



探究物联网系统中的安全威胁

Dean J. Coclin (丁考林) Digicert全球产品与标准副总裁



Security Threats in IoT

Dean Coclin VP of Product Standards

1995

威瑞信成为首个证书颁发机构



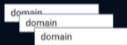
2003

DigiCert基于该问题成立：“难道没有更好的方法吗？”

digicert

2007

DigiCert与微软合作开发首个多域名证书



2013

DIGICERT建立了首个被谷歌接受的CT日志



2016

DigiCert收购Verizon SSL/TLS业务



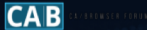
1997

威瑞信成为首个国际CA



2005

DIGICERT成为CA/浏览器论坛的创始成员



2010

赛门铁克收购威瑞信身份验证业务



2015

DigiCert推出可扩展的物联网平台



2017

DIGICERT收购赛门铁克的网站安全业务



2018

DigiCert受信任的根成为全球企业的加密基础





2019

“这种规模的迁移在CA行业中前所未有。在统一平台以及对组织提供支持方面,DigiCert做的非常出色。他们为客户提供工具,确保其Web服务器不会出现问题,所以现在就看安全团队了。”

*Zeus Kerravala, ZK Research的创始人兼首席分析师,
2018年3月*



2019

“A migration of this magnitude is unprecedented in the CA industry. DigiCert has done a remarkable job in unifying the platforms and support organizations. They have provided tools for customers to ensure that their web servers won't have a problem, so it's now up to security teams.”

*Zeus Kerravala, Founder and Principal Analyst, ZK Research,
March 2018*

▶▶ 以不同方式对互联网进行使用  2019



个人



企业

但是在物联网中，物与物之间相互通讯

▶▶ Using Internet Differently  2019



Personal



Business

But in IoT, *things* communicate with other *things*

▶▶ 物联网是什么？

IFT 2019

物联网 (IoT) 是实体设备、车辆 (也称为“互联设备”和“智能设备”)、建筑物以及其他物品的网络互联——而且嵌入了电子器件、软件、传感器、执行器，以及网络连接，使这些对象能够收集并交换数据。

▶▶ What is the IoT?

IFT 2019

The Internet of Things (or IoT) is the internetworking of physical devices, vehicles (also referred to as "connected devices" and "smart devices"), buildings, and other items—embedded with electronics, software, sensors, actuators, and network connectivity that enable these objects to collect and exchange data.

物联网是什么？

IoT 2019

“物联网终端的安装基数将从2014年的97亿增长到2019年的超过256亿，到2020年将达到300亿。” ——IDC*

* IDC Research, Inc., 全球物联网预测更新, 2015-2019, Carrie MacGillivray, 2016年2月, IDC #US40983216

What is the IoT?

IoT 2019

“The installed base of IoT endpoints will grow from 9.7 billion in 2014 to more than 25.6 billion in 2019, hitting 30 billion in 2020.” – IDC*

*IDC Research, Inc., Worldwide Internet of Things Forecast Update, 2015-2019, Carrie MacGillivray, February 2016, IDC #US40983216

▶▶ 物与物之间的“交谈”所带来 2019 的益处

- ✓ 获取实时信息
- ✓ 软件自动更新
- ✓ 远程访问设备
- ✓ 信息传递
- ✓ 远程控制设备
- ✓ 设备之间可以自主地相互“交谈”

▶▶ Benefits of Things 'Talking' 2019

- ✓ Access to real time information
- ✓ Automatic software updates
- ✓ Remote access to devices
- ✓ Information transfer
- ✓ Remote control of devices
- ✓ Devices can “talk” to each other autonomously



IFT 2019

可能会出现哪些问题？



IFT 2019

What Could Go Wrong?



▶▶ 针对汽车的黑客攻击

IFT 2019

有时人们对互联网的使用方式背离了初衷



▶▶ Car Hacking

IFT 2019

The Internet isn't always used the way it was intended



▶▶ 针对交通标志的黑客攻击

IFT 2019



▶▶ Traffic Sign Hacking

IFT 2019





“弱密码，默认及硬编码的供应商密码，如 ‘admin’ 或 ‘1234’ ；以及可以轻松识别并操纵设备的嵌入式Web服务器和管理界面”



“weak passwords, default and hardcoded vendor passwords like ‘admin’ or ‘1234’; and embedded web servers and administrative interfaces that make it easy to identify and manipulate devices”

▶▶ 针对玩具的黑客攻击

IFT 2019

一家销售互联毛绒玩具的玩具公司由于数据安全措施不到位，导致80万名客户的个人信息以及约200万条录音记录暴露于众，其中很多是儿童的录音。

那只柔软的泰迪熊看似无害，但黑客可能用它来监视您的孩子。

▶▶ Toy Hacking

IFT 2019

Sloppy data security practices at a toy company that sells a line of internet-connected stuffed animals has exposed the personal information of more than 800,000 customers, and some 2 million voice recordings — many of them from children.

That soft teddy bear seems harmless, until hackers can use it to spy on your kids.

▶▶ 重要的经验教训？

IFT 2019



在给家里添置任何互联设备之前一定要三思而后行，特别是儿童可能定期与之进行互动的设备。

▶▶ Main Takeaway?

IFT 2019



Think twice before you welcome any Internet-connected device into your home, particularly ones that children may interact with on a regular basis.

为什么物联网不安全？

IFT 2019

- × 制造企业缺乏网络安全经验（而且保障安全性很难！）
- × 确保安全的成本可能令人望而却步
- × 个人设备在设计时主要关注的是使用的便捷性，而牺牲了安全性
- × 竞争标准难以驾驭——造成安全“盲点”
- × 有些设备使用出厂默认密码

问题不一而足.....

Why is IoT insecure?

IFT 2019

- × Manufacturers lack cybersecurity experience (and security is hard!)
- × Costs to secure can be prohibitive
- × Personal devices are designed to be easy to use, sacrificing security
- × Competing standards can be difficult to navigate – creating security “blind spots”
- × Some devices use factory default passwords

List keeps going...

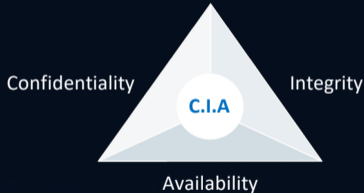
网络安全三角

2019



The Cybersecurity Triad

2019



通过设计提高安全性

IFT 2019

- ✓ 使用SSL/TLS对初始配置进行加密
- ✓ 需要物理访问才能启用设置
- ✓ 已签名的代码；没有适当的签名就无法进行修改
- ✓ 绑定的TLS证书能防范中间人（MITM）攻击
- ✓ 不连接互联网查找回答，而是使用预先记录的回答



Better Security by Design

IFT 2019

- ✓ Uses SSL/TLS to encrypt initial configuration
- ✓ Requires physical access to enable settings
- ✓ Signed code; unable to modify without proper signature
- ✓ Pinned TLS certificates which prevents Man in the Middle (MITM) attack
- ✓ Does not connect to Internet to find answers, instead uses pre-recorded answers



物联网攻击类型

IFT 2019



要求支付赎金：除非支付赎金，否则无法使用有价值的数据



窃取信息：窃取个人信息或私密信息并在暗网上出售



访问远程设备：访问远程控制设备，如安全摄像头或婴儿监视器

IoT Attack Types

IFT 2019



DEMAND RANSOM: Make valuable data unusable unless a ransom is paid



STEAL INFORMATION: Steal personal or private information and sell it on the Dark Web



ACCESS REMOTE DEVICES: Access remotely controlled devices such as security cameras or baby monitors

▶▶ 针对Dyn的Mirai与DDoS攻击 2019

- **MIRAI的工作原理**：不断进行扫描以找到受出厂默认凭证保护的物联网设备。Mirai使用恶意软件感染设备，使其变为可用于DDoS攻击的bot
- **处于危险之中的设备**：路由器、DVR、监控摄像机，以及任何其他“智能”互联设备都面临这类攻击的风险

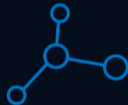
▶▶ Mirai & DDoS Attack on Dyn 2019

- **HOW DOES MIRAI WORK**: Continuously scans for IoT devices protected by factory default credentials. Mirai infects devices with malware by turning them into a bot that can be used in DDoS attacks
- **DEVICES AT RISK**: Routers, DVRs, CCTV cameras, and any other 'smart', internet-connected appliances are at risk of such attacks

▶▶ 物联网设备的基本安全建议

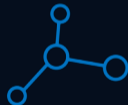
IoT 2019

1. 避免直接的互联网连接
2. 更改默认登录凭证
3. 更新固件
4. 检查默认设置
5. 避免P2P连接
6. 将代价纳入考虑之中



▶▶ Basic Security for IoT Devices IoT 2019

1. Avoid direct Internet connection
2. Change default credentials
3. Update the firmware
4. Check defaults
5. Avoid P2P connections
6. Consider cost



隐私：确保信息的私密性

身份验证：证明个人或申请人的身份

完整性：证明信息未被操纵

不可否认性：确保信息不能被否认

PRIVACY: to keep information private

AUTHENTICATION: to prove the identity of an individual or an application

INTEGRITY: to prove that information has not been manipulated

NON-REPUDIATION: to ensure that information cannot be disowned

隐私：加密 ✓

身份验证：证书 ✓

公钥加密 ✓

完整性：数字签名 ✓

不可否认性：证书与数字签名 ✓

PRIVACY: ENCRYPTION ✓

AUTHENTICATION: CERTIFICATES ✓

PUBLIC KEY CRYPTOGRAPHY
INTEGRITY: DIGITAL SIGNATURES ✓

NON-REPUDIATION: CERTIFICATES AND DIGITAL
SIGNATURES ✓

证书在物联网中的作用

FIIT 2019

1. 对设备的强身份验证
2. 实现端点之间的加密
3. 物联网设备中使用的代码数字签名



Certificates Role in IoT

FIIT 2019

1. Strong authentication of the device
2. Enable encryption between end points
3. Digital signing of code used in IoT devices



需要考虑的事项

IFT 2019

1. “是不是应该连接” 而不是 “能不能连接”
2. 将物联网的安全性视为必要因素和促成因素，而不是负担或者税费
3. 做人们会作恶的假设——要考虑某物有可能被如何使用，而不是您希望某物会被如何使用


Things to Consider

IFT 2019

1. “Should it be connected” NOT “can it be connected”
2. Think of security in the IoT is a necessity and enabler, not a burden or a tax
3. Assume people will do wrong – think about how something could be used, not how you want it to be used

物联网安全挑战


IFT 2019

 **指数级增长** 到2022年将会有1万亿个网络传感器，这一数字将在20年内达到45万亿

 **扩展性** 找到适合大规模物联网需求的安全解决方案


 **资源约束** 部署及管理数字证书非常耗时


 **关键需求** 满足三个需求：身份验证，加密与信息完整性


 **自动化的缺乏** 为数十亿台设备实现注册、设置、配置与部署的自动化


IoT Security Challenges


IFT 2019

 **EXPONENTIAL GROWTH** 1 trillion networked sensors by 2022, with up to 45 trillion in 20 years

 **SCALING** Finding a security solution that fits the large-scale need of IoT

 **RESOURCE CONSTRAINTS** Deploying and managing digital certificates is time-consuming

 **CRITICAL NEEDS** Addressing three needs: authentication, encryption, and message integrity

 **LACK OF AUTOMATION** Automating enrolment, provisioning, configuration, and deployment for billions of devices



我们关心客户与
民众



我们为实现数字安
全性而做正确的事



我们通过技术创新
解决问题



We take care of our
customers and
people



We do what's right
for digital security



We solve problems
with technical
innovation

REEBUF | FIT

THANKS