
工控固件分析	1.8.2
binwalk	1.8.2.1
工控漏洞	1.9
漏洞分析	1.9.1
工控安全相关	1.10
附录	1.11
名词术语	1.11.1
参考资料	1.11.2

工控安全概览

- 最新版本: v0.6
- 更新时间: 20201027

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，工控协议测试脚本，工控产品，工控相关框架和工具等。

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

此电子书教程的全部内容，如无特别说明，均为本人原创和整理。其中部分内容参考自网络，均已备注了出处。如有发现侵犯您版权，请通过邮箱联系我 admin 艾特 [crifan.com](#)，我会尽快删除。谢谢合作。

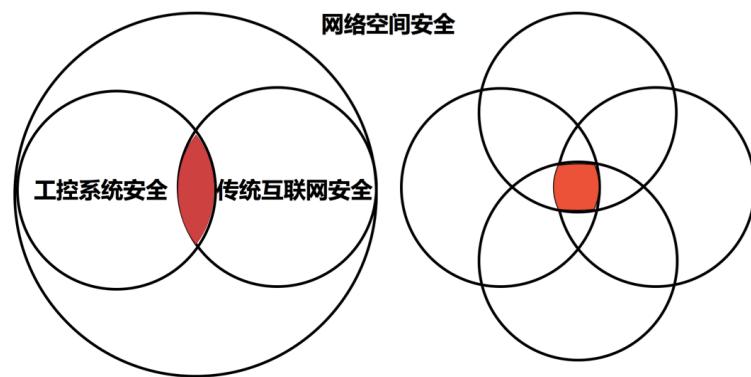
鸣谢

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。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 20:00:12

工控安全概览

- 工控安全和传统互联网安全关系

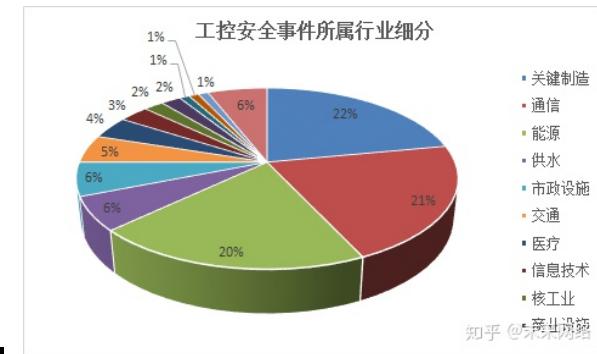


- 工控安全，即在工控领域的安全相关技术的统称

- 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



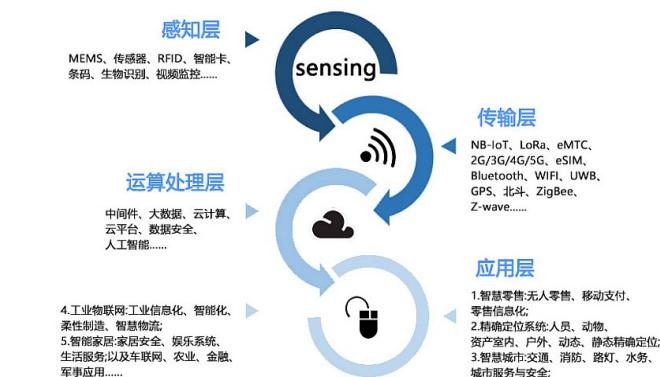
- 但目前工控市场安全只覆盖到了其中部分行业，要实现全面防护还有许多路要走

工业安全领域投入份额



- 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
- 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
- 工控安全的漏洞利用方法
 - 工控领域常见漏洞利用方式
 - 组态利用
 - 通信劫持
 - Web渗透

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

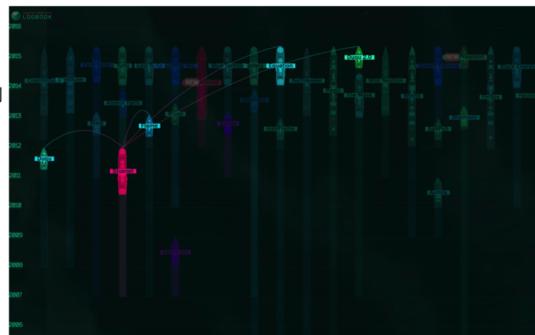
工控系统威胁情报

国家关键信息基础设施

针对能源、关键制造等行业的威胁加剧
Stuxnet/Duqu/Flame
BlackEnergy

针对SCADA系统的威胁加剧
远程可控制SCADA、PLC
遍布互联网的工控资产
针对工控专有协议的探测

针对工控设施的威胁行为更值得研究
全球网络空间“底线”
具备上层战略特征



<https://apt.securelist.com>

crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook最后更新：2020-10-29 19:46:06

工控协议

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:46:58

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协议是应用于控制器上的一种协议。通过此协议设备。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协议族的协议，使用s7-应用接口的通信不依赖于线系统。 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 Communication Protocol for Building Automation 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(EIA-485)对采暖、通风、空调、制冷控制设备同时也为其他楼宇控制系统（例如保安、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 6004-5-91。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 Protocol 网络协议 是一种应用于自动化组件的协议，常见于电力、水处理等行业。SCADA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 Process Control)。OPC包括一整套接口、方法的标准集，用于过程控制和制造系统

工控协议	传输协议	端口	说明
OPC DA	TCP	135	OPC (OLE for Process Control, 基于OLE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) : OPC 标准，通过提供一个完整的、可靠的跨平台的架构，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 、 Ethernet 网络所采用
Tridium Niagara Fox	TCP	1911	Fox协议是Tridium公司开发的Niagara的一部分，广泛应用于楼宇自动化控制
Crimson V3	TCP	789	
PCWorx	TCP	1962	PCWorx协议由菲尼克斯电气公司开发，广泛使用于工控系统。PCWORX是菲尼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的实时操作系统。它是一个高性能的PLC运行时引擎，目的在于基于嵌入式和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络通讯，该系列设备可以提供高速、数据处理和机器控制
IEC-61850 = MMS + goose + SV	TCP	102	输配电通讯协议。IEC 61850标准是自动化领域唯一的全球通用标准。它的实现，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得简单和透明
GE SRTP	TCP	18245	GE-SRTP协议由美国通用电气公司提出，PLC可以通过GE-SRTP进行数据冗余传输
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统一的接口标准来推进网络视频在安防市场上的应用。该接口标准将确保不同厂商生产的设备具有互通性
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/II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，由罗克韦尔公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公司推动的开放式通讯协定
HART-IP	TCP/UDP	5094	HART协议是美国Rosement公司提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表
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。欧姆龙网络协议FINS进行通信，可通过多级网络，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，定义了一对多应用程序如何有效地传送多媒体数据
SIP	TCP	5060	SIP协议是由IETF制定的多媒体通信协议。SIP的开发目的是用来帮助提供跨域电话业务

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技术所使用的协议
SAE J1939			一种CAN的变种，适用于农业车辆
USITT DMX512-A			灯光控制数据传输协议
BSSAP/BSAP			由Bristol Babcock Inc发展的通讯协议
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 Lion G306工控系统的HMI人机接口
Fox	TCP	1911	Fox协议是Tridium公司开发的Nias的一部分，广泛应用于楼宇自动化控制
secure-fox	TCP	4911	Fox协议是Tridium公司开发的Nias的一部分，广泛应用于楼宇自动化控制
moxa-nport	UDP	4800	Moxa串口服务器专为工业应用而设计，配置组合的串口服务器更能符合不同的需求。NPort系列串口服务器让1/2/4路RS232/422/485设备立即联网，提供1/4路串口联网解决方案
codesys	TCP	2455	CoDeSys编程接口在全球范围内连接上百个设备制造商的自动化设备，该编程接口

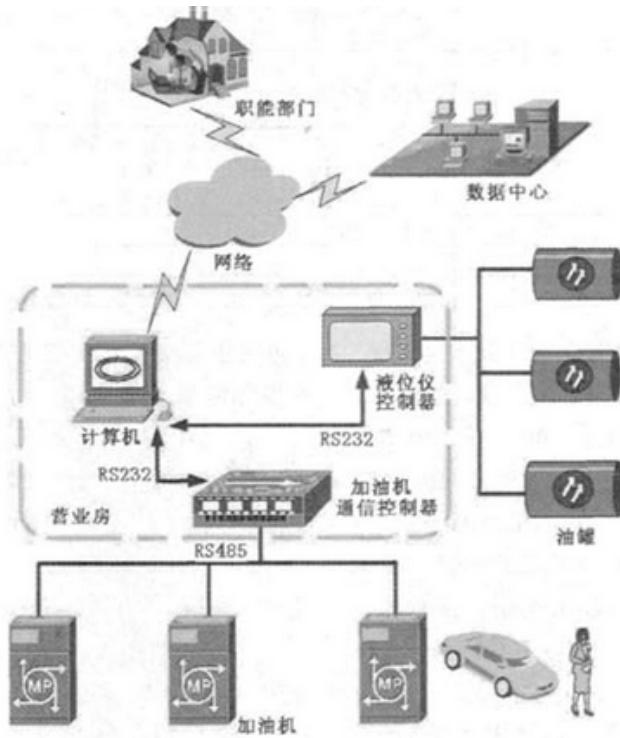
工控协议	传输协议	端口	说明
ddp	TCP/UDP	5002	DDP协议 (DTU DSC Protocol) 是DSC之间的通讯协议，DDP是一种私有公开性质的通信协议，用于数据DTU管理
lantronix-udp	TCP	30718	Lantronix串口服务器专为工业应用设计，串口服务器是一种具有串口转以太网功能的设备，它能将RS-232/485/422串口转为TCP/IP网络接口，串口服务器广泛应用于SCADA数据采集环节上，用于解决串口与太网的通信问题
wdbrpc	TCP	17185	VxWorks是世界上使用最广泛的一系列嵌入式系统中部署的实时操作系统，是由WindRiver公司于1983年设计开发的。VxWorks系统在工业控制领域应用广泛，WDB RPC是VxWorks的远程调试接口。
dahua-dvr	TCP	37777	DAHUA-DVR协议是浙江大华安防公司私有通信协议，该协议用于实时视频传输。
vstarcam-udp	UDP	8600	VSTARCAM-UDP协议是威视达康公司的私有通信协议，该协议用于获取摄像头的网络配置等信息。
CSPV4	TCP	2222	CSPV4是可以识别PLC5/SLC 500模块；罗克韦尔的SLC 500功能强大的指令集、丰富的输入输出模块，适用于现场恶劣的工作环境而设计。
general-electric-srtcp	TCP	18245	GE-SRTCP协议由美国通用电气公司提出，PLC可以通过GE-SRTCP进行数据冗余传输。
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业。
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业。
beckoff-ads	UDP	48899	Beckhoff-ads是一种私有协议，用于PLC的通讯，常见于风力发电等行业。
hollysys-lk	UDP	6000	Hollysys-lk协议是一种私有协议，用于Hollysys PLC的通讯，常见于电力、化工等行业。
hollysys-macs	UDP	8000	Hollysys-macs协议是一种私有协议，用于Hollysys DCS的通讯，常见于电力、化工等行业。

工控协议	传输协议	端口	说明
siemens-license	TCP	4410	Siemens License协议是一种私有协议，用于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Foxboro系统的通讯，常见于电力、石油、化工等工业领域
ilon-smartserver	TCP	1628	ILON-SMARTSERVER协议是ECI生产的iLon系列产品的私有通信协议。该系列产品可以广泛的应用于工业控制领域，类似于一台服务器，提供数据采集、处理、存储和转发等功能。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by Gitbook最后更新: 2020-10-29 19:46:52

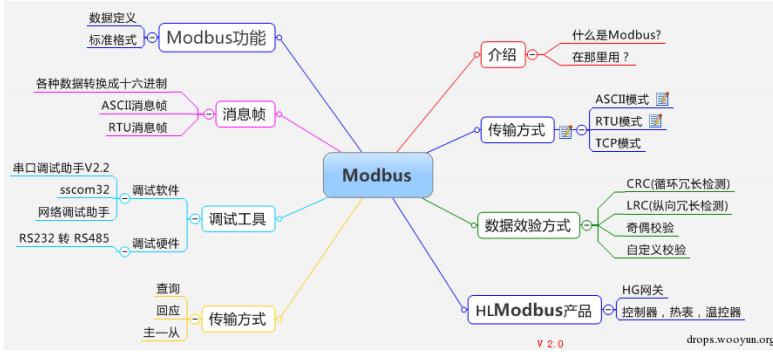
ATG

- 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



crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:46:10

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。
- 

The diagram illustrates the Modbus protocol architecture. At the center is a blue box labeled "Modbus". Various components are connected to it:

 - Modbus功能 (Modbus Functions):** Connected to "消息帧" (Message Frame).
 - 介绍 (Introduction):** Connected to "什么是Modbus?" (What is Modbus?) and "在那里用?" (Where is it used?).
 - 传输方式 (Transmission Methods):** Connected to "ASCII模式" (ASCII Mode), "RTU模式" (RTU Mode), and "TCP模式" (TCP Mode).
 - 数据效验方式 (Data Checksum Methods):** Connected to "CRC(循环冗长检测)" (CRC), "LRC(纵向冗长检测)" (LRC), "奇偶校验" (Parity Check), and "自定义校验" (Custom Checksum).
 - HLModbus产品 (HLModbus Products):** Connected to "HG网关" (HG Gateway) and "控制器, 热表, 温控器" (Controller, Thermometer, Temperature Controller).
 - 查询 (Query):** Connected to "回应 (Response)" and "主一从 (Master-Slave)".
 - 调试工具 (Debug Tools):** Connected to "串口调试助手V2.2" (Serial Port Debug Assistant V2.2), "sscom32" (sscom32), "调试软件" (Debug Software), "网络调试助手" (Network Debug Assistant), and "RS232 转 RS485" (RS232 to RS485).
 - Modbus功能 (Modbus Functions):** Connected to "标准格式" (Standard Format) and "各种数据转换成十六进制" (Convert various data to hexadecimal).

V 2.0 drops.wooyun.org
- 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

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-10-29 19:46:12

Siemens S7

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:46:56

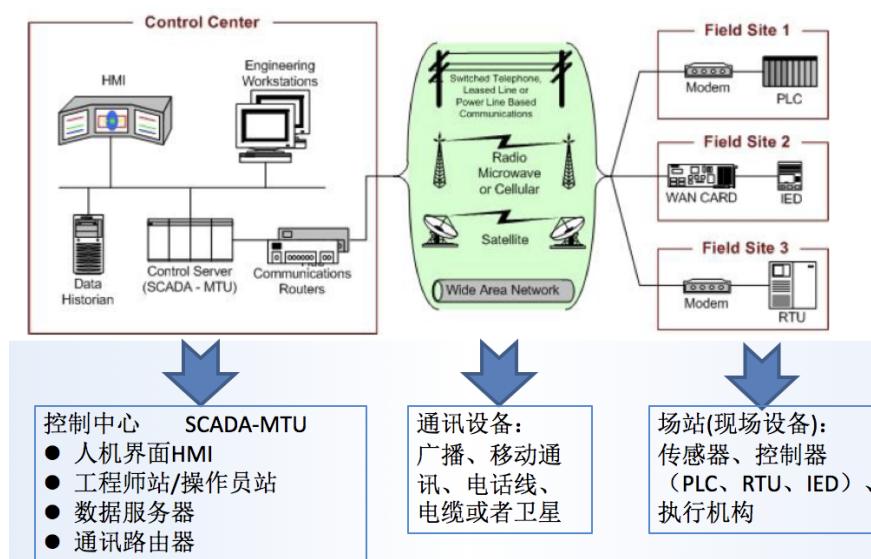
测试脚本

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:47:02

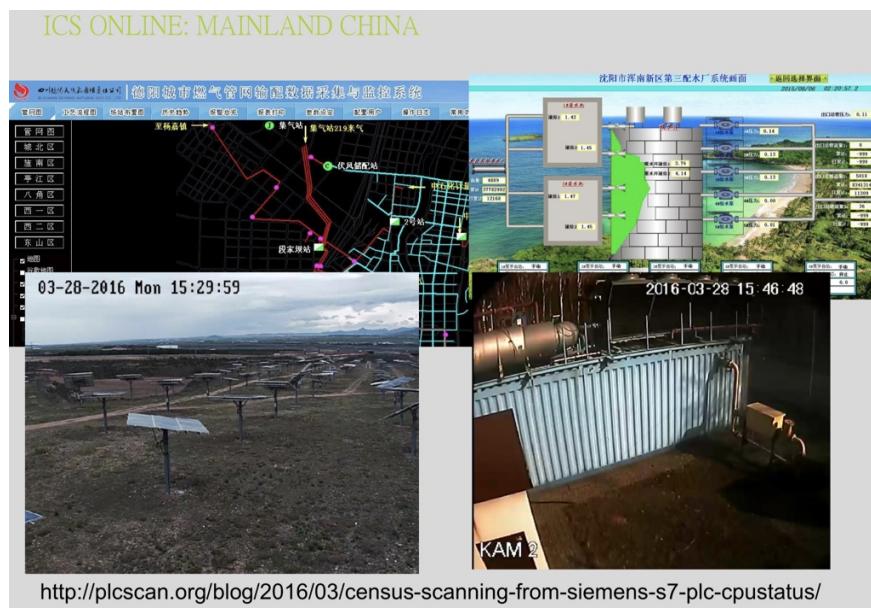
工控系统和产品

工控系统

典型工控系统架构



真实的工控系统举例



crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by Gitbook 最后更新: 2020-10-29 19:47:07

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 detecting 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/>

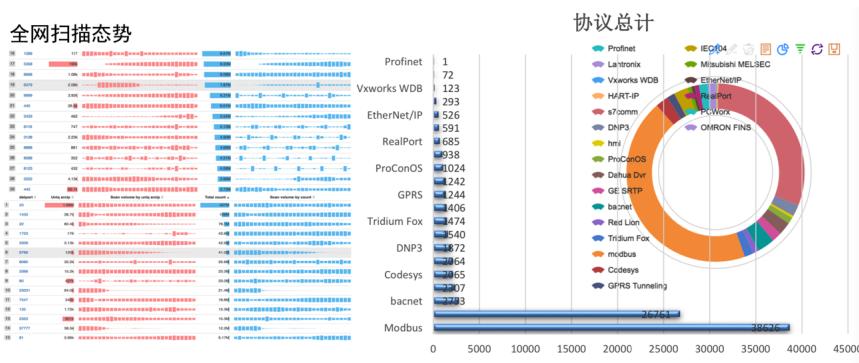
Internet connected ICS/SCADA/PLC Cheat Sheet 2013

Gleb Gritsai, Alexander Timorin, Alexander Zaitsev, Sergey Gordeychik, Valentin Shilnenkov

www.scadastrangelove.org

举例：

全网扫描和相关工控协议



工控安全全球检索网站和系统

- ICS-Radar

- http://radar.wincssec.com/html/search/search_topic.html



- Shodan搜索

- <https://www.shodan.io>



- 举例

Top Cities
Shenyang

218.61.155.234
China Unicorn Liaoning
Added on 09.02.2014
Shenyang
Details

Product name: DVP12SE
Vendor ID: Delta Power Electronics Center
Serial number: 0
Device type: Generic Device (deprecated)

drops.wooyun.org

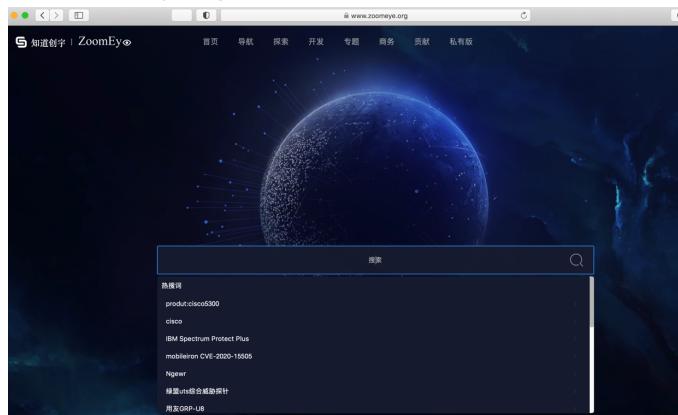
- Zoomeye搜索

- 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

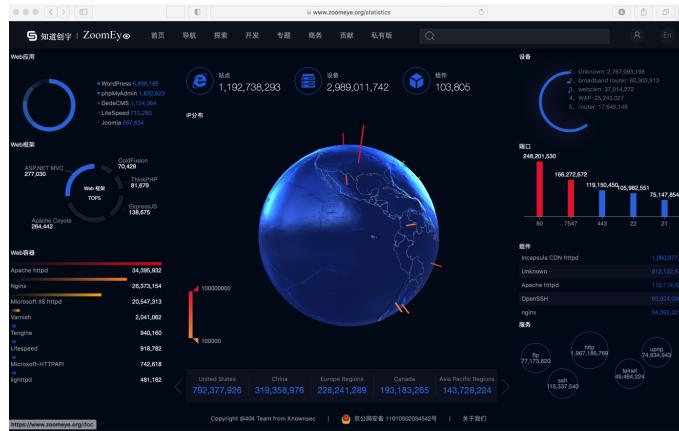
- ZoomEye - Cyberspace Search Engine

- <https://www.zoomeye.org>



- ZoomEye - Cyberspace Search Engine

- <https://www.zoomeye.org/statistics>



○ 举例

The screenshot shows the ZoomEye search results for "port:502". The results table includes columns for IP, Service, and Last Seen. One entry is highlighted:

IP	Service	Last Seen
31.209.*.*	Iceland Reykjavik	2015-08-21

• 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>

The screenshot shows the Diting homepage with the following sections:

- 谛听** 工控资产发现 安全工控服务 工控设备 用户手册 国内成员 国外成员
- 谛听网闻之万物 探尾龙潜渊以补天**
- 谛听工控设备** 搜索联网工控设备, 定位工控系统位置
- 谛听模块** 为了得到更精确的查询结果, 请从用户手册中的功能模块中选择对应的谛听模块
- 谛听能为你做什么**
 - 搜索工控设备
 - 发现网络安全威胁
 - 数据可视化分析
- ©2015-2020 谛听(上海)网络科技有限公司 | 工控安全堡垒

• Censys 全网引擎

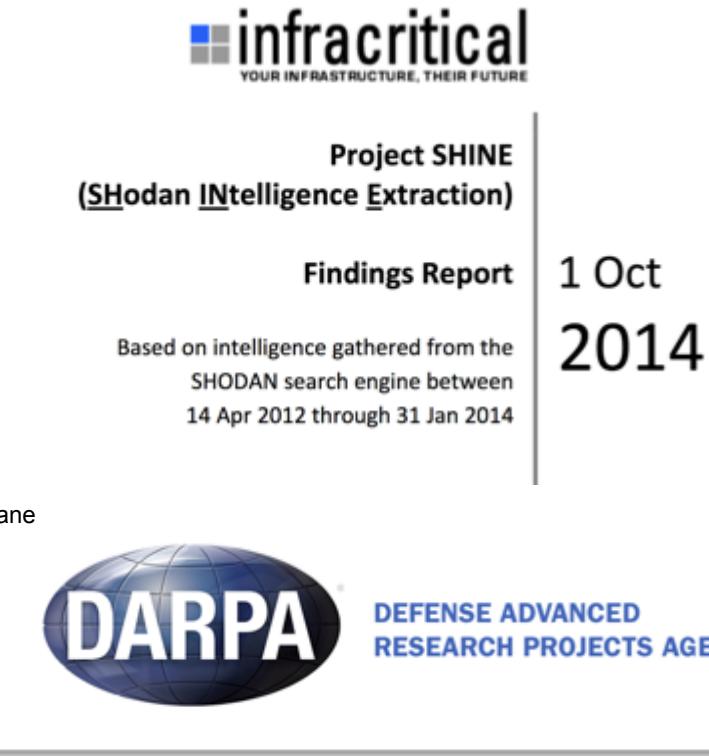
○ 概述

- 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

国外针对网络空间的情报收集计划

- SHINE计划——Project Shodan Intelligence Extraction



- X-Plane



[Defense Advanced Research Projects Agency](#) > Program Information

Plan X

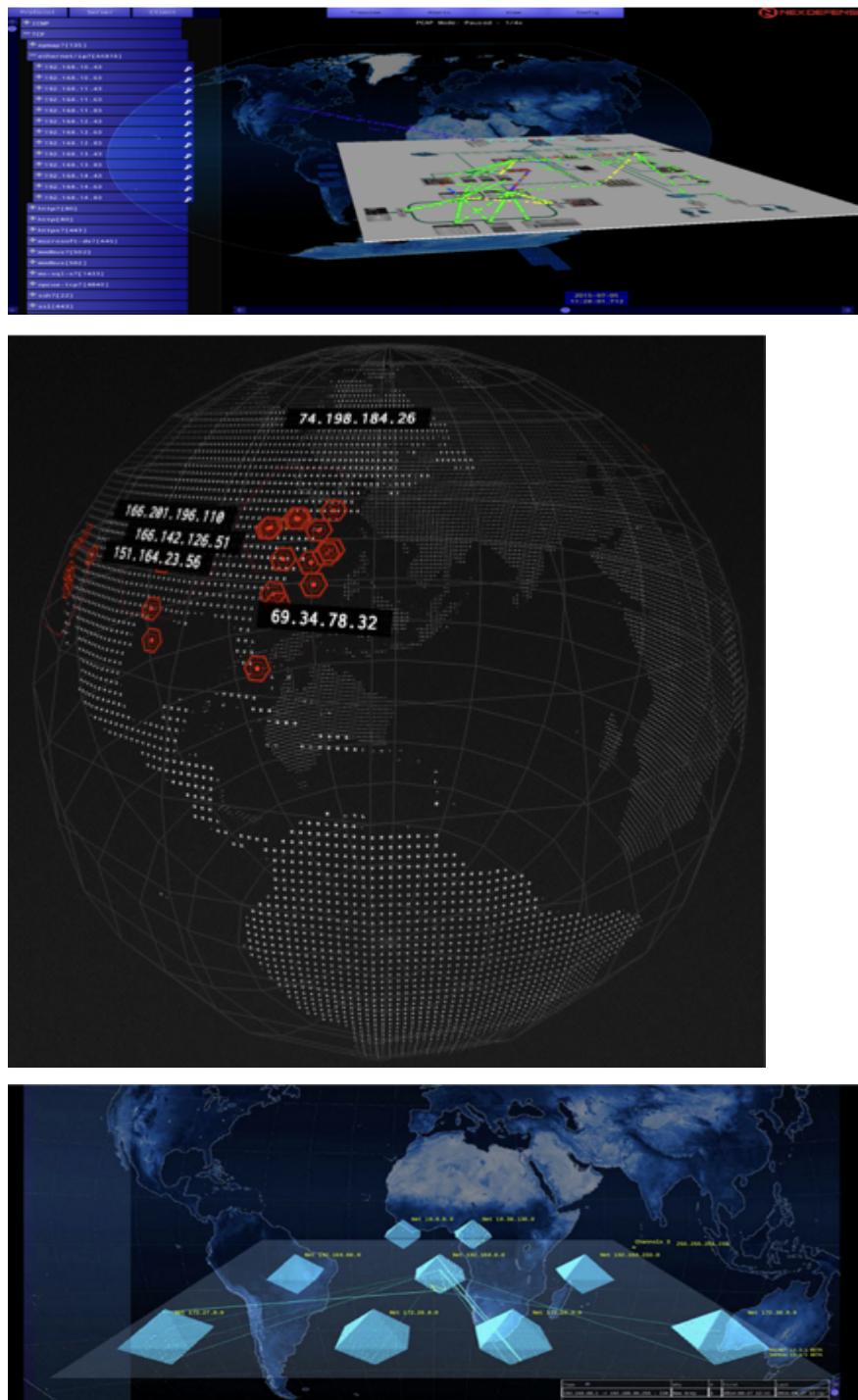
◦ [Mr. Frank Pound](#)

- Treasure Map
- NCR

扫描后

绘制网络空间地图，构建上帝视角感知能力

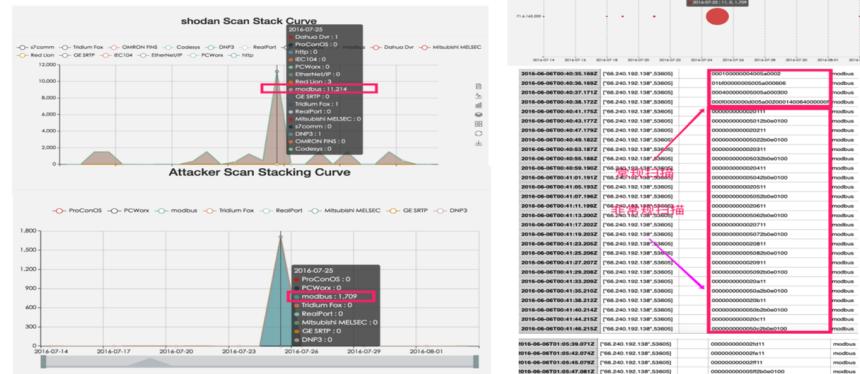
一般扫描出设备和风险、漏洞、威胁后，为了便于直观理解，往往会去绘制空间图。



出情报

扫描后，就可以给出总结报告，情报了：

Shodan组织战术威胁情报



crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:45:37

工控攻击

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:45:34

工控渗透

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:45:31

工具和框架

相关领域名词

蜜罐HonyPot

举例

通过Shodan搜索国外蜜罐

通过Shodan搜索国外蜜罐案例

103.6.87.106
Host Virtual
Location: 103.6.87.106, 16-09-01 04:11:29 GMT
India, Chennai
Details

23.106.59.127
Noble Technology Group, LLC
Location: 23.106.59.127, 16-09-01 04:11:29 GMT
United States, Phoenix
Details

162.218.89.26
ColoCrossing
Location: 162.218.89.26, 16-09-01 04:11:29 GMT
United States, Buffalo
Details

Shodan API

```
host = api.host('xxx.xxx.xxx.xxx', history=True)
```

Location designation of a module:
Copyright: Original Siemens Equipment
Module type: IM151-8 PN/DP CPU
PLC name: PG[random.random()*.1] f
Module: v.0.0
Plant identification: Power Generation One
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 8675399

Port: 102
Banner: Location designation of a module:
Copyright: Original Siemens Equipment
Module type: CPU 226
PLC name: Czajka-STUDOS
Module: v.0.0
Plant identification: MPWIK-ZOS-Czajka
OEM ID of a module:
Module name: Siemens, SIMATIC, S7-200
Serial number of module: 6E57 216-2AD23-0XB0

TIME: 2016-07-29T05:42:17.030523

存在问题

工控蜜罐存在的问题

易被甄别

针对工控协议的仿真交互低
配置繁琐容易留下疏漏
缺少针对工控业务的仿真

难管理

蜜罐部署繁琐
不具备分布式管理机制

难分析

数据日志机制陈旧
数据量增多难以分析
不具备结合威胁情报的能力

Anti-Honeypot Technology

Thorsten Holz

Laboratory for Dependable Distributed Systems

holz@informatik.rwth-aachen.de



RWTHAACHEN

cymmetria



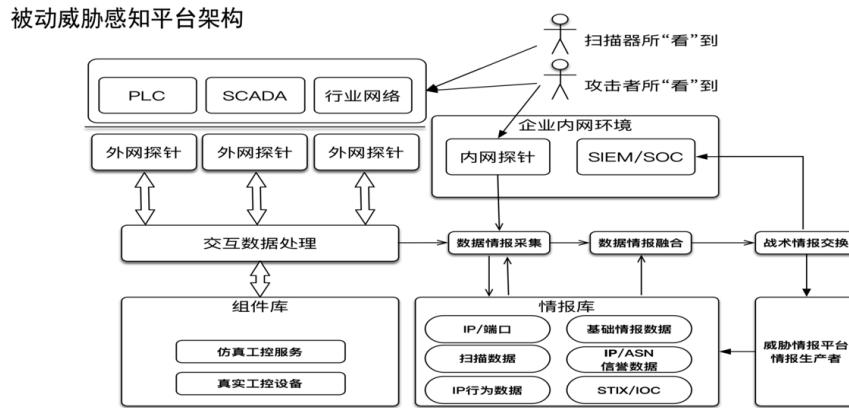
Breaking Honeypots for Fun and Profit

Dean Sysman
Itamar Sher
Gadi Eron



被动威胁感知

被动威胁感知平台架构



crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:46:02

ATT & CK

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:45:56

STIX and TAXII

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:45:58

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提取
- 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
- 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
- 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

crifan.com，使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-10-29 19:45:53

工控固件提取

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:45:50

工控固件分析

工控固件分析工具

常见的固件分析工具和系统有：

- binwalk
- BAT = Binary Analysis Toolkit
- FAT = Firmware-Analysis-Toolkit
- AttifyOS
- eimgfs
 - nlitsme/eimgfs: Tool for editing Windows CE/Mobile firmware images.
 - <https://github.com/nlitsme/eimgfs>

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-10-29 19:45:47

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

The diagram illustrates the integration of Binwalk with several key features. At the center is a dark blue rectangular box labeled "Binwalk". Five orange lines radiate from this central node to five light blue oval shapes, each representing a different functionality: "过滤功能" (top-left), "提取文件" (top-right), "比较功能" (bottom-left), "字符串分析" (bottom-center), and "插件功能" (bottom-right). In the bottom right corner of the slide, there is a small logo for "ArkTeam" featuring a stylized sailboat icon.
 - 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

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 sequence
  -A, --pcodes              Scan target file(s) for common executable opcodes
  -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 <ext>
  -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 (<str>)
  -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 extracted files
  -V, --subdirs               Extract into sub-directories named by the offset

Entropy Options:
  -E, --entropy               Calculate file entropy
  -F, --fast                  Use faster, but less detailed, entropy analysis
  -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 threshold

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

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 regex
  -s, --status=<int>           Enable the status server on the specified port

```


工控漏洞

真实案例

PLC攻击

真实的捕获案例

```
#向DB1数据区写入数据
2016-02-10 15:25:44 [209.133.66.214] Write request, Area : DB1, Start : 0, Size : 452 --> OK
2016-02-10 15:25:45 [209.133.66.214] Write request, Area : DB1, Start : 452, Size : 60 --> OK
#向DB1、2、3数据区写入数据
2016-02-22 06:54:19 [93.115.95.202] Write request, Area : DB1, Start : 0, Size : 16 --> OK
2016-02-22 06:54:19 [93.115.95.202] Write request, Area : DB2, Start : 0, Size : 16 --> OK
2016-02-22 06:54:19 [93.115.95.202] Write request, Area : DB3, Start : 0, Size : 16 --> OK
#删除CPU程序块
2016-02-22 06:54:43 [93.115.95.202] CPU Control request : Block Insert or Delete --> OK
#冷启动PLC CPU
2016-02-22 06:58:09 [37.48.80.101] CPU Control request : Warm START --> OK
#停止PLC CPU
2016-02-22 06:58:21 [37.48.80.101] CPU Control request : STOP --> OK
#修改PLC系统时间
2016-02-22 07:03:02 [37.48.80.101] System clock write requested
```

- 攻击动作
 - 写内存数据
 - 操作CPU状态
 - 修改系统时钟
 - 删除系统程序
 - 攻击影响
 - 数据异常
 - 程序停止运行
 - 系统时间异常
 - 系统运行故障

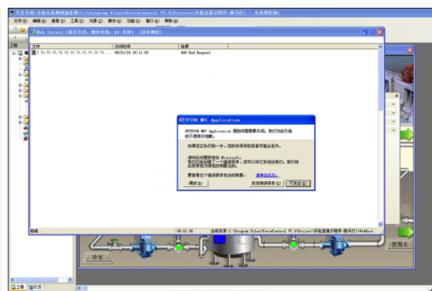


2016-02-22 07:03:02 [37.48.80.101] System clock write requested

GrimmEltonpa1	7673	56	d	epona.grimmett.[46.24.16]
MarioEltonpa1	7646	50	d	139.172.99.173.[39.59.172.93]
Eltonpa1	7645	50	d	139.172.99.173.[39.59.172.93]
Eltonpa1	7640	50	d	139.172.99.173.[39.59.172.93]
Eltonpa1	7572	445	d	[139.172.99.173.19]
kroabrum	7570	38	d	62.210.125.130.en.poneyelecom.eu.[B210.125.130]
relyingonthehappycats	7565	299	d	bawlo melon.l.[82.210.174.201]
fux3e	7564	13	d	ter.sebastianshaban.net.[78.47.8.110]
DigiGestor2eZ	7551	17	h	ter2e.digitale-gesellschaft.ch.[78.10.104.243]
Winter	7498	24	d	ter2-exohd.ohmnet.[146.165.177.103]

HMI溢出

针对HMI的溢出攻击



crifan.com, 使用署名4.0国际(CC BY 4.0)协议发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:47:13

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	漏洞原因	漏洞描述
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	VIA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	放统计代码，站长一秒钟变 APT 攻击专家 (wooyun-2012-09025 缝)
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	天津森然智能 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	姜堰市自来水公司 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 http://wooyun.org

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关键字的搜索：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

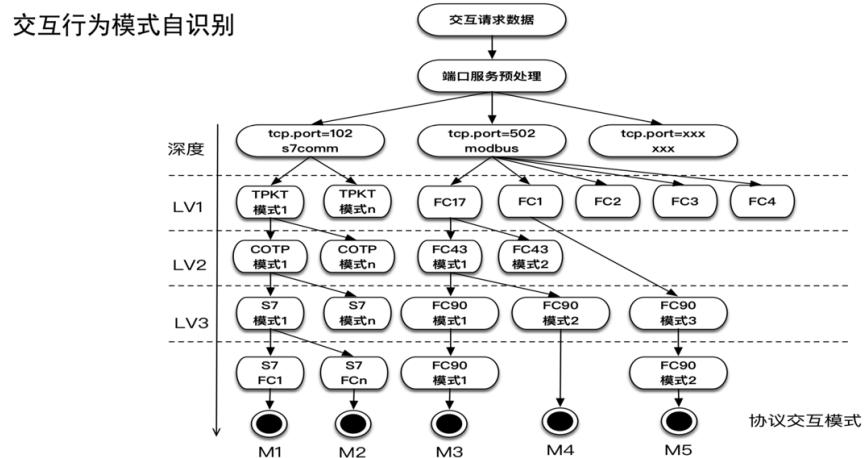
乌云工控相关的精华漏洞如下7个，在思路亮点中分析了漏洞的核心，同样也可能是获得打雷精华的理由。几乎共同点均是操控了对应的工控系统

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	scansf
wooyun-2015-116558	某电厂监管系统缺陷可能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-one
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-one
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-one
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

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:47:10

工控安全相关

交互行为模式



crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:47:04

附录

下面列出相关参考资料。

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:45:17

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

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新: 2020-10-29 19:45:27

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

crifan.com, 使用[署名4.0国际\(CC BY 4.0\)协议](#)发布 all right reserved, powered by
Gitbook最后更新：2020-10-29 19:45:23