Came Saw Conquered

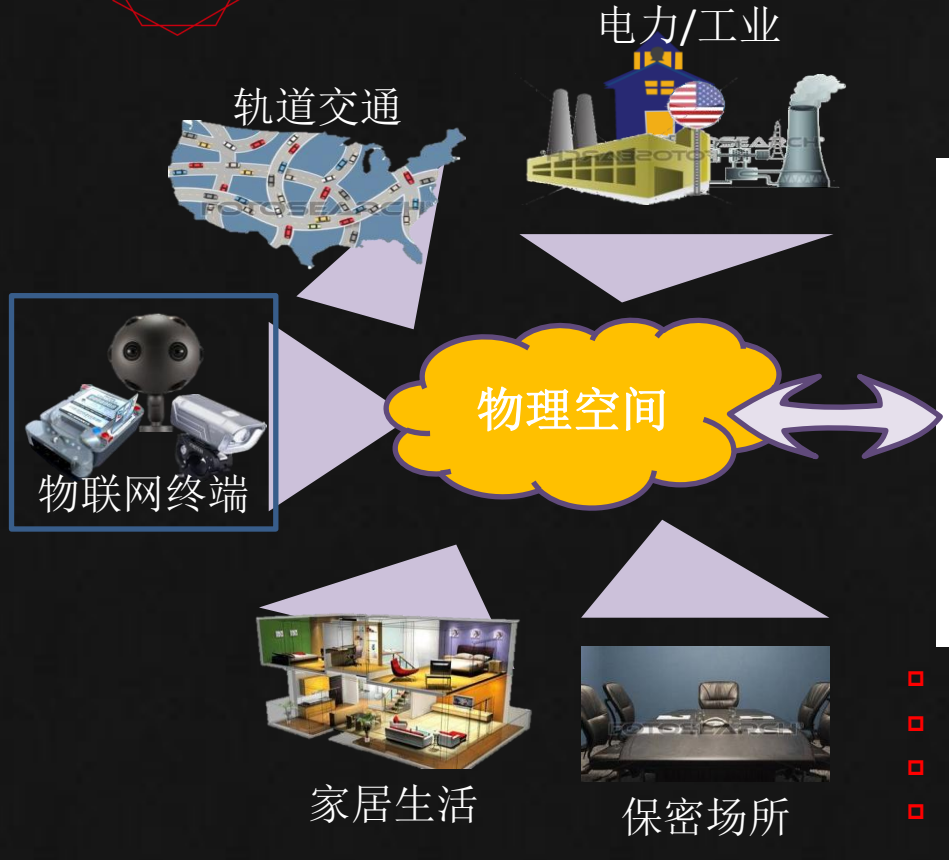
网络空间中的IoT安全

ID：ppprince
From:中国科学院信息工程研究所
物联网信息安全北京市重点实验室
yanzhaoteng@iie.ac.cn

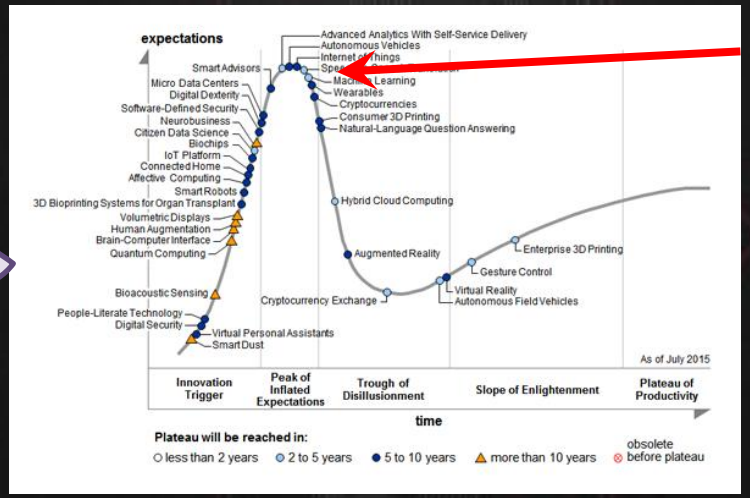
Part. 01

引言

物联网时代的到来



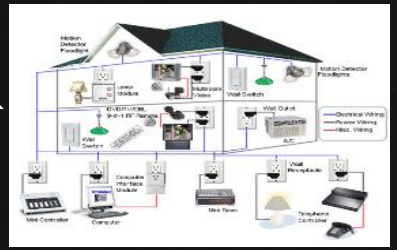
Emerging Technologies of 2015



- 2013年，物联网处于上升期
- 2014年，物联网取代大数据登上了成熟度曲线的最高点
- 2015年，物联网仍位于顶点
- 联网设备数：2015年49亿，2020年260亿(Gartner)

物联网时代的到来

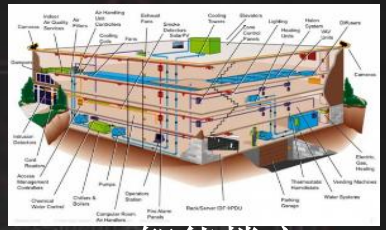
智能家居



可穿戴计算

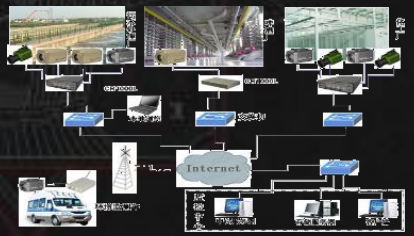
城市供水和燃气

泛在的设备互联



智能楼宇

智能电网



城市视频监控

物联网带来变革

- 改变了生活方式的改变，更加便利和智能（智能家居、智能医疗）
- 改变了生产方式、提高生产力（工业互联网、农业互联网）
- 改变了管理模式（智慧社区、智能城市）
- 推进了社会的发展历程

万物互联到物联网搜索

网络空间

互联网体系

搜索空间的拓展

从人类世界到物理世界
从文档网页到实体设备

物理空间

物联网体系

搜索引擎将庞大、复杂的互联网资源从地址索引映射为内容索引

- 成为信息与知识发现的入口
- 提升了用户访问接口的语义层次
- 降低了用户使用网络资源的门槛
- 是互联网高速发展的核心催化剂

Google 必应 微软搜索 Baidu 百度 SOSO 搜搜

物联网搜索使搜索对象从文档网页扩展到异构实体设备和动态数据流

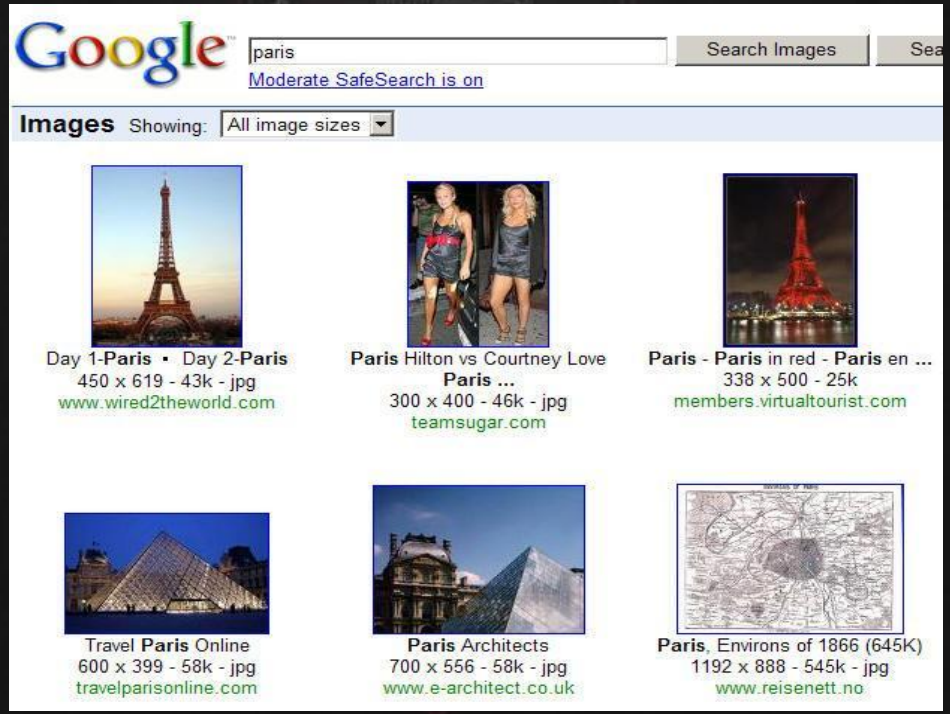
- 搜索对象规模与复杂性膨胀
- 资源容量和复杂程度显著提升
- 实体资源与服务对应多样化
- 是物联网潜在的“杀手”级应用

SHODAN Computer Search Engine censys ZoomEye Oshadan 傻蛋

互联网搜索

- 改变了人们获取信息的获取方式
  - 会议文献、期刊论文
  - 电影、歌曲、歌星、影星等娱乐信息
  - 旅游景点
  - 地图
- Google
  - Google Hacking
- 百度
  - 百度一下，你就知道

人肉搜索！



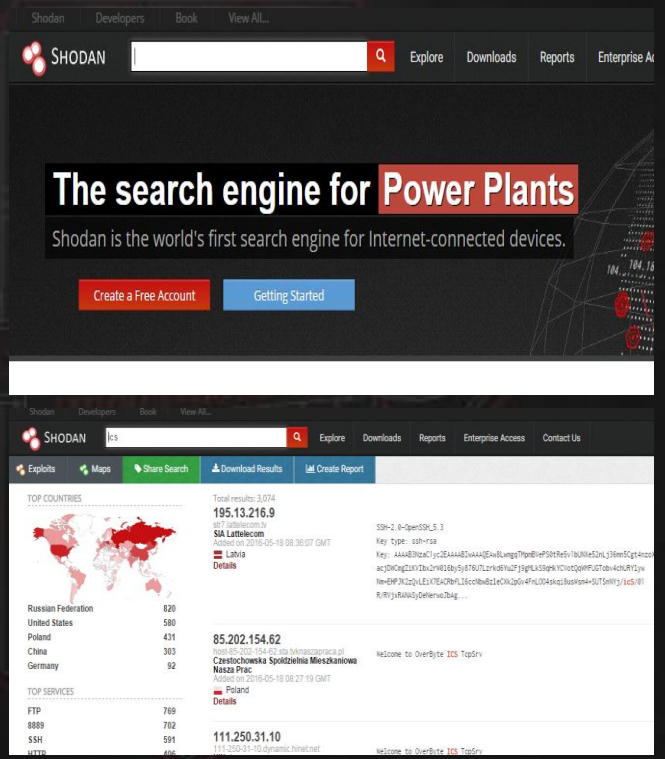
物联网搜索

- 发现设备找到服务
  - 旅游信息-摄像头在线
  - 天气信息
- 企业产品的分布
  - 多少产品在线，分布等
  - 连接在互联网上的品牌排名
- 安全事件分析和防护
  - 心脏出血漏洞的态势感知
  - 重大安全事件的全球影响分布

物联网搜索引擎

Shodan -- “黑暗谷歌”

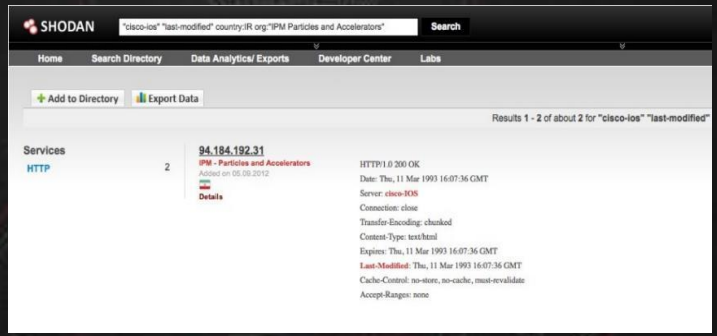
- John Matherly于2009年发布
- 第一个物联网设备搜索引擎
- 采用基于端口和协议标语抓取的方式，利用端口扫描工具在全球IP地址中进行查询，并对返回标语信息进行存储和整理，进而提供索引服务
- 在全球至少8个地点部署搜索服务器：美国东西海岸、中国、冰岛、法国、台湾、越南、罗马尼亚、捷克等
- 搜索端口达200多个，24h×7不间断扫描，从2009年维护至今。
- 最全面、最强大的搜索引擎



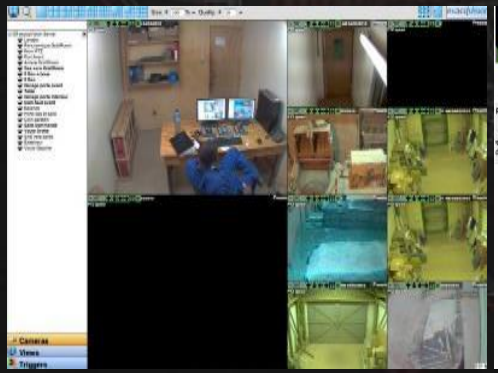
物联网搜索引擎

SHODAN
Computer Search Engine

- 发现思科设备
  - “cisco-ios” “last-modified”
  - 14,000+设备使用HTTP服务却未进行认证设置

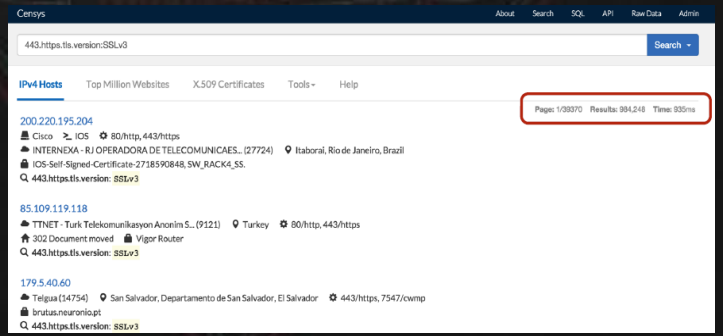


- 没有安全设置的网络摄像头、打印机
  - “camera” “printer”
    “default password”
    “password:123456”等关键字



物联网搜索引擎

- Censys – Internet-wide search engine
  - 密西根大学开发的搜索引擎
  - 2015年ACM CCS安全会议上发布
  - 更加偏重于学术研究（网络安全协议，TLS，SSL等）
  - 数据更新快(每天更新实时更新)
  - 开放源码
    - https://github.com/zmap/zgrab
    - https://github.com/zmap/ztag
  - 提供原数据下载（https://scans.io/）
- 应用
  - 可以搜索到互联网上多少设备使用了SSLv3安全协议，以及多少设备存在着“心血”漏洞



Durumeric Z, Adrian D, Mirian A, et al. A search engine backed by Internet-wide scanning[C]//Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security(CCS). ACM, 2015: 542-553.

Part. 02

物联网搜索技术

网络空间搜索的挑战

- 目标
  - 发现网络上的服务和设备
  - 搜索速度快
  - 搜索内容全
- 设备发现的难点（挑战）
  - 40亿IP的网络空间
  - 多端口、网络黑洞
  - NAT、Firewall等内网空间探测
  - 设备发现的礼貌性
  - 设备发现的隐蔽性

工控设备

监控设备

办公设备

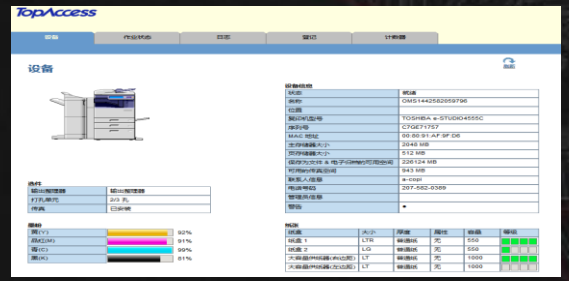
智能设备

物联网搜索

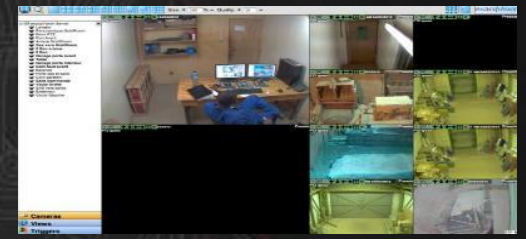
1. Came—来到你身边
2. Saw—看看你是谁
3. Conquered—快到碗里来

物联网搜索技术

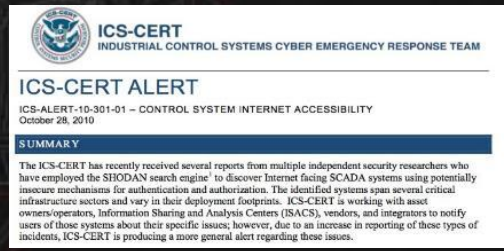
- Came—来到你身边
  - 快速发现技术
- Saw—看看你是谁
  - 指纹识别技术
  - 位置定位技术
- Conquer—快到碗里来
  - 漏洞利用技术
  - 获取信息或控制权



服务器、打印机



摄像头、路由器



工控设备

物联网搜索技术

- 设备特征：设备异构多样，存在大量不透明的专用协议
- 搜索空间：设备搜索的网络地址空间大，还存在有黑洞
- 设备发现：复杂异构网络条件，快发现设备
- 设备识别：不同厂家类设备，同厂家不同型号不同版本
- 设备定位：全球设备的精确定位

实体设备异构互联

高效设备识别发现

设备

特征提取

搜索发现

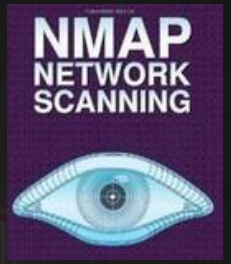
设备定位

设备防护

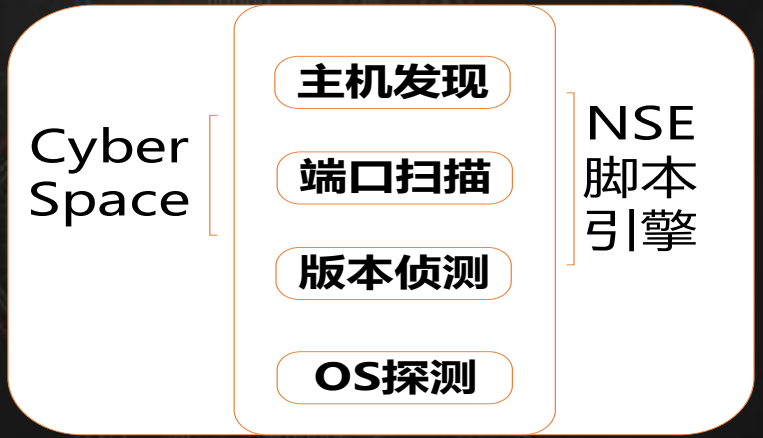
Part. 03

Came—来到你的身边

设备发现工具-Nmap

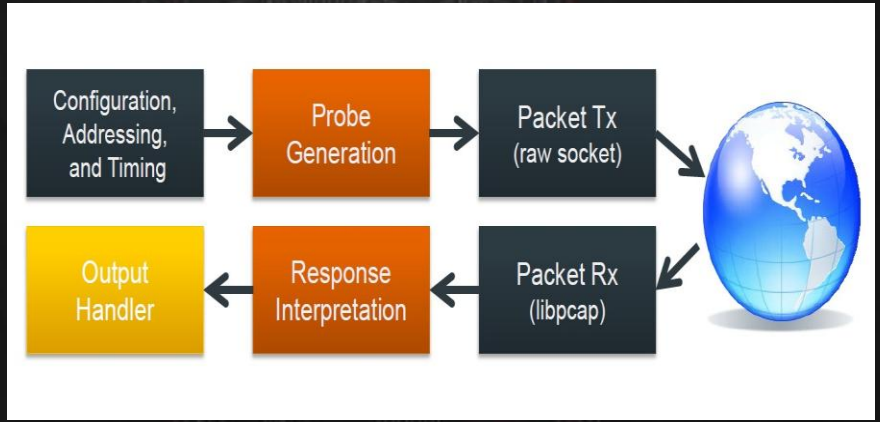


- Nmap – Network Mapper
  - 网络设备识别和安全审计工具
  - Fyodor在1997发布第一版本
  - 开源一直维护至今，最新版本Nmap 7.12
  - http://nmap.org/
  - 能够识别出2600多种操作系统与设备类型
  - 最为流行的安全必备工具之一



设备发现工具-Zmap

- ZMap – Internet Wide Scanner
  - 密歇根大学团队在2013年开发完成
  - 发布于22届USENIX会议上
  - 千兆以太网条件下，45分钟完成全网存活探测，是Nmap的1300倍
  - C语言开发，开源网络扫描工具，密西根大学的多个博士生一直维护
  - https://github.com/zmap/zmap
  - 设备发现技术领域里程碑式的工具

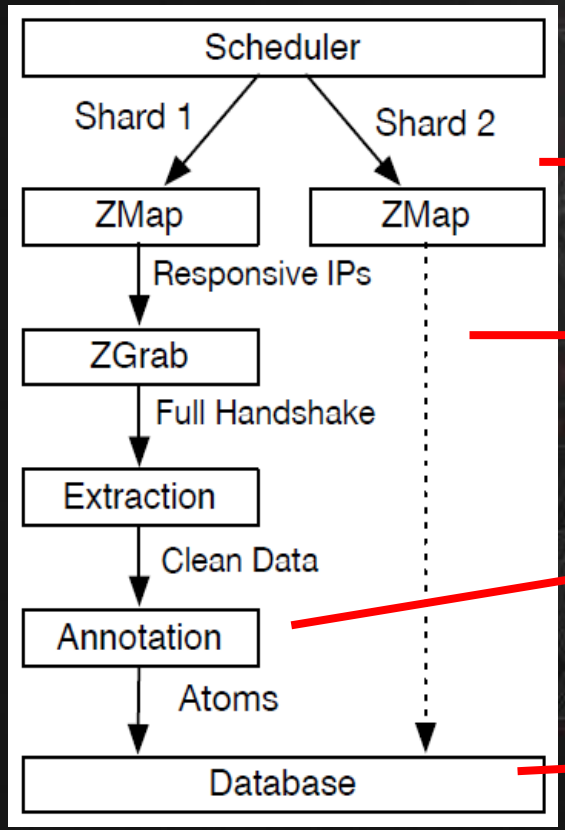


Durumeric, Z., Wustrow, E., & Halderman, J. A. (2013, August). ZMap: Fast Internet-wide Scanning and Its Security Applications. In *Usenix Security*(Vol. 2013).

快速扫描技术

设备扫描

- 主机存活
  - 做主机存活扫描，得到设备候选集
- 收集应用层数据
  - 对设备进行协议探测，抓取标语信息
- 标识
  - 对设备进行标识
- 数据整合存储
  - 整合数据存储数据到数据库




```
1.2.3.4
23.196.166.175
141.211.243.44
```

存活的主机IP地址

```
host: "1.2.3.4",
cipher: "DHE_AES"
version: "SSLv3",
certificate: …,
```

应用层协议标语信息

```
host: "1.2.3.4",
cipher: "DHE_AES"
version: "SSLv3",
certificate: …,
tags: ["POODLE"],
server: "nginx",
```

基于协议特征的标识

```
1.2.3.4,22,SSH
1.2.3.4,80,HTTP
1.2.3.4,443,TLS
```

数据整合

Part. 04

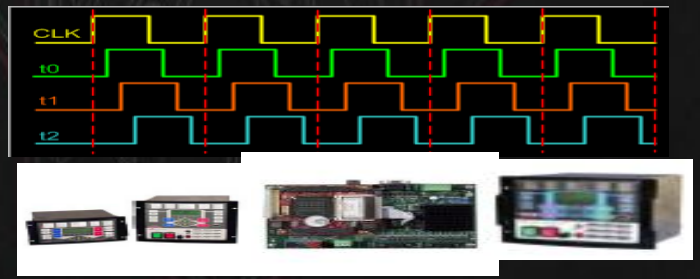
Saw—看看你是谁

设备指纹识别技术

什么指纹？

- 人的指纹：灵长类手指末端指腹上由凹凸的皮肤所形成的纹路，也可指这些纹路在物体上印下的印痕。(Wiki)
- 数据指纹：从一段数据中提取出的可以唯一确定该数据的特征
- 设备指纹：从远程设备中采集的用于确定该设备的信息

OS指纹



设备硬件指纹

设备指纹识别技术

OS指纹

```
FingerPrint  IRIX 6.2 - 6.4 # Thanks to Lamont Granquist
TSeq(Class=i800)
T1(DF=N%W=C000|EF2A%ACK=S++%Flags=AS%Ops=MNWNNT)
T2(Resp=Y%DF=N%W=0%ACK=S%Flags=AR%Ops=)
T3(Resp=Y%DF=N%W=C000|EF2A%ACK=O%Flags=A%Ops=NNT)
T4(DF=N%W=0%ACK=O%Flags=R%Ops=)
T5(DF=N%W=0%ACK=S++%Flags=AR%Ops=)
T6(DF=N%W=0%ACK=O%Flags=R%Ops=)
T7(DF=N%W=0%ACK=S%Flags=AR%Ops=)
PU(DF=N%TOS=0%IPLEN=38%RIPTL=148%RID=E%RIPCK=E%UCK=E%ULEN=134%DAT=E)
```

Nmap系统指纹

```
% sinfp.pl -Pf ~/sinfp4-passive.pcap
10.100.0.1:80 > 10.100.0.68:39503 [SYN|ACK]
P2: B10111 F0x12 W5672 O0204ffff0402080affffffffffffffff01030306 M1430
IPv4: BHOFHOWH1OHOMH1/P2: GNU/Linux: Linux: 2.6.x
```

SinFP系统指纹

协议指纹

```
Copyright: Original Siemens Equipment
PLC name: S7_Turbine
Module type: CPU 313C
Unknown (129): Boot Loader          A
Module: 6ES7 313-5BG04-0AB0  v.0.3
Basic Firmware: v.3.3.8
Module name: CPU 313C
Serial number of module: S Q-D9U083642013
Plant identification:
Basic Hardware: 6ES7 313-5BG04-0AB0  v.0.3
```

西门子指纹

```
HTTP/1.1 301 Moved Permanently
Date: Sun, 01 May 2016 12:13:53 GMT
Server: Apache
Location: https://smart-meter-portal.allgaeustrom.de/
Vary: Accept-Encoding
Content-Length: 251
Content-Type: text/html; charset=iso-8859-1
```

智能电表

```
ES-2026 Advanced Smart FE Switch

HTTP/1.1 401 N/A
Server: TP-LINK Router
Connection: close
WWW-Authenticate: Basic realm="Web Smart Switch"
Content-Type: text/html
```

智能开关

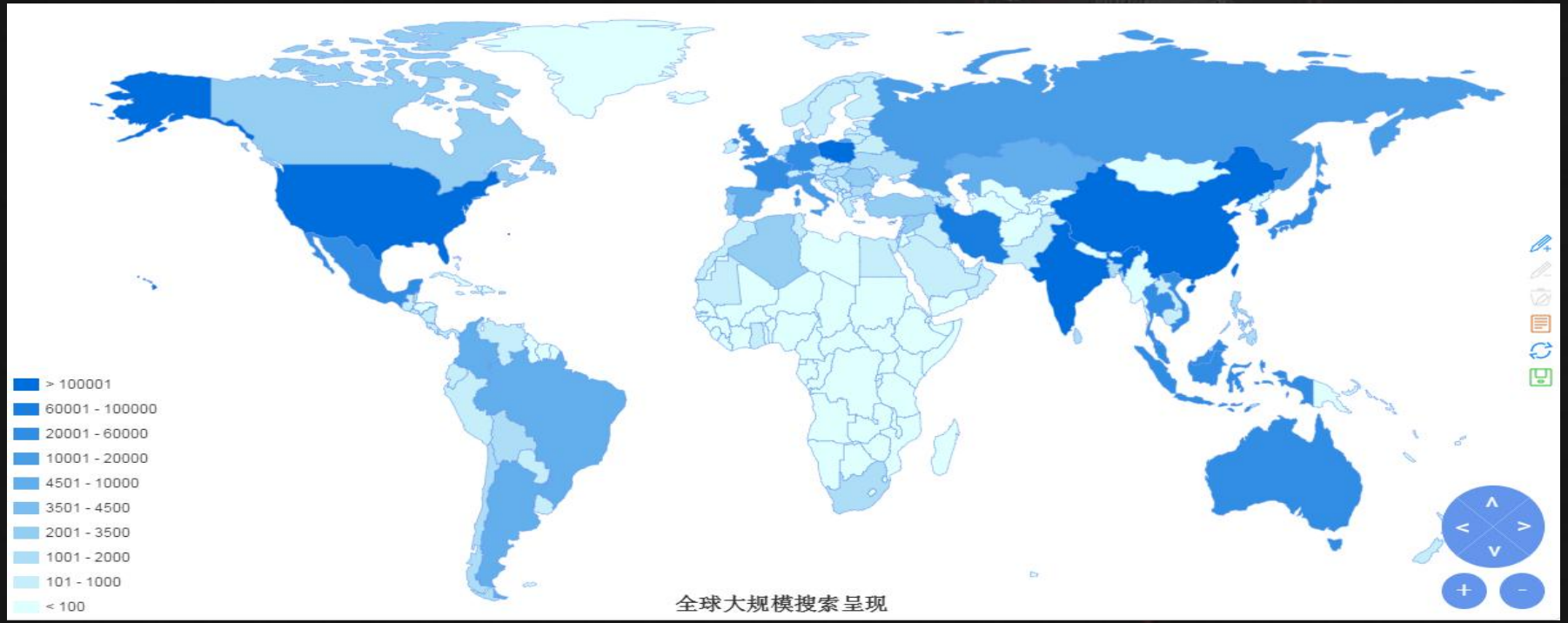
```
HTTP/1.1 200 OK
Server: nginx/1.1.19
Date: Sat, 03 Oct 2015 06:09:24 GMT
Content-Type: text/html; charset=utf-8
Content-Length: 6466
Connection: keep-alive
```

服务器指纹

Part. **06**

Our work

全球分布态势图


> 100001
60001 - 100000
20001 - 60000
10001 - 20000
4501 - 10000
3501 - 4500
2001 - 3500
1001 - 2000
101 - 1000
< 100
全球大规模搜索呈现

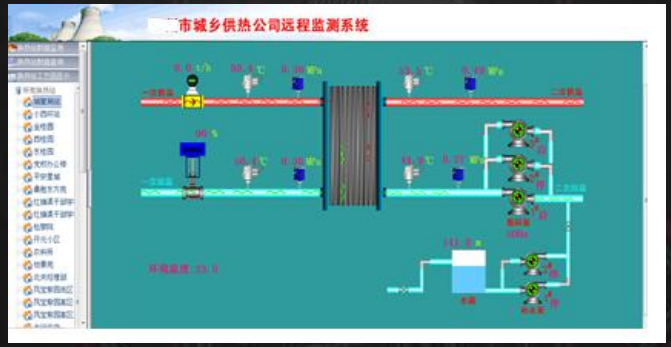
全国分布态势图


全国搜索结果
> 15001
10001 - 15000
4501 - 10000
3501 - 4500
2501 - 3500
2001 - 2500
1501 - 2000
1001 - 1500
501 - 1000
101 - 500
< 100
黑龙江
内蒙古
吉林
辽宁
新疆
甘肃
北京
天津
山西
河北
宁夏
山东
陕西
青海
河南
江苏
安徽
西藏
湖北
上海
四川
重庆
浙江
贵州
湖南
江西
福建
云南
广西
广东
台湾
香港
澳门
海南
南海诸岛
全国大规模搜索呈现

搜索结果

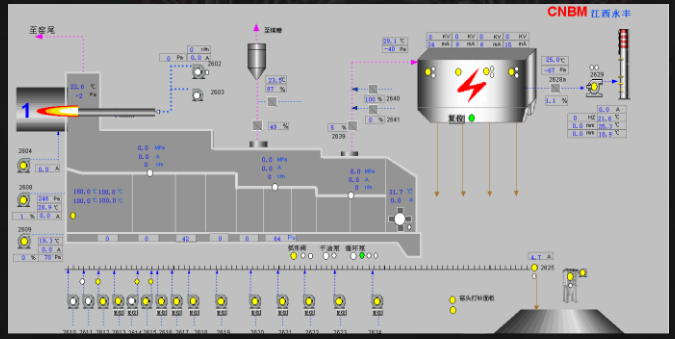
工厂

加气站



供热控制系统

施耐德设备



DCS系统

应用示范

视频监控系统安全评测

保存结果

- 认证缺失
- 缓冲区溢出
- 权限提升
- 弱密钥
- 硬编码
- 命令注入
- 验证绕过
- 信息泄露
- 目录遍历
- 拒绝服务
- 跨站脚本漏洞

扫描带宽 32M

58.130.81.0/24

默认扫描的端口是：
80,81,554,8080,37777

开始扫描

扫描结果(共 12 个，监控设备5个，漏洞11个)

58.130.81.36	58.130.81.15	58.130.81.34	58.130.81.16
80 554	80 554	80 554	80 554
监控设备 camera Hikvision	监控设备 camera Hikvision	监控设备 camera Hikvision	监控设备 camera Hikvision
弱秘钥(admin:12345:554:rtsp) 高危	弱秘钥(admin:12345:554:rtsp) 高危	弱秘钥(无:无:554:rtsp) 高危	弱秘钥(admin:12345:554:rtsp) 高危
未授权信息泄露 高危	未授权信息泄露 高危	权限提升 高危	未授权信息泄露 高危
ONVIF认证缺失 高危	ONVIF认证缺失 高危	未授权信息泄露 高危	
		ONVIF认证缺失 高危	

58.130.81.35	58.130.81.38	58.130.81.2	58.130.81.161
80	8080	80	80
监控设备 camera Hikvision	非监控设备 未知厂商	非监控设备 未知厂商	非监控设备 未知厂商
弱秘钥(无:无:554:rtsp) 高危	无弱密钥	无弱密钥	无弱密钥
权限提升 高危	无漏洞	无漏洞	无漏洞
未授权信息泄露 高危			
ONVIF认证缺失 高危			

current handling host and vul_num is :58.130.81.15 CVE-2014-4878
current handling host and vul_num is :58.130.81.36 CVE-2013-4975
current handling host and vul_num is :58.130.81.36 CVE-2013-4976
current handling host and vul_num is :58.130.81.36 CNVD-2015-00294
current handling host and vul_num is :58.130.81.36 CNVD-2015-00079
current handling host and vul_num is :58.130.81.36 CVE-2014-4880
current handling host and vul_num is :58.130.81.36 CVE-2014-4879
current handling host and vul_num is :58.130.81.36 CVE-2013-4977
current handling host and vul_num is :58.130.81.36 CVE-2014-4878
all task has done!
视频监控系统>>

看世界

《速度与激情7》中设计出一种超级黑客程序“天眼”系统，这个程序可以整合全球所有的数据采集、监控设备，可以通过手机音频、监控摄像头等手段大量采集数 据，再使用大数据和人脸识别等技术，短时间内把要找的人找出来。

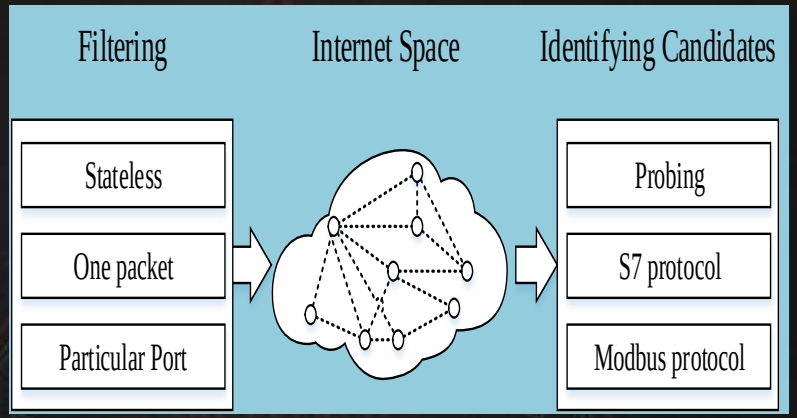
点我“看”世界

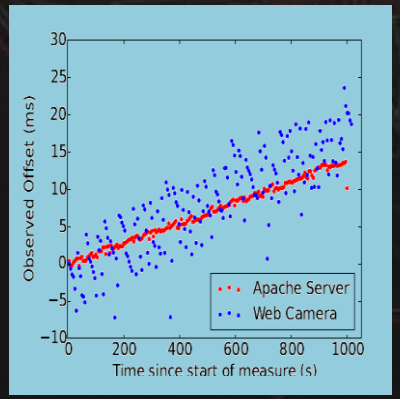
Part. 07

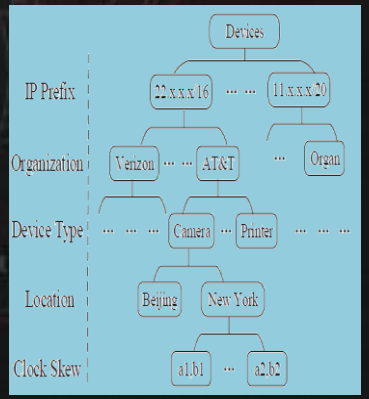
工控篇

工控设备快速搜索技术

- 问题与目标
  - 快速发现设备，并且对这些设备进行标识建立档案
- 技术要点
  - 快速筛选
    - 无状态连接、单包、跳过内核直接从网卡发送数据包、特定端口等方式获得工控设备候选集合
  - 精准探测
    - 通过贪心准则筛选最优探测数据包载荷
  - 建立档案
    - 结合多维度（时间、空间、设备）的特征，建立设备档案







工控协议指纹库

- 指纹库
  - 研究和提取了包括西门子、施耐德、浙大中控、和利时等知名品牌设备的指纹
  - Siemens等17种工控协议特征

搜索到的西门子S7 PLC

搜索到的施耐德BMX PLC

工控协议	工控品牌	类型	端口
Modbus	Schneider	TCP	502
S7	Siemens	TCP	102
Ethernet/IP	General	TCP	44818
Tridium Niagara Fox	Tridium Niagara Fox	TCP	1911
BACnet	General	UDP	47808
Redlion Crimson V3	Redlion	TCP	789
DNP3	General	TCP	20000
OMRON FINS	OMRON	TCP/UDP	9600
General Electric SRTP	GE	TCP	18245
ProConOS	-	TCP	20547
PCWorx	General	TCP	1962
MELSEC-Q	Mitsubishi	UDP	5006/5007
Codesys	-	TCP	1200/2454
HART-IP	FIELD COMM	TCP/UDP	5094/20004
IEC-60870-5-104	General	TCP	2404

全球工控设备态势分析

- 动态性
  - 工控设备大部分IP为静态，一个月内变化小，三个月会有1/3发生变化
- 与综合国力相关
  - 发达国家的工控设备较多，但一般不在最发达的城市
- 工控设备的分布显示长尾效应

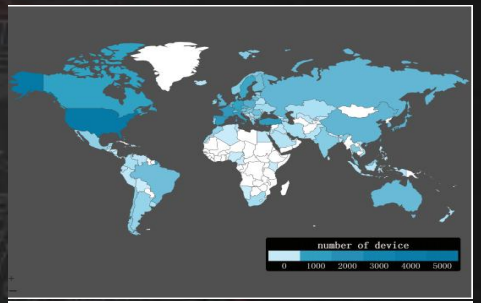
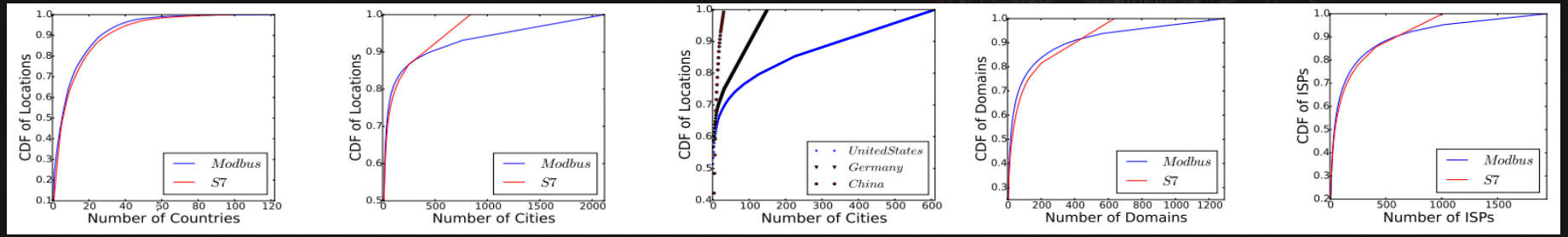


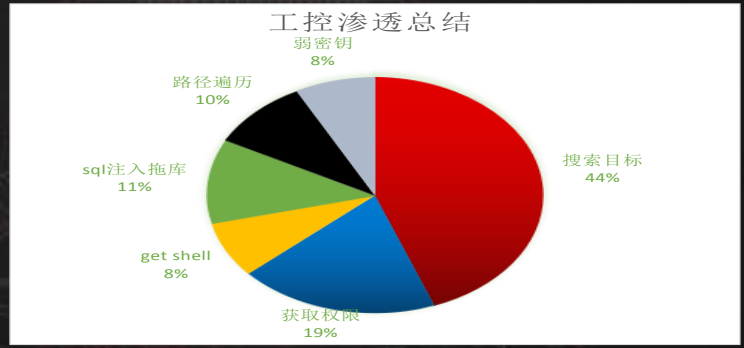
TABLE IV: Modbus: Top 10 Countries and its GDP

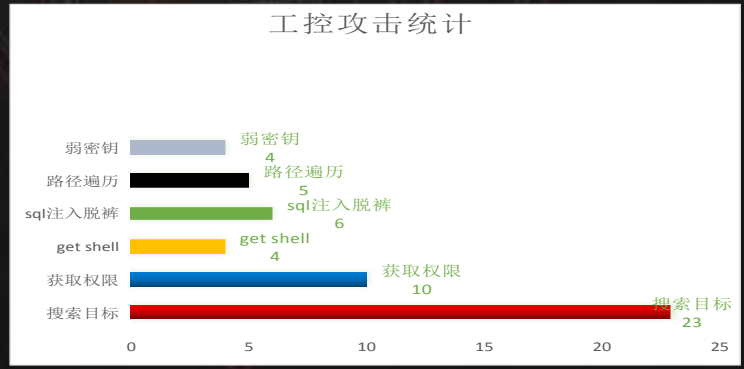
	Country/Region	Rank Of GDP	GDP (Millions of US$)
1	United States (4628)	1	17,418,925
2	Spain (1487)	14	1,406,855
3	France (1324)	6	2,846,889
4	Italy (1175)	8	2,147,952
5	Turkey (984)	18	806,108
6	Canada (936)	11	1,788,717
7	Germany (797)	4	3,859,547
8	Taiwan (772)	16	529,550
9	Sweden (714)	21	529,550
10	Japan (509)	2	4,616,335

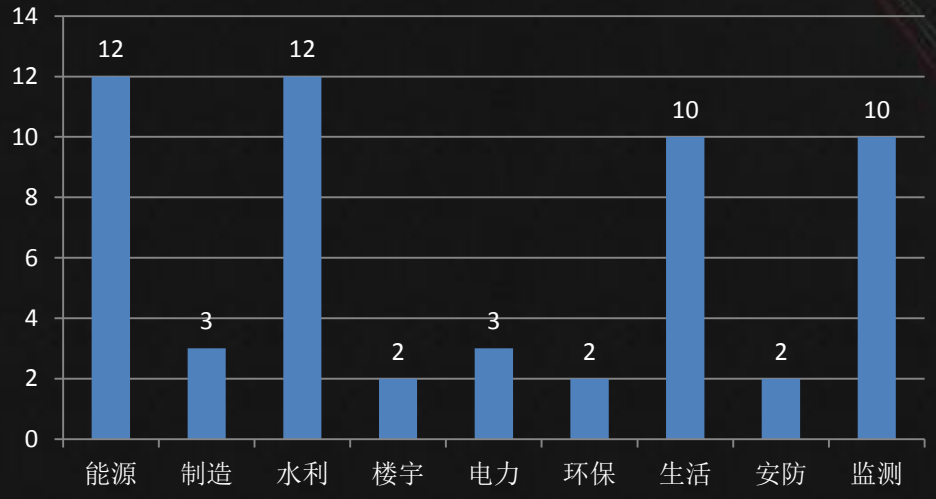


我国工控系统的安全现状

- 应**省对工控系统进行调研
  - 全国渗透了70多个工控系统
  - 涵盖了能源、电力、水利等要害行业

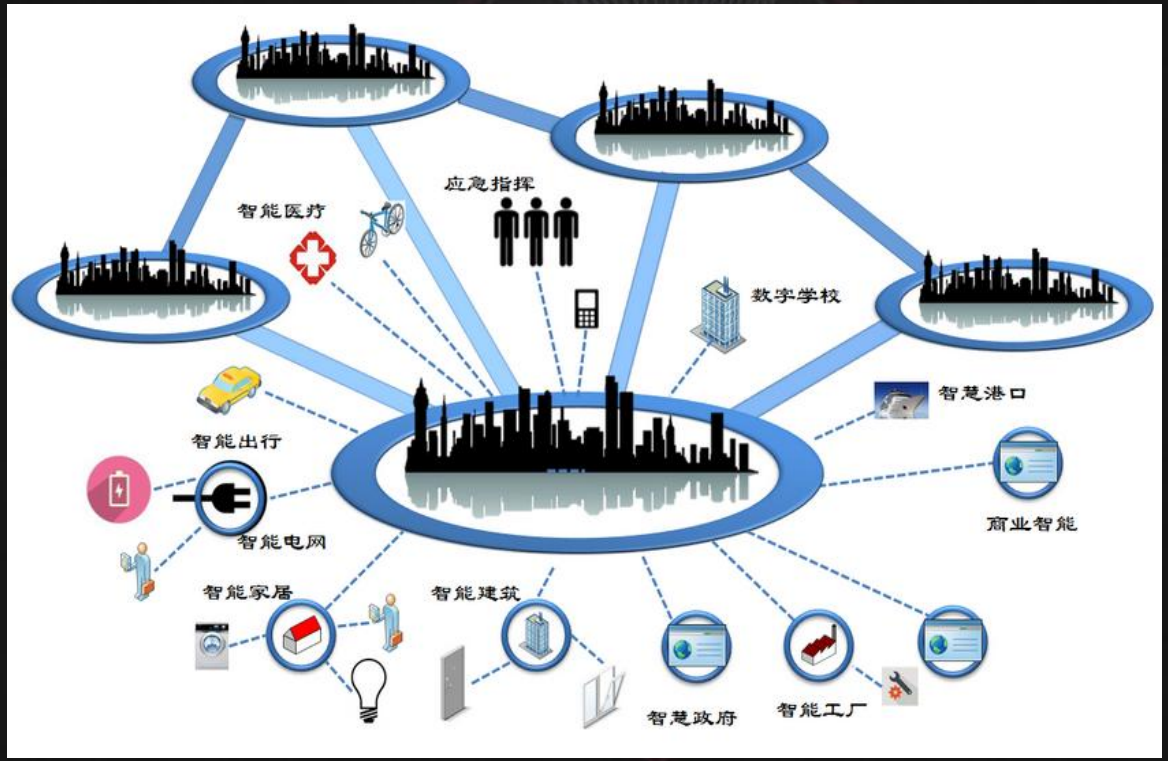






智能硬件的展望

- 智能电视
  - Sony电视
  - 关键词：“Bravia TV”
- 智能开关
  - TP-LINK开关
  - 关键词： Basic realm=“Web Smart Switch”
- 智能电表
  - IBM Tivoli WebSEAL
  - Smart Meter



T H A N K S

[yanzhaoteng@iie.ac.cn]