安全+
SECURITY
2018/07 总第038
技术版 ▶▶ 与安全人士分享技术心得 Share technique experience with security professionals

★ 本期焦点

新型基础设施支撑的物联网服务安全分析

物联网安全解决方案

智慧城市中的物联网安全

物联网设备安全评估的七种武器

绿盟科技官方微信

NSFOCUS

本期看点 HEADLINES

主办：绿盟科技
策划：绿盟内刊编委会
地址：北京市海淀区北洼路4号益泰大厦三层
邮编：100089
电话：(010)6843 8880-8670
传真：(010)6872 8708
网址：www.nsfocus.com

2018/07 总第 038

欢迎您扫描封面左下角的二维码，关注绿盟科技官方微信，分享您的建议和评论，或者来信nsmagazine@nsfocus.com与我们交流。

安全+ SECURITY+

© 2018 绿盟科技

本刊图片与文字未经相关版权所有人书面批准，
一概不得以任何形式、方法转载或使用。本刊保留所有版权。

SECURITY+ 是绿盟科技的专用图标。

需要获取更多信息，请访问WWW.NSFOCUS.COM

目录 CONTENTS

物联网 IoT（Internet of Things）是继互联网 (Internet)、移动互联网 (Mobile Internet) 后的又一新兴信息与计算技术。目前，世界主要国家都在把发展战略性新兴产业作为抢占新一轮经济科技发展至高点的重大战略，包括德国提出了工业 4.0 ，美国提出了工业互联网，我国提出了“中国制造 2025”。这其中，支撑万物互联的物联网 IoT 技术是一个关键基础。在我国，2016 年《“十三五”国家信息化规划》中的“应用基础设施建设行动”方案明确指出：要积极推进物联网发展，推进物联网感知设施规划布局，发展物联网应用。时至今日，物联网技术的发展已然成为推动社会智能化、可持续发展的重要引擎，在包括车联网、医疗健康、智能家居、智能可穿戴设备、智慧城市管理，智能工厂等领域催生创新和融合。

物联网终端方面，IT 咨询机构 Gartner 预测，自 2015 年至 2020 年，物联网终端年均复合增长率为 33%，安装基数将达到 204 亿台，其中三分之二为消费者应用。在联网的消费者和企业设备的投资为 2.9 万亿美元，年均复合增长率高达 20%，将超过非联网设备的投资。在连接技术方面，移动蜂窝接入技术包括 NB-IoT 成为主流，截止到 2018 年 8 月，中国移动已超过 3 亿物联卡用户，分布在车联网后装、共享单车、设备监控等应用领域。在平台技术方面，物联网平台也成为运营商，互联网巨头，工业制造巨头，以及新兴平台厂商之间竞争的主赛道。

高速发展的物联网技术背后难以避免存在着信息和网络安全的威胁，其中物联网设备的安全风险逐年升高。物联网攻防态势的特点是设备基数大、攻击扩散快、技术门槛低。2016 年 Mirai 大规模感染事件，2017 年 Rowdy、DarkCat、Gafgyt 等多种针对新型设备的僵尸家族，都为物联网设备及运营平台的安全防护拉响警钟。这些对用户的财产甚至生命安全带来的威胁风险是日趋增高，与此同时，设备厂商的不重视、运营防护方案的不成熟、用户的安全意识薄弱亦是造成如此局面因素的重要推手。不论在固件升级、配置核查、补丁维护等方面，物联网行业都还非常薄弱。

“智能物联 安全先行”，基于此，绿盟科技在物联网资产暴露情况、物联网设备的脆弱情况、威胁风险分析及安全运营防护体系等方面，进行深入剖析，并提供物联网安全解决方案，为物联网应用发展和安全运营实践提供了一个方向。

绿盟科技 高管层 杨传安

新型基础设施支撑的物联网服务的安全分析

创新中心 刘文懋

关键词：物联网安全 5G 边缘计算 云计算

摘要：随着云计算、物联网和运营商网络的快速发展，可预计未来十年左右各类新型基础设施的融合会成为一个明显的趋势。一方面，“中国制造 2025”的国家战略催生了工业互联网和 IT/OT 的融合，如工业云、边缘计算和新型工控网络的结合会更加紧密；另一方面，智慧城市、智能交通和智慧家居等细分领域的物联网应用日渐成熟，也推动如 5G 运营商网络和物联网云应用等基础设施的快速发展。

本文首先介绍支撑未来十年内的新物联网应用的基础设施及其关键技术，然后讨论这些基础设施给物联网应用带来的安全挑战，最终给出一些应对策略。

物联网应用的支撑关键基础设施

面向物联网应用的云计算基础设施

云计算技术的发展已经超过了十年，无论公有云还是私有云，都具备了提供大规模计算资源、平台服务或应用托管的能力。特别是公有云的平台即服务（PaaS），可为不同的场景下的应用提供诸如 AI 计算、数据存储、认证和消息队列等服务，通过按需调用这些服务，可组装成云原生（Cloud Native）的物联网应用，支持大规模物联网设备直连云端服务的应用场景。

如亚马逊 AWS IoT 平台 [1] 提供了物联网设备连接、管理和分析功能，并且提供了如 FreeRTOS 和 1-Click 等嵌入式操作系统和微服务接口，用于无缝对接 AWS 的各项云服务。

国内厂商如阿里云在物联网上推出了物联网云平台 Link Platform、边缘网关 Link Edge 和物联网操作系统 AliOS Things，同样提供了设备管理和数据分析的功能。在生态合作方面，阿里巴巴与传统厂商合作，开发物联网产品，阿里巴巴目前的产品非常多，截止到 2018 年 4 月 7 日，从天猫上搜索“阿里智能”就可以找到四千多个商品，覆盖环境管家、数码娱乐、全屋智能和运动健康等领域。

表 1 列出了一些在业界具有代表性的公有云服务商，无一例外地均提供了物联网云平台的服务。这些云服务商或多或少的提供了物联网操作系统或模组 SDK，与第三方厂商合作，生产可接入物联网平台的智能物联网终端。

除了以上云服务商从云端出发自顶向下地建立物联网应用外，还有一些物联网厂商虽然没有云计算的背景，但从物联网芯片和业务入

表 1 主流公有云服务商的物联网平台

云服务商	云服务	物联网云服务	边缘和终端功能	功能
Amazon	Amazon AWS	AWSIoT 平台，AWS Greengrass	AWS IoT 设备 SDK	设备接入和控制，APP 访问与控制，数据分析
阿里巴巴	阿里云	阿里云物联网套件	物联网操作系统 AliOS Things 边缘网关	设备接入、设备通信、安全能力、设备管理、规则引擎
Google	Google Cloud Platform	GOOGLE cloud IOT	TPU、提供板级 SDK 接入云平台	连接、管理设备，数据分析
腾讯	腾讯云	微信硬件平台 QQ 物联平台 腾讯云物联网套件 IoT Suite	物联网套件 IoT Suite SDK 支持 linux 和 android、RTOS	设备接入、消息转发、消息存储等，机器学习、大数据、云监控服务
百度	百度云	百度天工	百度云智能边缘，设备 SDK	数据采集、传输、计算、存储、展现到分析

手，为物联网厂商提供了物联网设备 SDK，同时建立了物联网平台，自底向上地提出了物联网应用解决方案，如国内的机智云、庆科云等。

此外，在一些工业物联网的场景中，一些云计算服务商直接提供了针对细分领域的物联网云平台服务，例如寄云（neucloud）将工业设备的运行数据保存到云端，并为企业运营者提供直观的运行情况展示，提供运营需要的支撑数据，还可通过计算分析找到运行异常的设备。

面向实时物联网应用的边缘计算和 5G 网络

物联网云服务主要部署在云服务商所在的数据中心，数据流从物联网终端设备经过互联网到达云计算数据中心，整个过程会存在一定的延迟。在一些低延迟近乎实时的应用场景中，如自动驾驶、工业控制，这样的延迟是无法接受的；此外互联网的链路存在不稳定性，一旦到云端的通道延迟或终端，弱终端就无法进行正常的数据处理，可能引发严重的后果。

所以，在很多物联网云服务商提出的解决方案中，除了云端和终端外，还引入了边缘网关的角色，该网关承担实时决策和部分数据处理工作，边缘侧和云端共同组成完整的设备控制和数据处理机制。例如，AWS 和百度云的物联网解决方案中均包含了边缘网关，最终提供了人工智能处理海量实时数据的功能。客户可在接入互联网的出口处部署边缘网关，在内部网络部署物联网设备，对内组成高速传输的网络。

除了云服务商可以在客户侧或 CDN 侧部署边缘网关外，运营商也积极参与到物联网和边缘计算的建设中。特别是 5G 标准的制定中，ITU-R 将超高可靠与低延迟的通信 (uRLLC,Ultra Reliable &Low Latency Communication) 作为三大应用场景之一，这就要求运营商了解物联网应用的区域，并在建设和运营时将边缘服务尽可能贴近应用基站附近。这将改变现在运营商数据中心和部署云服务的模式，给托管云服务提出了更灵活的要求。

需要说明的是上述基础设施将会是彼此融合的，例如 AWS 的 GreenGrass 云服务提供了物联网分析、存储服务。考虑在工业物联

网等场景下对实时性、网络中断业务不断的要求，GreenGrass 提供了边缘计算的支持，使得物联网设备可以运行 Lambda 函数处理收集到的数据，这样设备即使在离线状态也可以完成部分功能。

新基础设施下的物联网服务的安全挑战

云计算带来的安全挑战

随着云计算技术引入物联网应用，会出现两类安全挑战：云平台自身的安全问题，以及使用云服务后的物联网应用的安全问题。

第一 . 云平台数据秘密性

物联网设备的所有者将物联网设备产生的数据传输到了云平台中，并保存在云存储中。与传统的 on-premise 嵌入式应用平台相比，物联网云平台暴露的攻击面大大增加，如何规划整个云计算系统的安全防护能力，防止恶意攻击者攻破并窃取有价值数据，将是云服务商面临的巨大挑战。

第二 . 云平台可信度

物联网平台上存储的数据的拥有者为物联网设备拥有者或物联网厂商，但数据存放在云端，数据拥有者缺乏物理上的控制权会带来潜在的风险。此外，云服务商的恶意内部员工可能窃取或篡改物联网应用数据，云平台的可信度是物联网上云的挑战之一。

第三 . 云服务可用性

物联网应用会管理上百万规模的物联网设备，所以物联网服务的可用性就显得尤为重要。当云服务出现服务终端，或被拒绝服务，则整个物联网应用可能会陷入瘫痪。

第四 . 来自云平台的攻击

如果攻击者攻破了云平台，或恶意内部员工控制了物联网云服务，则可以通过云端指令向物联网设备下发指令，如下载恶意代码、对特定目标发动拒绝服务连接等，从而影响特定或所有的物联网设备的安全性。这将比破解一两个物联网设备的危害性大得多。

总之，当云计算应用在物联网场景下，既要考虑到云计算自身的安全问题，还要考虑物联网在云计算的应用中独特的挑战。

边缘计算带来的安全挑战

边缘计算将远程计算存储拆分成了云端和边缘两级，那么会存在以下安全挑战：

第一 . 认证机制

为了加快认证速度，会在云端和边缘侧实现协同的认证机制。当云端认证通过后，边缘节点会缓存认证信息。但整个过程需要考虑各种因素，例如重放攻击、凭证失效时间等，以防止攻击者绕过云端认证，伪造边缘节点控制物联网终端。

第二 . 由于带宽和实时性要求

业务安全的数据分析会将大量的训练过程放到云端，而将分类过程放在边缘节点，但该计算模型需要考虑数据分析的准确率和响应速度。在业务量巨大的物联网网络中，这将会是一个巨大的挑战。即便误报率降到很小的比例，乘以海量的事件数，也是人力难以处理的量级。

第三 . 运营商网络中的边缘节点尽可能靠近业务位置

该边缘节点除了业务处理外，还需要具备相应的安全能力，那

么边缘节点中按需的安全防护能力，一个安全防护机制，是在核心网络部署，还是在边缘节点部署，需要考虑资源约束条件和服务需求，都是考验运营商网络架构和安全体系成熟之处。

5G 网络带来的安全挑战

5G 网络存在三种应用场景，其中两个与物联网相关。其中：高可靠性与低延迟通信 uRLLC 可以将延迟降低到 1ms，那么这些实时性很高的应用中就应该将后端的处理时间也压缩到同等数量级左右，这对整体系统设计和性能优化提出了很强的要求；此外海量连接通信 mMTC 可在每平方公里管理十万台物联网终端，那么也对边缘节点的高并发长连接能力提出了要求。如果这些物联网应用在设计上不考虑通信网络、边缘节点和应用场景，很容易在服务可用性、认证和加密性能上出现瓶颈。

此外，5G 网络实现了全网络 IP 化，即在接入网、汇聚网和核心网都运行了 TCP/IP 协议，在此基础上可部署基于 X86 的计算存储资源实现服务编排，那么是否可以利用 SDN/NFV 技术，在上述网络中部署可快速生效的安全资源，并将安全能力融合进标准的 NFV 架构，形成可管理可控制的安全资源池，是向安全厂商和运营商提出了新的挑战。

合规性的挑战

当物联网服务保存用户终端的数据时，必然会涉及到用户隐私问题，2018 年 5 月欧洲的通用数据保护法案 GDPR 正式落地，届时会对物联网服务商的方案中的数据存储、数据传输提出了很强的合规性要求。例如车联网应用中需要对车辆标识、PKI 等做匿名化处理，以防止被攻击者跟踪行迹。

此外，一些国家考虑到网络空间主权，颁发的法律法规也对服务商数据存储的归属做出了规定。这对于物联网应用的架构、国际化（i18n）和服务承诺（SLA）都提出了挑战。

新型基础设施下的物联网服务的安全对策

云计算平台的安全防护

在云服务商的角度，首先应在设施、平台和应用层面保证云计算系统的安全性，从而保障运行的物联网平台安全。

例如，在云计算系统和虚拟环境建设时，应根据业务的安全需求，事先划分安全域，并在边界侧部署访问控制策略；并分析物联网服务所面临的安全威胁和自身的脆弱性特点，有针对性的部署检测和响应机制，在运行时检查网络流量和终端内部行为，建立正常场景下的基线，分析异常的行为，对恶意攻击进行隔离、响应和溯源取证。

面向物联网服务的安全云

在用户的角度，除了云服务商的安全机制外，还应该有独立的

第三方在安全厂商的提供专业的安全保证，例如对物联网终端到云端数据流进行安全防护，以及对物联网云服务的安全检查。这些针对应用即服务 SaaS 的业务，现在国外较为成熟安全机制为基于云访问的安全代理（CASB，Cloud Access Security Brokers）。

CASB 一般部署在终端到云端之间的某个位置，对经过的数据在业务层面进行分析和处理，CASB 通常有三种部署方式：

1. 云端代理

即通过反向代理设置数据流经过 CASB 云。在物联网场景中，安全厂商会构建一个面向物联网应用的安全云。

2. 企业侧

即 CASB 网关。在物联网场景中，该网关会演变为边缘网关，但有处理物联网业务的能力。

3. 云端 API 模式

用户在 CASB 云端和业务云平台设置订阅监控操作，当业务云端发生事件时，CASB 云会收到回调通知，进行处理。在物联网场景中，要求物联网云平台提供开放的接口，可向第三方安全平台提供事件订阅通知的功能。

总之，安全厂商可建立面向物联网应用的安全 CASB 机制，从业务角度分析物联网设备或物联网服务运行状态，找到潜在的异常和恶意攻击。

借助 SDN/NFV 构建管道侧快速响应能力

4G 网络在核心网可利用通用的 X86 服务器部署资源池，利用 SDN/NFV 技术实现按需的网络服务链，5G 网络则更进一步，在接入网、汇聚网和骨干网均具备了 SDN/NFV 的资源池能力。安全作为业务的一部分，自然也能成为服务链中的一环。

当物联网的业务数据经过运营商网络时，运营商可根据业务特点和威胁态势，在最靠近业务层调用安全资源，进行防护。例如当运营商的态势感知系统发现某地大量的物联网僵尸主机连接 C2，则可动态向 SDN 网络设备下发阻断指令；当发现有僵尸网络针对某个目标发动 DDoS 攻击，则可快速在近源侧准备好虚拟化清洗设备资源池，通过 SDN 控制器将流量调度到清洗资源池进行缓解。

可见，运营商可充分利用物联网设备和服务的威胁情报，构建针对物联网的知识库，利用 SDN 和 NFV 技术按需构建安全资源池，在此基础上针对多个物联网威胁或脆弱性场景提供安全增值服务，在管道侧实现全面的安全防护。

充分利用边缘计算提高安全服务质量

如前述所，运营商网络中可部署安全资源池，提供按需的安全服务；从物联网云服务商的角度看，也可以在云端侧部署相应的 CASB 安全机制。但考虑到安全检测机制的实时性和安全数据分析所花费的带宽资源，如果物联网服务商或运营商支持边缘计算，则可将上述安全机制一部分卸载（offload）到边缘侧，提高安全服务的质量（QoS）。

上一节提到运营商用靠近物联网设备侧的接入层安全资源池对 DDoS 流量进行清洗，就是一个典型的边缘侧提供的安全服务。此外，基于代理的物联网 CASB 服务在一些实时性要求较高的异常检测应用中，也需要在边缘侧部署一些偏分类功能的检测节点，当发现异常行为时进行实施阻断，而不需要考虑与 CASB 云服务的延迟开销或网络

状态。

改进的认证方式和密码算法

借助新型基础设施和新的技术发展，很多实时性要求很高的物联网应用成为可能，例如智能交通中的协同驾驶、工业互联网下的业务控制。这些应用场景下必然会存在安全攻击，例如在 V2V 无线网络中，恶意攻击者伪造身份实施女巫攻击；在工业互联网中，攻击者伪造或重放控制指令，那么身份认证和通信加密就成为了物联网应用的必选项。

但在车联网场景下，高速运行的车辆通常交互时间不会超过数秒，在此间隔内完成身份认证、密钥交换、数据加密等操作，就要求在设计认证和密码算法时考虑到时延。

此外，在涉及到隐私的物联网场景下，密钥生成还需要考虑到匿名性、可管理的不可回溯性等属性。在弱终端的场景下，加密算法还需要考虑能耗和处理性能等问题。

总之，实现安全的物联网应用必须考虑认证和加密机制，但设计或选择适合相应场景的认证和加密机制尤为重要。

设想的物联网安全架构

综上所述，在新型基础设施支撑下的物联网安全架构将是层次化复合体系。

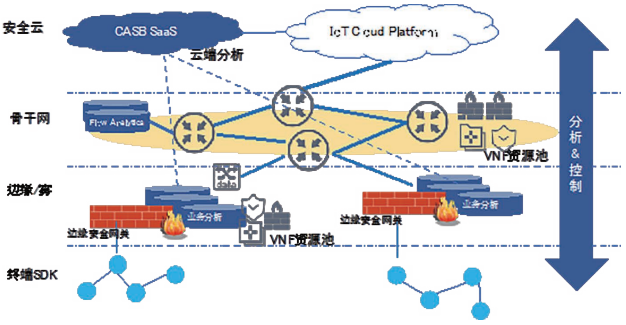
在终端或边缘侧，应内置安全 SDK 或 Agent，除了安全加固外，还可接收安全云端的安全处置指令。

此外，边缘侧应具备安全分析的部分能力，对流经的数据进行在线实时的分析识别；同时，具有根据云端指令按需准备虚拟化安全资源的能力。

在运营商骨干网侧，可利用 SDN 和 NFV 技术实现快速、按需和灵活的威胁感知、安全检测、应急响应的安全能力，提供定制化的安全服务。

在云端，安全厂商部署安全 SaaS 服务，在业务层面提供海量、细粒度的物联网业务安全分析和物联网威胁情报服务。物联网云服务商提供完备的云安全防护机制，应对针对应平台的种种攻击。

需要说明的是图中只给出了主要功能组件的关系，要实现前述的物联网安全防护，还需关注两个核心控制应用：第一是 CASB 云服务和边缘侧业务分析的整体检测机制；第二是运营商整体的安全防护决策和调度应用，涵盖了骨干网和边缘侧的所有资源池管理。设计好这两类应用的架构，是实现灵活有效物联网安全体系的重要前提。



参考文献

[1] AWS IoT Service, https://aws.amazon.com/iot/

2017年国内恶意物联网设备分析

创新中心 桑鸿庆

关键词：物联网 IP 画像 恶意分析

摘要：近两年来，随着物联网相关技术的发展，几乎所有的家用电器都可以接入网络。智能化的应用给生活带来便利的同时，其副作用也随之而生。2016 年，攻击者使用 Mirai 病毒用僵尸物联网设备让一个新闻网站的重要防火墙瘫痪之后，紧接着 Dyn DNS service 遭受到攻击，使得美国网络中流砥柱的公司大面积瘫痪，影响遍及数百万人群。而 Mirai 能够在识别物联网设备的同时令其感染病毒使之成为僵尸网络，进而集中控制物联网设备，发起分布式拒绝服务 (DDoS) 攻击，大量垃圾流量会渗透进入目标服务器，令服务器瘫痪。如今，受到威胁的不再只是电脑，网络摄像头和路由器也早已危机四伏，因此对物联网僵尸网络的识别及攻击预测，显得尤为重要。

一 . 引言

通常情况下，可以从地址类型、网络位置、行为位置、风险类型等多个方面对某一 IP 进行描绘，IP 维度上产生的信息，可以在很多业务场景中配合使用，如果对一些可疑的 IP 进行合理的描绘，输出相关的情报信息，从某些方面讲也可以为恶意攻击提供一定的预

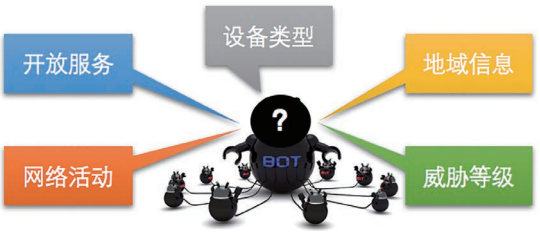


图 1 物联网恶意 IP 可选的描绘维度

警能力。本文对物联网设备的 IP 进行了分析，主要从**设备类型**，**开放服务**，**地域信息**，**攻击类型**四个方面进行描绘，而且对这些维度进行分析，从中得出现有的恶意物联网 IP 的特征，并分析这些特征产生的可能原因。

由 2017 年 3 月份绿盟科技创新中心物联网安全实验室和威胁情报实验室联合发表的《国内物联网资产的暴露情况分析》中了解到，国内有十几种物联网设备存在数量较多的暴露情况，根据数量排序

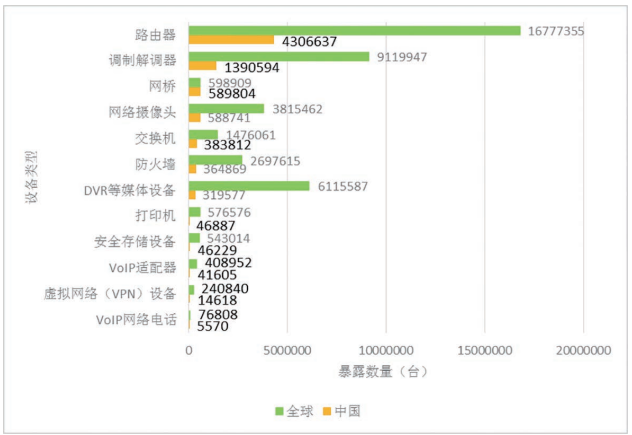


图 1.1 全球和国内物联网相关设备暴露情况

依次列出。

本文物联网资产数据全部来源于 NTI（绿盟威胁情报中心），通过设备类型标签提取出物联网资产，将结果与历史攻击事件数据库 (2017 年上半年数据) 中 3000w IP 进行撞库处理，最后共获得 77860 条恶意物联网资产记录，并将以上两个数据库的字段相结合做了如下相关分析。

二 . 恶意物联网设备分析

2.1 攻击类型分析

观点 1：恶意的物联网资产以肉鸡为主，主要发动扫描和 DDoS 攻击

我们对威胁 IP 历史攻击事件数据库中提取的恶意物联网资产的攻击类型字段进行统计，对于物联网资产而言，多数恶意的物联网设备都是被其他主机控制，组成僵尸网络进行攻击。如图 2.1 所示，

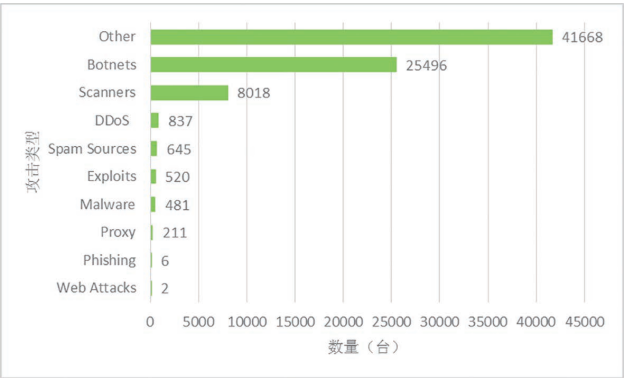


图 2.1 恶意物联网资产攻击类型数量分布

除了其他攻击类型以外，Botnet（僵尸网络）总量占比最多，主要做 Scanners（扫描器）和 DDoS 攻击。当初的 Mirai 事件就是黑客利用物联网设备的弱口令等安全漏洞，主要对网络监控设备实施入侵，并植入恶意软件构建僵尸网络进行 DDoS 攻击，致使被攻击的网络瘫痪的现象。

2.2 设备类型分析

观点 2：恶意物联网设备中路由器和网络摄像头数量最多，占恶意总量 90% 以上

从上图可以看出恶意物联网 IP 中路由器和网络摄像头两种设备占总量的 90% 以上，是什么导致二者数量占比这么多呢？分析猜测有以下几点原因。首先，从图 2.2 物联网资产暴露情况来看，恶意物联网设备类型的数量排名与暴露的数量的排名几乎相吻合，暴露的基数越大该设备被控制的数量可能就会越多；其次，因为多数人并不知道路由器，摄像头等物联网设备会被大规模植入恶意软件，所以此类设备很少有防护，而且具有常开的特性，操控者不担心会失去连接，这为攻击提供了很大的便利；最后也跟 NTI 的物联网资产数据有关，可能因为 NTI 对摄像头和路由器识别基数大，所以路由器和摄像头的恶意资产较多。以上等等均为推测，欲知确切原因，还需要更多数据进一步佐证。

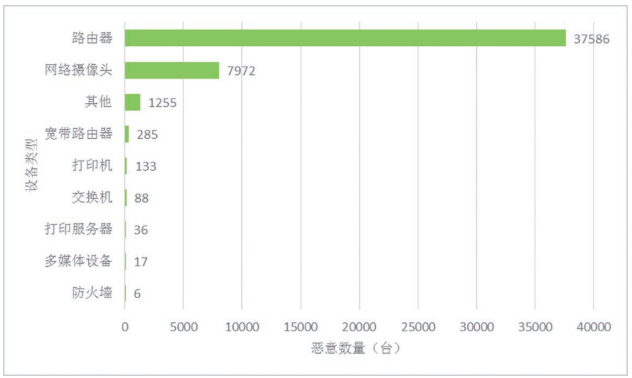


图 2.2 恶意物联网设备类型分布情况

2.3 地域分布分析

观点 3：全球恶意的物联网僵尸网络大多数分布在人口较多的发展中国家

印度的物联网僵尸网络数量最多，其次是中国和巴西，三个都

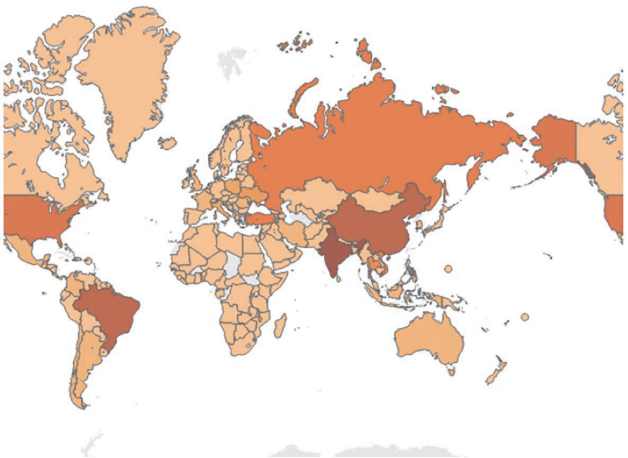


图 2.3 恶意物联网设备全球分布示意图

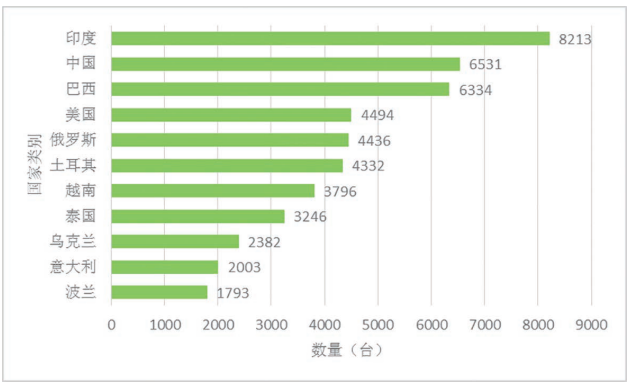


图 2.4 恶意物联网设备国家数量分布

是发展中国家，而且人口基数都很大，可能对路由器、摄像头等物联网设备需求也较多，并且一定程度上说明这些国家地区的人们对物联网安全意识相对薄弱。

观点 4：国内恶意的物联网僵尸网络主要分布在东南沿海地带，包括长三角，珠三角和京津冀经济带，香港地区是重灾区

如图 2.5 所示，恶意物联网设备主要分布在东南沿海和京津冀地带，产生这一现象可能是因为发达的经济带物联网设备的基数本身就大，所以这些地区的恶意物联网设备数量相对其他地区会多一些。当然这只是一种猜测，具体原因还需进一步的数据支撑和分析得出。由图 2.6 可知，香港地区的恶意物联网资产数量最多，且根据《国内物联网资产的暴露情况分析》显示，该地区的物联网设备暴露情况令人堪忧，看来暴露情况和恶意情况很可能正相关。

图 2.5 恶意物联网设备国内分布示意图

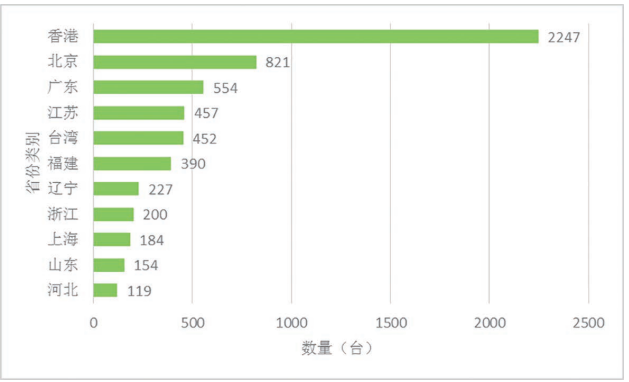


图 2.6 恶意物联网设备国内数量分布

2.4 开放服务分析

观点 5：被控制的物联网设备大部分开放多个端口，开放最多的是 WEB 服务。

对恶意的物联网设备开放的服务数量进行统计（端口开放可能包

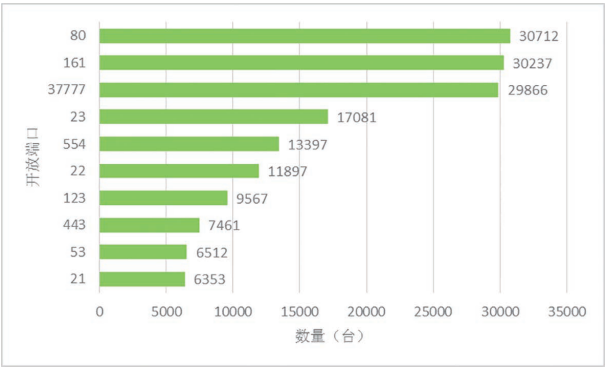


图 2.7 恶意物联网设备的端口分布

括历史数据），其中绝大部分开放端口为 80，161，37777。通过分析恶意物联网资产协议和默认端口的对应关系，发现开放最多的协议为 HTTP 协议（图 2.8），也就是说在恶意的物联网设备中，开放最多的是 WEB 服务。

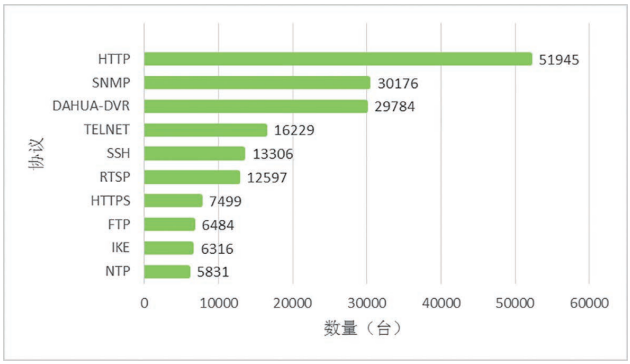


图 2.8 恶意物联网 IP 开放协议情况

三 . 总结与展望

当然以上都是从客观的维度进行的分析，但是如果想找到恶意的物联网设备，还需根据具体的网络活动看其是否有恶意的行为，包括是否与 C&C 主机连接行为和是否有攻击行为两个方面。如果能查到某物联网资产与已知的 C&C 主机连接，该物联网设备就有肉鸡的嫌疑，而该物联网资产有攻击相关流量，就可以进一步确定其为肉鸡。

分析了这么多，作为使用者我们该如何防止自己的物联网设备，不被他人攻击呢？这里结合我们的分析，简单的总结了一些建议：

1. 修改初始口令以及弱口令，加固用户名和密码的安全性；

2. 关闭不用的端口和服务，如 FTP（21 端口）、SSH（22 端口）、Telnet（23 端口）等，WEB 服务尽可能的不暴露在公网；

3. 及时升级设备固件，修复漏洞。

如果您对技术不是很了解或者没有精力设置设备，但又担心家里的物联网设备遭受攻击，也许你需要一款具备安全能力的路由器。根据上文的分析安全路由器应至少具备以下能力：

• 扫描识别能力

对接入路由器内的设备进行定期扫描，识别其设备类型、开放服务、固件版本号等信息，提示使用者关闭不必要的端口和服务，对存在高危的固件版本提示升级。

• 恶意行为监测

对路由器内设备的访问连接行为进行识别，根据威胁情报等信息对设备连接的恶意的 IP 或 URL 进行告警或阻断，保护内网设备不被恶意主机连接控制。

随着家庭物联网设备种类的增多，其攻击面也必然会越来越广，相对于安全问题，消费者可能更会将精力放在产品的使用。可安全问题怎么办呢？所以如果在家庭的场景中配置一个安全路由器，让其来辅助消费者保护家中的智能设备的安全，似乎可以很好的解决以上冲突。随着技术的进步，人们对智能设备需求的增加，物联网设备的攻击面肯定不仅限于本文提到这些，所以关于安全路由器的能力可能还需进一步的挖掘和探讨。

物联网弱设备防护方法

创新中心 张克雷

关键词：弱终端 固件安全 网络安全 防护方法 硬件安全

摘要：物联网设备存在许多的安全隐患，如何消除这些安全隐患呢？本文以弱设备为例，阐述如何对弱设备进行加固，着重介绍物联网弱设备存在的安全隐患和加固方法，以解决已经出现的安全隐患。希望可以对网络安全从业者和嵌入式工程师提供有价值的信息。

一 . 简介

近年来，随着物联网技术的迅速发展，物联网产品的数量也在呈爆发式增长。Gartner 预测，两年后，物联网设备的装机量将超过 200 亿 [1]，这些物联网设备所带来的信息量将非常庞大。与此同时，因物联网设备导致的大量的信息安全隐患也在逐年增加，甚至有些隐患已经造成了不可挽回的损失，如 2016 年底的 Mirai 事件 [2]，就是因为大量的暴露在互联网上的物联网设备存在弱口令和未修复的漏洞引起的。2018 年 3 月 27 日，《绿盟科技 2017 物联网安全年报》[3] 发布，其中对物联网资产的暴露情况、物联网设备的脆弱性和物联网设备面临的威胁风险进行了分析，并给出了物联网安全防护体系。

物联网设备之所以存在安全隐患，是因为其暴露了足够的敏感信息，从而被攻击者利用来制造攻击。这些敏感信息，从暴露位置来看，可分为两类：一类是存储在设备中的固件和印制在产品内部的信息（如 PCB 丝印、芯片型号）等，在本文我们暂时称其为本地信息；另一类是传输在网络（不仅仅是以太网、Wi-Fi、蓝牙等）中的信息。

目前看来，不论是生产厂商还是用户，对弱设备 [3] 的安全问题的关注并不是非常足够。例如，在 2017 年 9 月的 XPwn2017 未来安全探索盛会 [4] 上，某黑客逆向了某共享单车的单片机程序，从而挖掘出了漏洞。2017 年 10 月，物联网安全研究人员渗透进 LIFX 智能灯泡的 Zigbee 网络 [5]，并对设备的固件进行逆向破解，从而得到了其 Wi-Fi 网络密码。

由此可见，物联网设备存在许多的安全隐患，而且，我们面临一个挑战：如何消除这些安全隐患。本文就以弱设备为例，阐述如何对弱设备进行加固，解决已经出现的安全隐患。

后续小节中，笔者会先介绍物联网弱设备存在的安全隐患，再介绍物联网弱设备的加固方法与建议，最后再进行简单地总结。

二．物联网弱设备存在的隐患

一般，攻击者会收集足够的信息，以利用现有的漏洞或挖掘新的漏洞对设备发起攻击行为。如果攻击者拿不到可以利用的信息，设备的安全隐患也就不会存在。物联网弱设备一般会暴露哪些信息呢？从信息的位置看，可以分为本地的信息和网络中的信息两类。接下来，将从这两方面介绍物联网弱设备存在的安全隐患。

2.1 本地信息

所谓本地信息，这里定义为可以通过购买设备，观察或者使用工具直接对产品接触式操作获取到的信息。一般包含 PCB 丝印、硬件接口、固件信息等。

2.1.1 PCB 丝印

PCB 中文名称为印制电路板。在设计和制作 PCB 的过程中，丝印为工程师的焊接、调试工作带来了极大的便利。然而，在产品出厂后，它上面的 PCB 丝印信息对用户没有任何帮助，反而为攻击者的成功破解提供了信息。

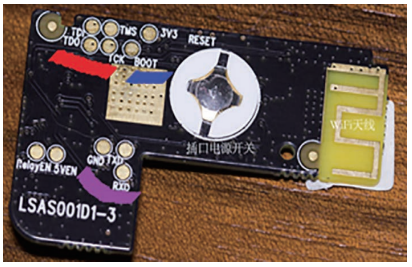


图 1-- 某智能插座 PCB 丝印信息

以图 1 所示的 Wi-Fi 智能插座 [6] 为例，在 PCB 上，插座暴露了三类敏感信息：JTAG 调试接口（红色标记的位置）、UART 接口位置（紫色标记的位置）和设置程序启动位置的 BOOT（蓝色标记的位置）。JTAG 和 UART 是芯片供应商提供给工程师进行读取和下载程序的两类接口。攻击者也可以利用这两类接口尝试把固件读取出来。其具体的读取、下载方法，可参考《渗透低性能智能设备的关键技术 - 固件提取》[7]。

2.1.2 硬件接口和芯片信息

上节已经提到了 JTAG、UART 接口信息。事实上，这两类接口对攻击者是最有帮助的，因为只需要一些工具，就可以把设备内的固件信息读取出来，进而分析出更多的信息。

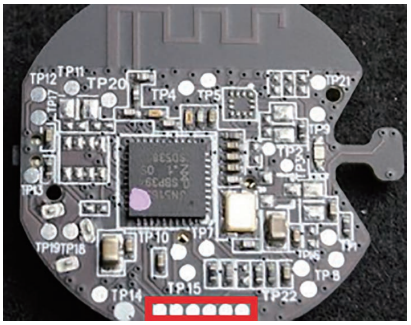
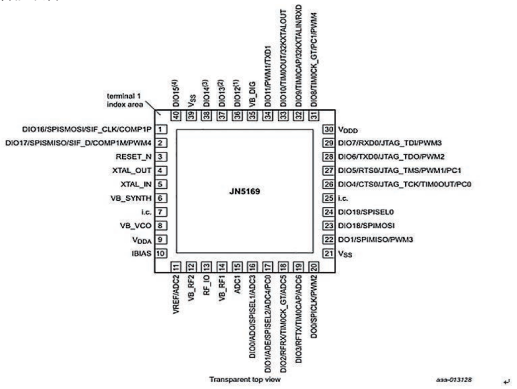


图 2-- 某智能设备 PCB

以图 2 所示的 PCB 为例，我们很容易发现规则排列的 6 个焊盘（红色方框标记），结合芯片上的型号信息（JN516x），很容易在芯片手册 [8] 中查到该芯片的引脚图和芯片的固件下载方式，如图 3 所示。

根据图 3，结合万用表，可以测试出这 6 个焊盘和芯片的引脚是否直接相连（短路测试），如果是直接相连，就可以确定，该接口是用来下载程序的。事实上，芯片 JN5169 下载程序使用的接口，一共需要的也是 6 个。



[3] UART programming mode: leave pin floating high during reset to avoid entering UART programming mode or hold it low to program.

图 3--JN5169 的芯片引脚图

f8wConfig.cfg

```
-DMAX_RTG_ENTRIES=40

/* Maximum number of entries in the Binding table. */
-DNWK_MAX_BINDING_ENTRIES=4

/* Maximum number of cluster IDs for each binding table entry.
 * Note that any value other than the default value may cause a
 * compilation warning but Device Binding will function correctly.
 */
-DMAX_BINDING_CLUSTER_IDS=4

/* Default security key. */
-DDEFAULT_KEY="{0x01, 0x03, 0x05, 0x07, 0x09, 0x0B, 0x0D, 0x0F, 0x00, 0x02, 0x04, 0x06, 0x08, 0x0A, 0x0C, 0x0D}"

/* Reset when ASSERT occurs, otherwise flash LEDs */
//-DASSERT_RESET
```

图 4--Z-Stack 中的默认密钥信息

以图 2 所示的 PCB 为例，我们很容易发现规则排列的 6 个焊盘（红色方框标记），结合芯片上的型号信息（JN516x），很容易在芯片手册 [8] 中查到该芯片的引脚图和芯片的固件下载方式，如图 3 所示。

根据图 3，结合万用表，可以测试出这 6 个焊盘和芯片的引脚是否直接相连（短路测试），如果是直接相连，就可以确定，该接口是用来下载程序的。事实上，芯片 JN5169 下载程序使用的接口，一共需要的也是 6 个。

攻击者定位程序下载接口所需的信息，只是通过搜索设备拆解文章，或者把设备买回来拆解后即可获取。攻击者获取这些信息的目的非常明确：拿到固件，从而分析出更多的信息或挖掘出网络通信相关的漏洞。

2.1.3 固件信息

固件中几乎包含了除了网络信息中的全部信息，包括程序执行流程，初始化参数等。如果双方通信的内容一开始就是被加密的，那初始或默认的加密参数（如密钥、初始向量）等信息将被编码到固件中。如 Z-Stack 协议栈中，Zigbee 通信的默认密钥会被硬编码，如图 4 和图 5 所示。如果再深入一些，

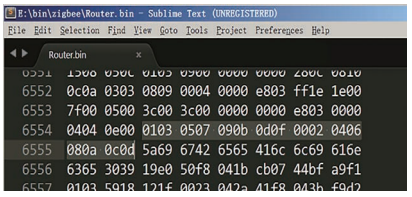


图 5-- 编译 Z-Stack 得到的固件中，Zigbee 通信使用的默认密钥

在 IAR 编译环境下生成多个固件，分析该密钥出现的位置，就会发现密钥出现的位置比较有规律。

2.2 网络信息

网络中包含两类信息，一类是用于控制的信息，另一类是用于共享、存储的信息。一般，如果网络信息存在隐患，说明前者会存在设备失控的隐患，或者后者存在隐私泄露的隐患。

一般，网络中存在的攻击有以下几种：

1. 重放：蓝牙、wifi 等协议，云管端通信的应用层控制报文等。

2. 明文：HTTP 协议等不安全协议的应用，导致敏感信息泄露、设备受控等。

3.DoS：拒绝服务攻击，使设备不能正常提供网络服务。

接下来，笔者以低功耗蓝牙协议栈为例，简单介绍控制信息和存储 / 共享信息在网络传输过程中存在的隐患。

低功耗蓝牙协议栈和其他的协议栈一样，也可以采用分层模型来理解。一般，制造低功耗蓝牙芯片的厂商会在芯片手册中介绍协议栈，并总结出类似的分层模型。此处引用 Nordic[9] 总结的模型，如图 6 所示，大抵可分为 3 层，底层为 Controller，中间层为 Host，顶层为 Profiles。

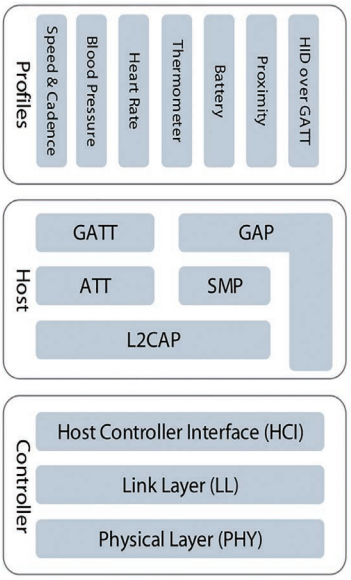


图 6-- 低功耗蓝牙协议栈分层模型

这里不对协议栈做深入的分析，但是，需要注意的是 GATT 部分。当蓝牙设备通信在 GATT 层时，通信双方可理解为 Client 和 Server，当二者建立连接后，可以相互对双方的服务(以 UUID 标识)进行读写。例如:

介绍两个例子，分别代表控制信息被利用，用于共享、存储的信息被非法获取这两种情况。一般情况下，如果往 UUID 为 0x1802 的服务中写入值，会引起设备报警。如果低功耗蓝牙设备（A，用户实际使用的产品）没有对攻击者使用的蓝牙设备（B，电脑、手机等双模蓝牙设备）进行身份认证，攻击者在利用 B 攻击 A 时，非常容易写入成功，即引起设备异常报警。同样，也可以读取 A 设备内 UUID 为 0x180D 的服务中的数据来获得用户的心率（前提是信息没有被加密）。事实上，某些厂商的手环类产品的通信过程是没有经过加密的，造成了设备可控或隐私信息泄露。

```
#define BLE_UUID_HEART_RATE_SERVICE                0x180D    /**< Heart Rate service UUID. */
#define BLE_UUID_HUMAN_INTERFACE_DEVICE_SERVICE    0x1812    /**< Human Interface Device service UUID.
#define BLE_UUID_IMMEDIATE_ALERT_SERVICE           0x1802    /**< Immediate Alert service UUID. */
#define BLE_UUID_LINK_LOSS_SERVICE                 0x1803    /**< Link Loss service UUID. */
```

图 7-- 协议栈中预定义的 UUID

三 . 加固方法与建议

一般，漏洞挖掘过程会涉及代码审计、黑盒测试、文档研究等。本节的弱设备加固方法会最大限度地保证攻击者无法对弱设备进行代码审计，保证黑盒测试结果中不会存

在有价值的信息。所以，笔者提出防护方法的目的很明确：不让攻击者获取到源码、固件、端口等信息。禁止这些信息泄露的方法很直接，可以分两步：信息读保护设置和信息加密设置。这样能保证: 有信息不可读（不可见），即使读出来，也极难解密。

3.1 信息不可读的方法

针对 PCB：

一般，PCB 上会有丝印、接口、芯片型号等信息，这些信息为攻击者查找固件提取接口提供了便利。如图 1 所示，暴露的 JTAG、UART、BOOT 模式选择接口能使攻击者可以有目标地提取出固件。

所以，建议开发工程师把 PCB 丝印、芯片型号等信息清除，同时，把下载固件的接口移除。但是，这并不能从根本上解决问题，如果攻击者熟悉主控芯片的封装，通过测试总是可以匹配上的。

针对固件 -MCU 内部：

弱设备由控制芯片和外围模块（如传感器、联网模块等）组成，代码在控制芯片中或联网控制芯片上或联网模块中。可以做到固件不可读。存储设备有读保护能力。可以通过设置一些读保护选项，使内存里的内容不可读。

以常见的 STM32f1 系列的单片机为例：

可以通过设置 RDP（Global Read-out Protection）寄存器的值来改变单片机内部 flash 读保护选项。当启用读保护选项时，单片机的固件是无法通过 JTAG 和 UART 接口读出来的。也就是说，必须破坏芯片结构，才有可能把芯片内部的程序读出。

这项保护是通过设备 RDP 选择字节启动的。当保护字节被写入相应的值以后，实施下述保护：

- 只允许从用户代码中对主闪存存储器的读操作（以非调试方式从主闪存存储器启动）。
- 第 0~3 页（小容器和中容量产品），或第 0~1 页（大容量产品）被自动加上了写保护，其它部分的存储器可以通过再主闪存存储器中执行的代码进行编程（实现 IAP 或数据存储等功能），但不允许在调试模式下或在从内部 SRAM 启动后执行写或擦除操作（正片擦除除外）。
- 所有通过 JTAG/SWD 向内置 SRAM 装载代码并执行代码的功能依然有效，亦可以通过 JTAG/SWDCONG 从内置 SRAM 启动，这个功能可以用来解除读保护。当保护的选择字节转变为存储器未保护的数值时，将会执行整片擦除过程。

图 8--STM32f1 系列单片机的 RDP 功能

类似的功能不仅仅出现在 ST 公司的芯片中，还有 NXP 的 CRP（Code Read Protection）、TI 的 FMPRE 寄存器等。

实现这一安全能力，需要产品研发团队投入足够的精力在 MCU 的读保护策略的学习上，以保证代码安全。

针对固件 -MCU 外：

对弱设备来说，目前市场上，MCU 外的固件会存放在专门的 ROM 芯片中，如以 SPI 总线进行通信的 SOP8 封装的 W25Q128 系列，如图 9 所示。

一般，之所以选用 Flash 芯片作为存储固件的存储器，是因为仅仅一个 MCU 中集成的 Flash 容量，不足以保证协议栈的完整

图 9--SOP8 封装的 Flash 芯片

移植。

所以建议协议栈的代码和产品业务相关的代码分开，在 MCU 中运行业务相关的代码，并使用读保护功能开启，这样即可保证业务代码不可读。必要时，可以对协议栈的代码进行部分加密保护和混淆，以防止攻击者进行逆向分析或漏洞挖掘。

3.2 信息加密

比较安全的加密算法是 RSA，而且，根据目前的 MCU 发展情况看，在 MCU 中实现 RSA 加密体制并不难。如 IEEE 802.15.4 无线芯片 cc2538 的内部集成了 ECC RSA-2048 加速器，可以提高单片机在 RSA 密码体制下的工作效率；ST 公司提供了加密的库函数（Cryptographic Library）。从当前芯片的性能看，在弱设备上做 RSA 加密已经不是一个难题了。

协议栈

以 lwip 协议栈为例，在协议栈的官方文档中，找不到关于加密传输的内容，所以，有必要对该协议进行二次加密功能的集成，如图 10 所示。

```
FEATURES

 * IP (Internet Protocol, IPv4 and IPv6) including packet forwarding over
   multiple network interfaces
 * ICMP (Internet Control Message Protocol) for network maintenance and debugging
 * IGMP (Internet Group Management Protocol) for multicast traffic management
 * MLD (Multicast listener discovery for IPv6). Aims to be compliant with
   RFC 2710. No support for MLDv2
 * ND (Neighbor discovery and stateless address autoconfiguration for IPv6).
   Aims to be compliant with RFC 4861 (Neighbor discovery) and RFC 4862
   (Address autoconfiguration)
 * UDP (User Datagram Protocol) including experimental UDP-lite extensions
 * TCP (Transmission Control Protocol) with congestion control, RTT estimation
   and fast recovery/fast retransmit
 * raw/native API for enhanced performance
 * Optional Berkeley-like socket API
 * DNS (Domain names resolver)
```

图 10--lwip 协议栈的特性

比较理想的是利用 RSA 和 AES 混合加密方法：利用 RSA 来加密传输 AES 密钥，再基于 AES 加密实现数据传输。因为，设备端保存的公钥是没有解密能力的，仅仅根据密文和公钥解密出 AES 密钥非常困难，攻击者得不到解密密钥，那就没办法对信息解密，从而保证了信息传输的安全。

应用层通信

应用层加固的方法有三个：加密应用层传输的数据、关闭不必要的端口开放、黑白名单策略。

加密应用层传输的数据可以解决 2.2 节中提到的蓝牙数据包被解密的导致的一系

列问题。安卓手机可以对蓝牙通信过程以日志的形式进行抓包保存，保存后，可以使用 wireshark 等工具软件打开该日志文件进行分析，而此时的数据包是经过蓝牙协议栈解密的。如果在产品开发过程中，消息传输的内容是明文的，会导致信息（gatt 的描述信息和值等）泄露的问题出现。此时，加密（依然是采用 RSA 和 AES 加密混合方式）是一个比较好的方式，有助于防止黑客进行加密重放。

作为弱设备，要尽可能的关闭不必要端口，笔者建议不开启端口。弱设备和云端的交互过程中作为客户端角色存在即可。良好的黑白名单机制可以保证设备的通信对象合法。这里对这两种方法不再深入介绍。

四 . 总结

本文通过从本地信息、网络信息这两个角度介绍物联网弱设备存在的安全隐患，进而提出设备加固的方法。总的来说，弱设备防护的思路比较简单，就是消除冗余的信息。只要生产厂商的产品设计方案和研发流程都比较规范，产品存在的安全隐患会比较少，甚至没有。

希望本文的发表能抛砖引玉，甚至可以对大家的安全研究工作和产品研发工作有一些启示和帮助。由于笔者的知识储备和见识有限，如果您在阅读过程中发现一些错误，或者您也有这方面的兴趣或需求，欢迎联系我们。

参考资料

[1]Forecast Analysis: Internet of Things — Endpoints, Worldwide, 2016 Update, Gartner, G00302435, https://www.gartner.com/doc/3597469/forecast-analysis-internet-things-

[2]1127 德国断网事件到底是谁干的？ 绿盟科技发布 Mirai 变种恶意软件技术分析与防护方案，http://toutiao.secjia.com/deutsche-telecom-mirai-attack-analysis

[3] 物联网安全年报，http://www.nsfocus.com.cn/event/iot_security/index.html

[4]XPwn 2017，开创一个安全极智的未来（北京），https://www.anquanke.com/post/id/86778

[5] 如何入侵联网智能灯泡——LIFX 智能灯泡，https://weibo.com/ttarticle/p/show?id=2309404160876054708433

[6] 小米智能插座质量可靠吗? 小米智能插座拆机教程 (2), http://www.pc841.com/shoujizhishi/36768_2.html

[7] 渗透低性能智能设备的关键技术 - 固件提取，http://blog.nsfocus.net/firmware-extraction/

[8]JN5169 芯片手册，https://www.nxp.com/docs/en/data-sheet/JN5169.pdf

[9]NRF51822，蓝牙芯片编程说明，http://www.nordicsemi.com/eng/content/download/34055/573345/file/nAN-36_v1.1.pdf

渗透低性能智能设备的关键技术-固件提取

创新中心 张克雷

一 . 简介

近十年，随着传感器技术、无线通信技术的迅速发展，越来越多的物联网产品出现在我们的视野中，Gartner 预测，到 2020 年，物联网设备的装机量将超过 200 亿，但很多物联网设备受到成本、研发人员安全素质等因素的限制，存在大量的安全问题。例如 2016 年底的 Mirai 恶意代码发动的创纪录 DDoS 攻击，就是因为弱口令和长时间未修复的漏洞引起的。物联网终端的安全，也越来越受到人们的关注。

2017 年 10 月 8 日，物联网安全研究人员渗透进了某智能灯泡，获取到了 mesh 网络内传输的 Wi-Fi 信息（包括 Wi-Fi 密码）。尽管在该案例中 Wi-Fi 密码被加密，但是研究人员依然通过获取设备的底层固件，得到了加密算法和密钥信息，最终得到了明文的 Wi-Fi 密码。固件提取进而分析固件是攻击者常见的渗透手段，反之如果厂商要产出高安全级别的智能灯泡，第一步就是要防止固件内容被窃取。

接下来，我们对这次案例做个简单的分析，然后进一步分析提取固件原理和过程，最后总结在现有的技术背景下获取固件的方法和相应的防护方法。为了描述方便，我们把这种获取固件的技术暂时称为固件提取。

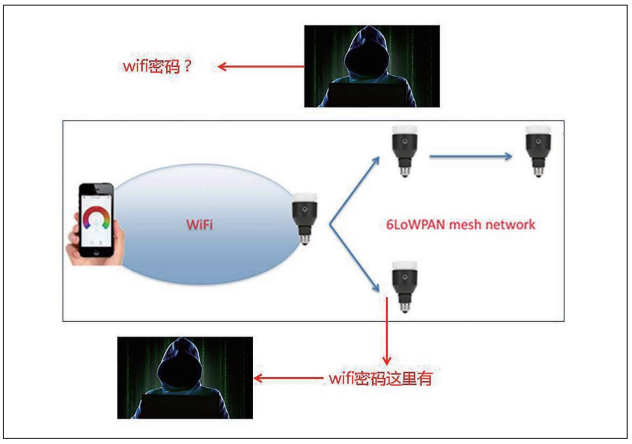
二 . 案例回放

文章中提到的攻击，可以分 3 步：

1. 利用单片机和 zigbee 模块抓取 6LoWPAN 流量中的数据，提取出 Wi-Fi 信息（此时加密的）。

2. 通过提取固件、分析固件，得到 AES 加密函数，并分析出密钥。

3. 根据 2 中获取的信息来解密。



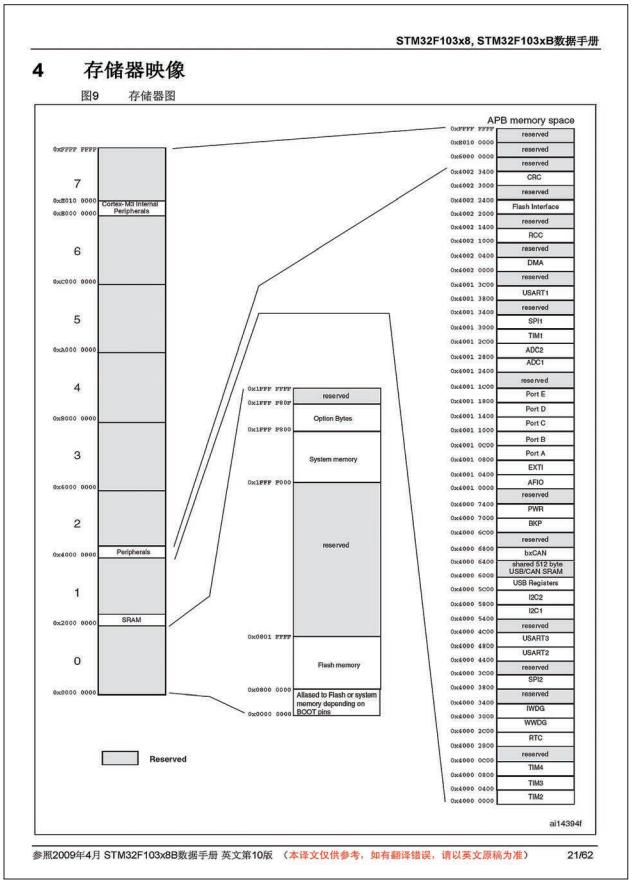
这是一个典型的针对家庭局域网络内的嗅探攻击。今后的物联网设备将有一大部分是作为 mesh 网络节点存在，只不过网关可能是手机、路由器、笔记本电脑等一切具备蓝牙、zigbee、Wi-Fi 等无线联网能力的设备。基于现有的网络来看今后的物联网，设备如果想要具有联网能力，则必须利用至少一条有线或无线的通道连接到互联网。如果是通过 Wi-Fi 连接，必要的信息就是 Wi-Fi 的 SSID 和密码。

案例中，攻击者通过分析固件得到了解密所需的信息——加密密钥。那为什么研究人员可以获取到固件呢？我们就需要分析固件提取的原理，并且分析在现有的技术背景下，提取低性能的物联网节点上的智能设备的固件方法。

三 . 固件提取的原理与方法

我们已经理清楚了攻击的方法，本次就针对其中重要一环：固件提取，谈一谈固件提取的原理，进而总结现有的提取固件的方法有哪些。

以 stm32f103 系列单片机为例。该单片机基于 ARM Cortex M3 内核，片内带有 64KB 的 Flash，20KB 的 SRAM。单片机读取程序到 SRAM 再进行译码。目前已知的有两个地方会存储需要运行的程序:



1. 单片机内的 Flash/ROM。

2. 单片机外挂的 Flash/ROM。

对于存储器来说，读和写的操作是最基本的，即：必然存在一种方式，可以把存储器中的数据读取出来。如果读取的数据是单片机需要翻译的机器码，那么我们就把读取的过程叫提取，把要读取的数据称为固件。

stm32f103c8t6 单片机的片内 Flash 的地址是 0x08000000-0x0801ffff（如上图所示），总共 64KB。如果要提取出固件，有必要了解代码是如何烧写进芯片内的 Flash 区域里面的。

在开发过程中，会有如下过程：

1. 搭建好编译环境，编写高级语言（C 等），编译、生成可执行文件。

2. 搭建好烧写环境，把可执行文件传到单片机芯片中，使单片机上电可以运行。

编译环境就是用把单片机 C 语言程序编译成汇编、机器码等，生成 16 进制 hex 文件或者二进制文件（xxx.bin），一个编译器即可。烧写环境就是把机器码下载到上图的 Flash 区域的过程中所需的工具，包含 J-link、U-link、ST-LINK（stm32 单片机专用）等硬件工具和 STVP、mcuisp 等软件（使用一套软硬件即可）

请注意，烧写、下载、传、提取这四个词，说白了，就是对 Flash 区域读写的过程。目前发现两种读取固件的方式，第一种是依托于生产厂商固化在芯片内的 bootloader，把 Flash 中的固件读取出来，第二种是通过调试接口把固件读出来。第一种需要 bootloader 支持，而且一般是都支持的。第二种是依靠硬件调试工具直接读取。

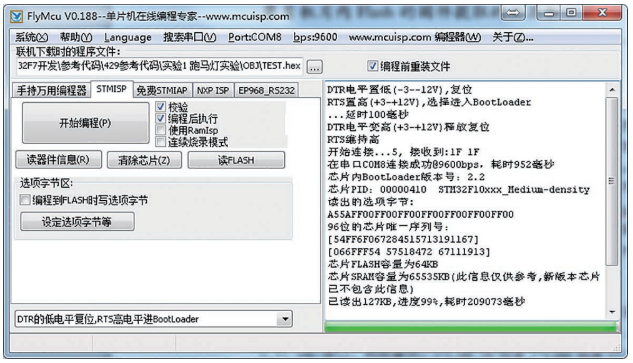
篇幅所限，读取过程中的交互细节不多介绍，直接介绍两类固件提取的工具和方法，一类是以 stm32 单片机为例的单片机固件提取的工具和方法，一类是外挂 Flash 形式的 Flash 固件提取的工具和方法。

3.1 单片机片内 Flash 的固件提取的工具和方法

单片机固件提取方式有两类，一类是通过 bootloader 读取，一类是通过调试接口读取。

1. 利用 bootloader 提取

通过串口，把芯片和电脑相连，运行 mcuisp 软件，点击读



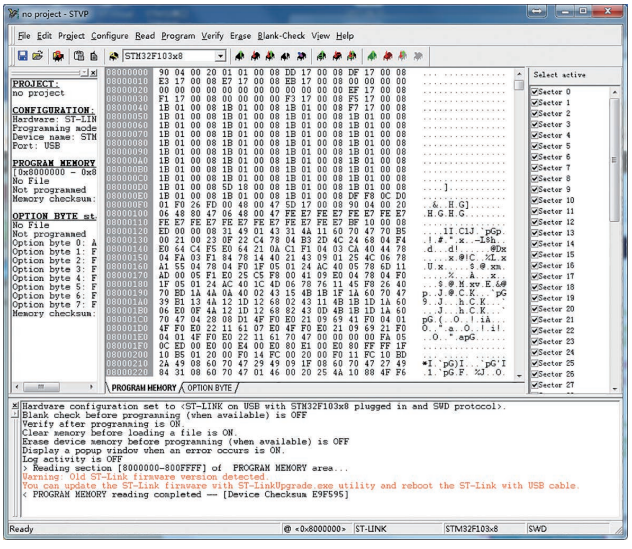
Flash 即可。

mcuisp 软件通常被用来通过串口通信下载固件到单片机。串口通信也是通信技术的一种，目的是实现芯片 A 到芯片 B 的数据传输，是芯片之间经常用到的通信方式。例如：如果我的目的是把程序代码 “abcd” 传输到芯片 A 中，但是，我仅仅通过电脑与没有

bootloader 的单片机进行串口通信，“abcd” 是没办法直接储存到 Flash 区域的，必须在单片机内部写好一段代码，在 “abcd” 已经通过串行接口，一个一个的到达单片机内部的缓冲器时，把 “abcd” 一个一个的转存到 Flash 区域。这样就实现一种电脑直接写入“abcd” 到 Flash 的假象，达到用户无感知或是透明传输的效果。提取固件的过程相反与上述过程相反，只需要利用 bootloader 把 Flash 的内容通过串口通信发送给电脑即可。

2. 利用硬件调试接口提取

在开发单片机程序时，会用到硬件调试工具，实现单步运行来查看程序实时运行的效果。一般可以通过下面两类调试接口，把 Flash 中的数据读取出来。



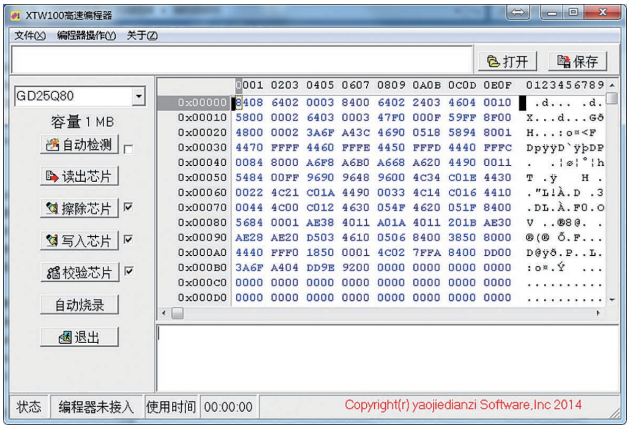
2.1：SWD 接口，利用硬件：J-LINK OB 或者 J-LINK 或者 ST-LINK；利用软件：J-LINK 驱动自带的 J-FLASH 或者 ST 官网提供的 STVP。

2.2：JTAG 接口，利用硬件：J-LINK；利用软件：J-LINK 驱动自带的 J-FLASH。

如果找不到串行接口，可以用这种方式，当然，前提是产品电路板上可以引出这两类接口之一，否则只能取下芯片了。

3.2 单片机片外 Flash 的固件提取工具和方法

作为一个存储器，上电之后不可能自己就把数据显示给我们，就好像 U 盘买回来，得插电脑上，加载完驱动才能读取到里面的数据。对于片外 Flash，需要把 Flash 芯片从产品的电路板中取下来，再放



到另外一个带有 MCU 的电路板上来读取数据。万能的淘宝提供了编程器，方便了对众多 Flash 芯片的内部数据的提取。

这种方式有两个缺点：一是比较暴力，需要把 Flash 芯片从电路板上取下来，再把 Flash 芯片放到编程器上面，利用配套的 PC 端软件，把固件读取出来。二是 Flash 芯片型号需要得到编程器的支持。那问题来了，如果这个编程器不支持我的 Flash 的型号呢？那就自己写个单片机程序把程序读出来吧。一般，在大学本科修读电子信息工程、通信工程或自动化专业的，有独立硬件项目开发经验的同学，都可以独立实现。

四 . 防护措施

介绍了这么多提取固件的工具和方法，那现在有哪些方法能有效防止产品固件被提取出来呢？

针对单片机固件提取的防护：我们可以通过编程的方式，把内部 Flash 区域设置为读保护状态，这样只要不对 MCU 进行解封，利用显微镜对内部 Flash 的电平状态进行破坏，是很难篡改固件的，至于读取固件，基本上不可能。例如，我们对 stm32 单片机的 RDP 寄存器进行设置，使内存保护等级提升至 level 2，或者把重要的程序和数据利用 PCROP 功能保护起来，防止读取。

对外挂的 Flash 内的固件，目前，就本人所知，只要能取下来，获得型号，就可以得到固件。那问题就变成了：如何不让攻击者把 Flash 安全的取下来？我建议硬件设计工程师把 PCB 上的 Flash 芯片，依靠电路设计保护起来。例如：设计 Flash 芯片在线检测电路，一旦 Flash 芯片的引脚出现断线，则立刻发动强电压攻击，将 Flash 芯片破坏，防止攻击者读取出 Flash 芯片中的固件。

五 . 总结

我们通过分析固件提取的原理，介绍固件提取可用的方法和工具以及相应的防护措施，希望可以使更多的电子工程师、嵌入式软件工程师重视智能设备固件的保护。同时，我们希望这篇文章可以给物联网安全从业人员带来一些物联网设备的防护建议。希望在智能设备开发工程师和安全测评工程师的共同努力下，我们身边的智能设备将越来越安全，企业的利益可以得到足够的保护。

参考资料

[1] cc2538 芯片资料：

http:/www.ti.com.cn/cn/lit/ds/symlink/cc2538.pdf

[2] stm32f103x8 芯片资料：

http://www.st.com/content/ccc/resource/technical/document/datasheet/33/d4/6f/1d/df/0b/4c/6d/CD00161566.pdf/files/CD00161566.pdf/jcr:content/translations/en.CD00161566.pdf

[3] Flash 编程器：

https://detail.tmall.com/item.htm?id=43496647283&ali_refid=a3_430583_1006:1109983619:N:%E7%BC%96%E7%A8%8B%E5%99%A8:eb3ec9d62bc0b3966ede063b9df1b415&ali_trackid=1_eb3ec9d62bc0b3966ede063b9df1b415&spm=a230r.1.14.1

[4] 新闻参考链接：

http://weibo.com/ttarticle/p/show?id=2309404160876054708433

智能硬件固件安全分析

TSG技术团队 李开

关键词：弱终端 固件安全 网络安全 防护方法 硬件安全

摘要：物联网设备存在许多的安全隐患，如何消除这些安全隐患呢？本文以弱设备为例，阐述如何对弱设备进行加固，着重介绍物联网弱设备存在的安全隐患和加固方法，以解决已经出现的安全隐患。希望可以对网络安全从业者和嵌入式工程师提供有价值的信息。

一 . 智能硬件的技术背景

1.1 智能产品与技术的发展

随着芯片、云计算、人工智能技术的发展，智能硬件如今发展也趋近于白热化。智能家居从 2013 年在国内火起来，当时 Zigbee 还算主流，广泛应用在各种传感器、报警器等设备上，这些设备配合 Zigbee 网关一起工作，还可以实现联动控制、远程报警。而当时也比较流行的网络摄像头 (IPC) 由于对带宽要求高，只能有线网或者通过 Wi-Fi 接入，实现了远程监控、入侵报警等功能，在当时，IPC 称得上是智能家居中相对比较复杂的产品了。那个时候国外也有很多智能家居的厂商，推出了很多成熟的智能家居方案，不过很多是基于有线的连接方式，如比较有名的 Control4 公司。

后来到 2015 年，随着 Wi-Fi 芯片的成本大幅降低，以及路由器的性能不断提升，Wi-Fi 的应用越来越广泛，由于不需要额外的网关，直接通过接入路由器可以连到云端，一时间涌现了大量的 Wi-Fi 接入的智能硬件，如家电、插座、灯泡等。国内的家电厂商如海尔推出 U-home，美的推出 M-Smart，同时国内的各大互联网厂商也推出了自己的物联网云平台，如阿里、腾讯、小米等，另外各种电商也基于自己的产品销售优势，推出自己的云平台，如京东、苏宁、国美等，设备和终端制造厂商华为也推出自己的物联网平台。所有设备基本都是通过 Wi-Fi 直连云，但是由于考虑到产品的成本问题，很多厂商直接使用的通用低端的 Wi-Fi 模组，如一直都很火的高通 (收购的 Atheros)，还有美满电子 (Marvell，如今已经退出 IOT 市

场），台湾的瑞昱 (Realtek) 和联发科 (MediaTek, MTK) 等，而高端的 Wi-Fi 模组一般用于对带宽比较高的运行 Linux 或者 Android 系统的产品。

国内 AI 技术是从 16 年慢慢步入消费市场，开始京东基于全志 (Allwinner) 的 R16 芯片推出了第一代的叮咚音响，采用科大讯飞的环形麦克风阵列技术，可以进行准确的远场音源定位和语音识别，后端的自然语言处理 (NLP) 也能够很大程度理解人的意思，并且进行比较有效的交互。而后智能机器人行业也发展了起来，如 Rokid 的第一代带投影的机器人，roobo 公司的布丁机器人等，都加载了语音和图像方面的识别技术。而国外的亚马逊 (Amazon)，早就通过一款名叫 Echo 的智能音响，闻名遐迩，它也是国外最早一批大力投入人工智能研究的公司之一。

如今的智能硬件，渗透到生活的方方面面，物联网安全，也成为了行业关注的焦点。

1.2 产品的固件及系统分析

不同的产品由于功能与成本的要求，会选择不同的芯片和系统，一般对于成本低功能单一的产品来说，基本都是不用操作系统的（行业内称之为裸奔）；而需要运行一些协议栈，就会用到一些简单的 OS；对于功能复杂的系统来说，一般都需要运行 Linux 乃至 Android 系统（以前工业界 Wince 应用比较广泛，但是现在也慢慢淘汰了）。以下是几种 OS 的对比，如：表 1.1。

表 1.1 中列出的 FreeRTOS、ThreadX、MbedOS 是实时操作系统，能够快速响应中断并及时处理，适用于对实时性要求比较高的控制系统，当然很多控制系统也会选择“裸奔”的方式，这样实时性更高，对 flash 和 ram 使用量也更低。而 Linux 和 Android 系统都称为非实时操作系统，它们对中断的响应没有那么及时，适用于对业务逻辑要求比较高的场合（因为这种芯片的计算和处理能力都非常强）。

系统种类	用途	产品	说明
无 OS	低成本 MCU	传感器，红外，SubG	功能简单，成本最低
类 OS	低成本 MCU，需要运行特定协议栈，低功耗	BLE，Zigbee 等	不算完整意义的 OS，但是也提供信号量、锁、队列等功能
FreeRTOS	功能相对复杂的系统，需要运行一些协议栈等	WIFI 模组	开源免费，使用非常广泛
ThreadX	同上	同上	非免费，某些芯片厂商使用
MbedOS	Iot，低功耗	穿戴式、物联网产品	开源免费，发展比较快
Linux	复杂的功能和任务调度	穿戴式、物联网产品	工具多，开发容易，资源丰富
Android	带高端显示、触摸功能	需要与用户进行强交互的产品	开发更容易（可以用 java），调试方便，但是成本比较高

表 1.1 几种不同 OS 的对比

在芯片行业，基本不同的芯片厂家针对于自己的 MCU 或者 CPU，都适配了有一些 OS（当然对于开源的 OS，用户一般也可以自己进行移植），对于 MCU 来说，根据需求可以选择是否运行 OS，

而对于高端一些的 CPU，绝大部分都会适配 Linux 甚至 Android 系统，用户可以基于芯片厂家提供的 SDK 可以进行快速的开发。

1.3 智能硬件的文件系统

由于大部分的 MCU 的内部 flash 都比较小(一般都在 1M 以内)，很少有内部 flash 里面加载文件系统的情形，文件系统用得最多的就是在外部的 TF 卡或者 SD 卡里面，用来保存一些音视频文件等，就算应用比较多的外部 SPI flash 一般也不会去存储文件系统。

而对于 Linux 和 Android 系统，文件系统是必须得存在，如 SPI flash 里面用得比较多的 squash、jffs2 等，还有 Nand Flash 和 Emmc 里面用得比较多的 ubifs、yaffs2 等。当 Linux Kernel 启动完毕，就需要挂载 rootfs，然后不同的设计可能还需要通过直接挂载或者以 overlay 的方式挂载其他的一些分区，所以在一个固件里面，存在一个或者多个文件系统。

二 .Refirm Labs 报告详解

Refirm Labs 是一家专注物联网安全公司，他们开发的 Centrifuge Platform 平台，是全球首创自动化检测固件漏洞的平台，用户上传固件后，该平台能够自动分析固件中的漏洞，弱口令、缓存溢出等问题，并在半个小时内给出分析结果。

如图 2.1，是一个网络摄像头的固件分析后得到的分析结果，里面给出了固件大小以及解析出来的文件系统的大小，统计了里面的文件个数和可执行文件的个数，另外，对文件系统里面的秘钥、密码哈希、弱加密算法、带有安全隐患的可执行文件的数量都做了统计。

进去每一项分析，可以提供更加详细的分析报告，比如每一个

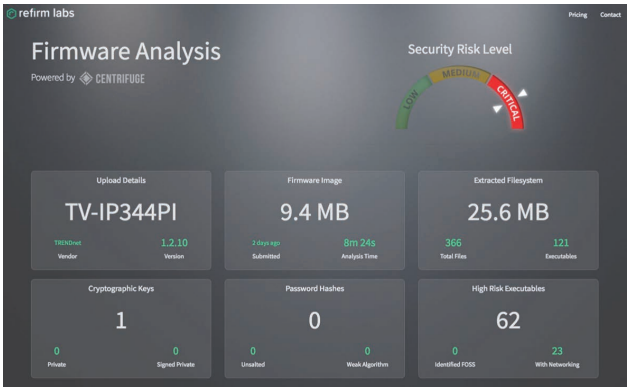


图 2.1Refirm Labs 的一个报告页面

可执行文件里面会缓存溢出危险的个数、命令注入危险的个数、网络调用次数等，如图 2.2 所示。

另外，除了固件分析之外，Refirm Labs 还可以对实际产品进行测试和分析，当然这个不算对固件进行直接的分析，而是分析运行该固件的产品，可以称这种方式为在线分析，而仅仅分析固件文件的方式称为离线分析。

离线分析，只是为了在最短的时间，给出大致的分析结果，从 Refirm Labs 的报告看出，危险指数第二是 wpa_supplicant，这个已经非常成熟并且应用特别广泛的开源 Wi-Fi 管理程序，里面的安全问题应该相对比较少，所以通过这种结果来看，Refirm Labs 的报告仅仅只能参考，或者说，这种逆向分析可执行文件的方式还远远不够智能，以后也还有相当远的路要走。

另外，Refirm Labs 的这种分析机制，也仅仅针对于 Linux 或者

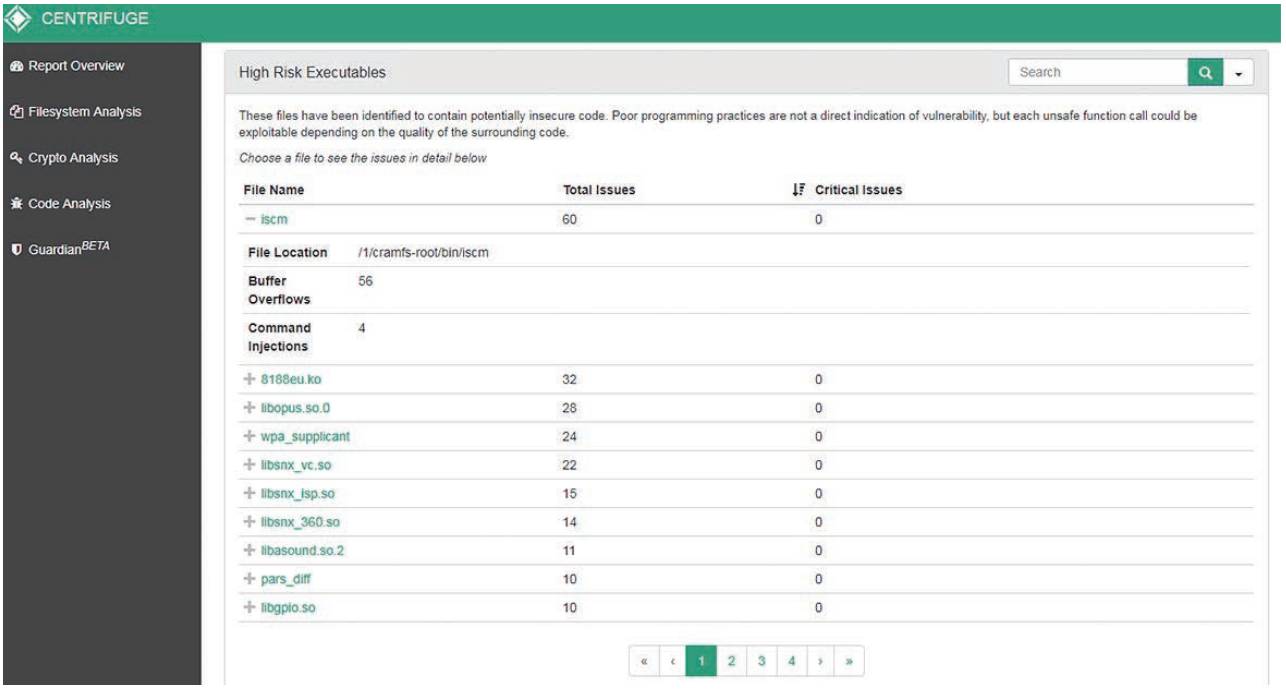


图 2.2 可执行文件的详细结果

Android 这种带文件系统的固件有效，所有的后续分析，全部都依赖于解析出来的文件系统，而对于一些低端的 MCU 固件，无法解析出里面的文件，所以也无法分析出结果。

三 . 分析策略研究

以下从几个方面分别阐述一下固件分析涉及到的技术和方法。

3.1 文件系统提取

分析的第一步，就是需要从固件里面提取可能存在的文件系统。

Refirm Labs 在 github 上面开源了他们的一套固件分析的程序 “binwalk”，这个是用 python 写的一个在 bin 文件中去搜索文件系统或者一些特定文件（如 Linux 内核，压缩文件等）的工具，还可以把搜索到的文件系统解压出来，供用户进行二次分析，而该工具的搜索方式，就是通过匹配一些特定的文件头或者 Magic 数据，来遍历整个 bin 文件。不过 binwalk 也有自己的局限性，比如不支持 Nand Flash 里面的 ECC（Error Checking and Correction），因为 Nand

Flash 或多或少都有一些坏块，数据写入后会进行校验，校验不通过，程序会标记这个坏块，导致写到 Nand Flash 里面的数据的分布，可能与实际的固件有比较大出入，而如果我们从一个产品的 Nand Flash 把里面固件读取出来，通过 binwalk，很大几率提取不出来里面的文件系统。而对于实际烧写的固件文件，binwalk 都能够比较好地分析出结果。

3.2 文件分析

由于 Linux 系统对于可执行文件或者动态链接库等，都是采用的 ELF 文件格式，所以解压出文件系统后，可以通过 readelf 命令去获取每一个 ELF 文件的头部信息，可以获取文件的类型、外部依赖、处理器等各种信息，而如果仅仅是通过文件后缀判断文件类型的方式，往往会带来很多误判或者漏判（例如通过后缀中是否带有 .so 来判断是否是动态链接库）。同时，如果想获取文件中的一些常量，可以通过 strings 工具来分析。另外，如果需要进行更深入的分析，则需要通过 IDA 来对文件进行反编译，利用汇编指令和调度流程来分析具体的一些数据，如特定函数调用次数，或者在 strcpy 之前有没有对参数进行 strlen 判断字符串长度等。

3.3 依赖库分析

Linux 环境下很多开源的依赖库，从诞生到如今，各种依赖库也在不断迭代更新，包括添加新功能、修复以往版本的 bug。所以可能某些老版本的依赖库或者工具存在一些已知的漏洞，但是由于厂家使用的 SDK 比较老，里面的一些工具没有及时升级，导致开发出来的很多应用，间接也具有这些漏洞，让黑客有机可乘，特别是一些 web 服务相关的依赖库，一旦出问题，就会带来非常严重的后果。

所以对于依赖库的分析，需要大量的积累，比如搭建一套数据库，对于各种开源的代码和工具，进行版本管理和统计，针对于不同版本存在的已知问题都进行标注，分析固件文件的时候，依次进行对比，分析出一个可执行程序所依赖的所有动态链接库的安全性，并进行打分，评判出可执行程序的安全性。

3.4 秘钥与加密算法分析

一般秘钥存储都是以文件形式存在，像 RSA 的公钥（PEM 格式存储），或者 X509 的证书之类的，然后有些应用把公钥写到代码里面（转化成 DER 格式），这种就比较难分析出来。秘钥或证书可以通过特定的正则表达式去文件里面搜索，如果匹配到比如 “---BEGIN XXXX---” 和 “---END XXX---” 这种字符串，就认为是秘钥文件。

嵌入式系统中，大部分情况都会调用通用的加密库，如 openSSL、wolfSSL 等，如果可执行文件是动态链接到这些加密库，可以通过 ELF 信息来获取该程序调用了哪些加密算法，但是如果是静态链接，并且对文件进行了 strip 操作（基本大部分产品出厂都会对文件执行 strip 操作），那么就很难知道该程序调用了哪些加密算法，除非通过反编译去分析指令，但是这种方式比较复杂，可靠性不高。一些大公司对产品加密要求比较高，通常会采取静态编译的方式，把所有的算法集成到可执行文件中，所以这种时候逆向分析就比较困难。如果一个应用通过动态链接，调用了一些弱加密算法，那么很容易通过 ELF 发现。

四 . 实战分析

笔者在网上下载了某公司网络摄像头的 OTA 固件进行了几个简单的分析，以下是分析的过程和对应的分析结果。

1. 分析固件中文件系统

方法：通过 binwalk 分析固件里面的文件系统

结果：发现该固件中包含一个文件系统，ubi 格式，固件大小是 33M，解包出来的文件系统一共是 63M，解出来的系统比固件大得多的原因是 ubi 文件系统进行了文件压缩。

2. 查找文件系统中可执行文件数量和动态链接库的数量

方法：通过 readelf 去遍历文件系统的每一个文件，如果 Type 是 EXEC，那么这个文件就是可执行文件，如果 Type 是 DYN，那么就是动态链接库，这样可以过滤掉动态链接库的软连接

结果：系统中一共发现 46 个可执行文件，11 个动态链接库，其中芯片 CPU 是 ARM v7-a，使用的是 Thumb-2 指令集，同时该 CPU 还有浮点计算单元 FPU（Float Processing Unit），还支持 NEON 技术。

3. 分析可执行文件的网络行为和缓存溢出危险

方法：通过 readelf 工具去分析每个可执行文件的外部符号表（包括所依赖的第三方动态链接库），如果有 socket、send、recv、sendto、recvfrom 这种调用，就认为该执行文件有网络操作行为；如果有 sprintf、strcpy 等函数调用，就认为该文件具有缓存溢出的风险

结果：一共发现有 13 个可执行程序具有网络操作，30 个可执行程序有缓存溢出风险。

4. 分析可执行文件中的常量

方法：通过 strings 工具去扫描文件中的数据区域的常量，然后在结果中去搜索如 “admin”、“123456” 这种可能是固定账号和密码的字符串

结果：一共发现有 2 个可执行程序的数据区域包含这种常量，虽然不敢确定这种是否是我们需要的账号或密码。

5. 分析文件系统的秘钥数量

方法: 利用正则表达式“-----BEGIN ([A-Z]* (PRIVATE|PUBLIC) KEY|CERTIFICATE)-----” 去文件中 grep 对应的字符串

结果：发现文件系统中一共有两个文件保存了 2 个证书文件。

6. 分析结果总结

笔者用了比较基础的方法，简单分析了一个固件的内容，还有很多需要进一步分析的内容，比如查找各种动态链接库对应版本的安全问题，当然这都需要足够的时间积累，还可以利用 IDA 工具去分析一些厂家的业务程序的流程逻辑等。不过所有的分析都是静态分析，并不能完全反应固件的问题，真正的问题还需要将固件升级到产品里面，针对产品的各方面进行在线手工分析。

五 . 小结

固件分析，只能作为研究智能硬件安全的第一步，可以通过这种方式快速发现一些潜在的问题，但却无法覆盖所有的问题。

也许，安全这条路上，没有捷径可以走，必须得有足够的技术底蕴，才能把一个产品的各种问题分析透彻。

物联网安全解决方案

解决方案中心 刘弘利

关键词：物联网 安全体系 漏洞与威胁管理 安全准入 安全可视

摘要：物联网在感知设备和通讯协议两个方面快速发展，在智慧城市和数字工业等领域开始应用，这带来了新的安全挑战。绿盟科技物联网安全解决方案，以层次化分析物联网安全体系，提出安全威胁检测，漏洞扫描，物联网资产和风险可视化的解决方案。

一．物联网应用和安全威胁

1.1 物联网应用

物联网 (Internet of Things) 是一个基于互联网、传统电信网等信息承载体，让所有能够被独立寻址的普通物理对象实现互联互通的网络。

在“互联网 +”时代，物联网发展迅猛，正加速渗透到生产、消费和社会管理等各领域，物联网设备规模呈现爆发性增长趋势，万物互联时代正在到来。根据咨询机构 Gartner 报告，2015 年物联网设备只有 29 亿，而 2020 年将会达到 204 亿。

物联网应用广泛分布在各行各业。智慧城市、智慧家庭、智能交通、智能物流，都是由物联网相关应用来支撑。随着不同类型的感测设备面世，会有越来越多的物联网应用出现。城市共享单车是最大的单品物联网应用，每个单车配备的物联网锁，通过手机扫描二维码实现远程解锁，车辆骑乘中，进行卫星定位。

物联网应用

物联网给我们的工作和生活带来便捷的同时，也引入了风险。其中，最为著名的案例是 Mirai 僵尸网络。数十万的摄像头被入侵，2016 年底对美国域名服务商 Dyn 发动 DDoS 攻击，造成众多知名网站无法打开的后果，影响深远。

物联网的多源异构性、开放性、泛在性使其面临巨大的安全威胁。

相比于 PC 互联网和移动互联网，物联网覆盖领域广泛，接入设备数量大，应用地域和设备供应商标准分散，物联网时代的应用多样性和复杂性远超互联网。

物联网安全风险，保留了互联网的安全风险，增加了由感知设备带来的新的风险。与信息安全领域威胁不同的是，物联网是与实际物体产生关联的，如果物联网安全受到威胁，损失的可能不仅仅是信息资料，更有可能影响到人身安全或者生产设备运行安全。

1.2 物联网安全威胁

典型的物联网架构，一般是由感知层、平台层和应用层三层架构组成。其中感知层是各种传感器，负责感测数据，并回传到平台层，进行数据存储和分析处理，然后在应用层进行呈现。应用层还可以向感知层发送信息和指令，控制感知层设备的感测行为。

物联网三层架构之间，数据通过网络进行流通。物联网和互联网的区别，在于感知设备庞杂，物联网规模更大，更复杂。此外，云计算、大数据、机器学习、区块链等技术的演进，也和物联网相结合，一方面带来更广泛，更准确，更快捷的技术应用，另一方面，也引入了相关的安全风险。

物联网层次	安全威胁	描述
物联网感知层	设备仿冒	攻击者通过利用物联网终端的安全漏洞，获得节点的身份和密码信息，假冒身份与其他节点进行通信，进行非法的行为或恶意的攻击，如监听用户信息、发布虚假信息、置换设备。
	设备入侵	物联网感知设备存在漏洞，或者使用缺省密码，被攻击者控制，或者安装恶意代码，成为僵尸主机。
	隐私数据泄漏	被入侵后，攻击者窃取感知设备的信息。
物联网平台层	平台入侵	物联网应用系统平台本身的漏洞，例如云平台的漏洞、大数据平台的漏洞等导致平台被非法攻击和利用。物联网平台会采用很多的组件，操作系统、平台组件和服务程序自身漏洞和设计缺陷易导致未授权的访问、数据破坏和泄露。数据结构的复杂性将带来数据处理和融合的安全风险，存在破坏数据融合的攻击、篡改数据的重编程攻击、错乱定位服务的攻击、破坏隐藏位置目标攻击等。
	数据窃取和篡改	平台入侵后，攻击者可以窃取、篡改、删除数据。物联网平台层是感知层的数据汇聚节点，影响整个物联网应用。
	APT 威胁	高级持续性威胁，攻击者利用零日漏洞等高级攻击，持续不停的对平台系统攻击。

物联网层次	安全威胁	描述
物联网应用层	业务中断	攻击导致应用程序无法与平台通讯，获取感知数据失败，无法与感知设备交互。
	间谍软件	应用程序所在的主机或者移动设备安装了间谍软件，窃取物联网数据。
	勒索软件	应用程序所在的主机或者移动设备安装了勒索软件，磁盘数据被加密，无法与物联网应用交互。
物联网网络层	网络嗅探	感知层接入网络到平台层，平台层与应用层之间的网络连接，存在明文传输网络嗅探的威胁。
	信息篡改	攻击者嗅探后对，更改数据，后台接收到的是被篡改的。

二 . 物联网安全防护体系

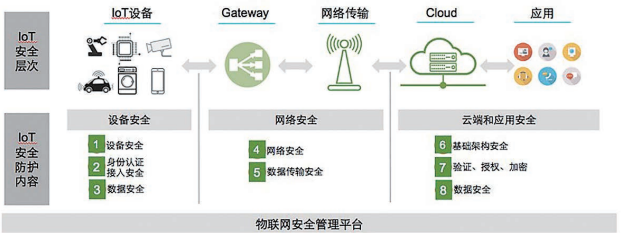
从物联网的威胁来看，物联网时代安全风险无处不在，大到系统平台，小到传感器，任何一处风险都有可能使威胁扩散到整个网络与核心系统。

物联网所对应的传感网的数量和终端物体的规模是单个传感网所无法相比的，物联网所联接的终端设备或器件的处理能力将有很大差异。加上物联网所处理的数据量将比现在的互联网和移动网都大得多，已有的对传感网、互联网、移动网、安全多方计算、云计算等的一些安全解决方案在物联网环境中可以部分使用，但另外部分可能不再适用。

鉴于以上原因，对物联网的发展需要重新规划并制定可持续发展的安全架构，使物联网在发展和应用过程中，与之相匹配的安全防护措施能够不断完善。

2.1 物联网安全体系

物联网安全解决方案的框架，包括感知层安全、网络层安全、平台层和应用层安全、以及物联网安全管理平台组成。与物联网的各个层次的安全威胁相对应，每一层面都有响应的安全措施来保障安全。下图是整体安全防护内容。

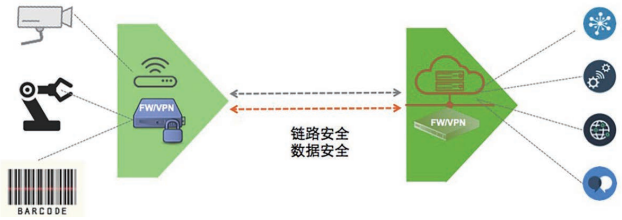


2.2 感知层安全防护

物联网感知节点的安全，对于智能设备，有操作系统，可以通过安装保护模块 SDK 入侵检测和防护，避免蠕虫感染。非智能设备，只能通过接入网关，在网络层面防护。智能设备还可以设置认证方式，对其身份验证实现准入控制。

2.3 网络层安全防护

网络安全防范网络嗅探和数据篡改。采用加密传输比如 VPN 隧

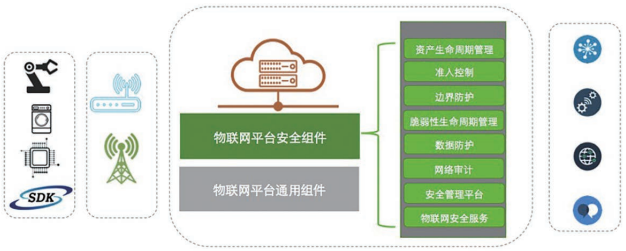


道保护数据的完整性。

2.4 平台与应用层安全防护

物联网平台提供计算和存储服务支撑其应用需求，对物联网终端所收集的数据信息进行综合、整理、分析、反馈等操作，主要提供海量终端的管理、数据管理、运营管理和安全的管理。

平台和应用层和传统 IT 安全一样，考虑基础设施安全，虚拟化安全等防护措施。



三 · 物联网安全解决方案

3.1 安全防护

物联网设备，尤其是具有 IP 能力的智能设备，如摄像头等设备，在接入层的准入控制是基安全需求。物联网前端设备大量而分散，部署在街道室外环境，无人值守，容易被黑客利用，接入视频专网，进而渗透到整个网络，导致核心业务系统被入侵、视频资料被删除、敏感信息被窃取等风险。物联网设备安全，首先要以身份认证等手段建立资产接入管控机制，其次要对网络入侵，蠕虫感染进行防护。

终端识别

物联网设备的准确识别是准入控制技术的前提。传统主机终端设备，可以安装客户端主动识别，并检查主机自身的安全性；但是物联网嵌入式操作系统，如摄像头终端设备，路由器网络设备，无法安装客户端软件，就需要识别其硬件编码，网络地址，特征指纹等信息，确定是否为授权可接入设备。

终端识别还能为物联网管理平台提供资产可视化的能力。通过终端识别，管理平台可以发现和识别各种类型的物联网资产，根据资产类型，结合漏洞管理和外部威胁情报进行安全风险管理。

准入控制

物联网设备经过识别后，通过 MAC 地址、IP 地址、设备指纹等设备认证方式对网络接入设备进行管控，只有通过认证的设备才允许接入到网络中，防止前端设备的非法替换接入。

设备准入方式有多种方法。对于智能物联网设备，可通过认证授权方式，还可以对其运行环境进行合规性检查。对于非智能物联网设备，不能通过账号密码认证方式，可以采用 MAC 地址，IP 地址绑定，以及指纹识别的技术识别设备后，进行准入控制。

入侵防护

物联网设备需要限制访问控制，避免蠕虫自动扫描，以漏洞利用方式或者缺省密码方式感染。需要的主机设置访问控制列表，这是最基本功能，可以防范大部分的类似 “Mirai” 蠕虫感染。网络上利用漏洞方式尝试攻击渗透，需要入侵检测与防护模块。

感染节点防扩散

网关设备除了防范从外到内的扫描、入侵外，一旦物联网感知设备遭到入侵，还需要对其隔离，避免同网段的设备全部感染。

3.2 安全评估

物联网设备存在脆弱性，既有安全配置问题，如缺省密码问题，也有设备漏洞问题，如品牌的摄像头的 CVE 漏洞。定期或者实时进行利用脆弱性评估工具识别漏洞，并利用云端专业漏洞情报和资产暴露稽核能力，关联安全威胁与漏洞，实现物联网资产的安全风险全景视图。

漏洞识别

物联网设备脆弱性采集探针。包括专业的安全漏洞扫描探针、资产配置安全性检查探针等平台专用脆弱性数据采集探针，通过平台进行集中的调度和驱动。

威胁情报采集与关联

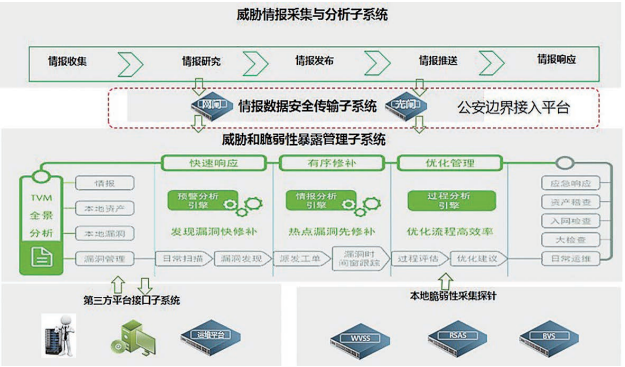
采用基于大数据架构的互联网情报智能收集与处理。威胁情报采集重点是将安全厂商、安全社区、行业共享和互联网搜集到的情报进行统一整合，并依据物联网内部资产特点，将相关的情报进行筛选后进行威胁关联分析。

互联网资产稽核

物联网资产与来自情报平台互联网上暴露的资产稽核、本地扫描探针引擎集中管理和脆弱性采集策略管控、脆弱性暴露可视化展现、漏洞及资产库管理支撑等功能。

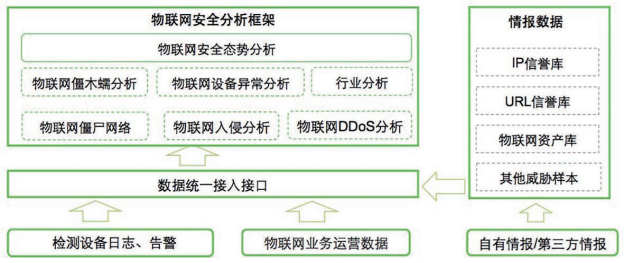
漏洞修复

漏洞修复包括脆弱性修复工单处理系统、弱口令自动化修复引擎、专家加固建议生成引擎等，通过对大面积重复性的加固修复工作以人工向自动化方式实现为目的，形成准自动化的全面脆弱性修复工作机制。



3.3 态势感知

“全天候全方位感知网络安全态势”是总书记对网络安全态势的要求，物联网安全也不例外。网络安全态势感知包括网络安全态势觉察、网络安全态势理解、网络安全态势投射层面，是对网络安全全景的完整认知。它不仅仅是将网络中的安全要素进行简单的汇总和叠加，而是根据不同的用户需求，以一系列具有理论支撑的模型为支持，找出这些安全要素之间的内在关系，实时地分析网络的安全



状况，并预测网络安全形势的演进，为网络拥有者提供相关安全维护和建设决策支持。

流量采集

通过全流量探针和高级威胁检测器，对网络出口流量进行双向解析，包括 4 层流量解析、应用层流量解析、文件解析等，并将原始流量 PCAP 文件、协议元数据、告警、日志等经过多维度解析的信息汇总至分析平台。

风险评估

通过主动探测方式及时获得网络上设备、系统和应用的运行状态以及资产信息，时刻知晓最新的安全防护范围，有效调整安全防护策略，更可以结合外部的威胁情报，完成对物联网设备、网络的安全分析，包括设备状态、漏洞风险评估、入侵检测、外发攻击检测等。

威胁检测

集合规则检测、智能引擎、沙箱检测、机器学习、情报关联等手段多措并举，集多种安全检测能力于一身，按需提供检测能力，并进一步实现对 APT 攻击的检测。

攻击溯源

以全流量解析数据为基础，进行基于时间、协议类型、告警、日志等数据的综合关联分析，形成基础攻击路径，再结合流量信息，补全并向前追溯，关联与告警威胁相关的流量信息，进而完整回放攻击场景。

关联分析

使用机器学习和数据挖掘技术，基于各种安全数据实现对网络行为、主机行为、应用行为的特征学习，通过大数据构建出网络环境中的各种行为模型，从而识别出正常和异常、趋势和对比等信息，实现自动学习、自动适应和自动规则生成，降低人员操作失误风险，提高安全响应速度。

联动防护

基于深度学习的专家分析和准确及时地威胁情报支持，将严重安全事件、高危安全威胁、重大损失等进行预判，通过安全通告、实时信息推送等方式提供安全警报，并提醒用户采取相应的防范应对措施。联合管理平台，对各种漏洞风险进行加固，对各种安全事件及时下发流控等防护策略。

可视化

物联网资产、漏洞、威胁组成整体安全态势，物理网业务系统安全风险情况，以可视化呈现出来。可视化仪表盘，显示物联网设备总数，存在漏洞和弱口令的终端，已经被黑客控制的物联网终端，严重威胁事件统计信息，威胁情报关联情况。在态势平台显示已经被攻陷的设备，需要管理员立即采取行动进行处置。

态势感知

采用安全模型和算法对多源异构数据从时间、空间、协议等多个方面进行关联和识别，通过大数据平台能力，对网络安全状况进行综合分析与评估，形成网络安全综合态势图，借助态势可以精确定位网络脆弱部位并进行威胁评估，发现潜在攻击、预测未知风险，提高全局网络安全防御能力和反击能力。

运营商物联网卡业务安全分析

创新中心 吴子建

简介

物联网卡指的是运营商用在物联网业务中的 SIM 卡。物联网卡的类型与功能如表 1 所示。

行业卡与普通手机用的 SIM 卡功能相同，因此可以直接放入手机中进行语音通话，发送短信或者上网。专网卡的语音，短信实行白名单管理，只能与已经注册的白名单号码进行通信，但是其上网的功能是开放的，因此专网卡可以被用来放在手机等终端中进行上网业务。

术语	定义
专网卡	一种应用于物联网业务中的 SIM 卡，具有专用号段。分为两种，13 位的号卡有短信和流量的功能，没有语音功能。11 位的号卡有短信，流量和语音的功能。
行业卡	一种应用于物联网业务中的 SIM 卡，号码为 11 位，与普通手机号码的号段相同，具有语音，流量和短信功能。

表 1 物联网卡的类型与功能

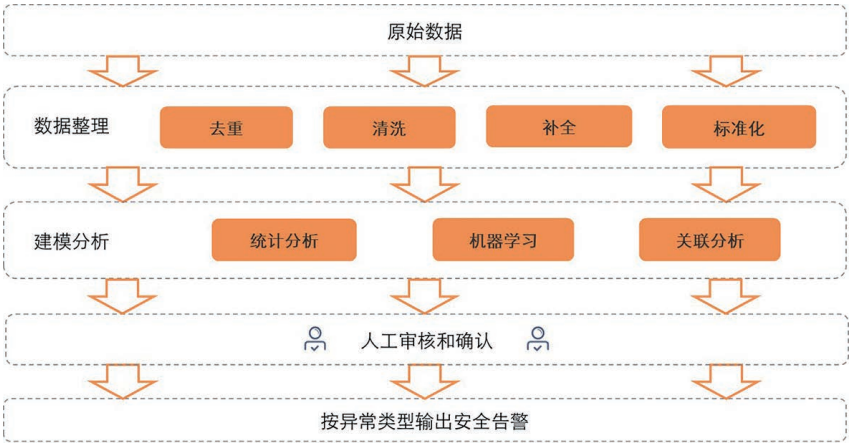


图 1 物联网卡异常分析流程

不同物联网业务对短信、话音、数据等基础功能需求存在差异。物联网卡在资费方面存在流量池计费、无漫游、资费较优惠等特点。这些卡在销售给客户后存在被异常使用的风险。例如物联网卡被用在个人手机业务中，享受更优惠的资费，或者被用来进行薅羊毛、电信诈骗等，即卡被滥用。另外，由于物联网卡一般不会与设备进行绑定，所以也会存在物联网卡实际应用的业务场景与合同约定的场景不同的情况，即卡被挪用。基于大数据分析和机器学习的方法可以有效的发现物联网卡业务数据的异常，进而发现被异常使用的卡。

物联网卡异常分析数据源

采集物联网卡的语音话单、短信话单、流量话单和上网日志数据，发卡与用卡单位相关信息，根据异常分析模型数据需求，从话单中提取出有效的关键数据特征，如通话信息、短信发送信息、上网行为信息等，用来分析物联卡的各类异常行为。

物联网卡异常分析方法

物联网卡的异常分析流程与方法如图 1 所示。

数据整理

对原始数据进行去重，清洗，补全，标准化等操作，将原始数据转化为结构化的数据。由于原始数据是无标签的数据，所以首先要对数据进行标签化处理，即给卡号打上所属行业的标签。采用层次聚类的方法对原始数据进行聚类，将聚类的结果经过人工打标签，即可以得到标签化的数据，为接下来的分析做准备。

建模分析

采用上文提到的统计分析，机器学习分析和关联分析的方法对数据进行建模分析，找出数据异常的卡，将这些卡标示为疑似异常，并给出异常的评分。具体的分析方法如下:

统计分析

对原始话单中的数据进行统计，例如统计每张卡的语音通话信息，发送短信的特征信息，以及上网行为信息等数据。由于物联网行业中的业务场景比较固定，所以卡的行为模式的统计特征也比较固定。如果出现偏离较大的统计特征，则卡可能存在被异常使用的情况。根据统计结果，结合专家知识，即可发现被异常使用的物联网卡。

机器学习分析

机器学习方法用来发现使用行为发生突变的物联网卡。基于卡的历史数据，通过聚类，分类等方式学习出卡的历史行为特征。基于历史行为特征对卡的当前行为进行检测。如果卡的当前行为特征发生突变，则卡可能存在被异常使用的情况。例如可以通过卡的特征数据和行业标签来训练行业识别分类器，用训练好的分类器对待检测卡的数据进行检测。如果分类器给出的行业场景与数据标签中的行业场景不匹配，则卡可能存在被异常使用的情况。

关联分析

统计分析和机器学习分析主要是针对数据的部分维度进行分析。而在实际的业务场景中，物联网卡被异常使用以后，其行为模式会存在多个维度的异常。将多个维度进行关联分析可以大幅度提高异常检测的准确度。

调查验证

数据分析方法可以给出疑似有异常的卡的列表。而卡是否确实存在被异常使用的情况需要进一步由人工进行调查确认。调查方法为将疑似有问题的卡号下发到发卡的分公司，由分公司找到用卡单位，将疑似异常的卡目前的应用场景与发卡合同中规定的应用范围进行比对，以确认卡是否存在被异常使用的情况。

分析与调查结果

通过对物联网卡的相关数据进行分析，并结合人工调查的结果，得出物联网卡主要存在以下几种异常使用的情况：

挪用异常

物联网卡被应用的场景发生了变化。例如原来被用在电梯卫士中的 SIM 卡被用在了车务通中。由于物联网卡的发卡合同规定不允许私自变更卡所应用的物联网业务，因此这种情况属于异常使用。

滥用异常

物联网卡只能应用在物联网业务中，不能应用在个人业务中。在实际的分析与调查中发现有些卡被用在了个人的手机中，这种情况属于卡被滥用的情况。另外还发现一部分卡被用来发送垃圾短信，这部分卡已经被关停。

合同及管理异常

在实际调查中发现，有很多的卡虽然在数据分析的结果中被认为是异常，但实际上这种异常并非由于卡被异常使用所引起，而是由于在管理中的疏忽所导致。例如有些卡存在个人业务的行为特征，而实际调查中发现这些卡本身就是已经实名制的个人手机卡，但卡的相关信息却出现在了物联网卡的数据集合中。这种情况一般是由于卡在被管理的过程中出现差错导致的，而卡本身并不存在被异常使用的情况。另外还有一种情况是物联网卡的发卡合同中只规定了卡所对应的收费套餐，而没有规定卡所应用的行业场景。这种情况也属于对卡的管理存在漏洞导致的异常，而不是卡本身存在被异常使用的情况。

通过大数据分析和机器学习的方法对物联网卡的使用行为进行分析可以有效发现卡被异常使用的情况，为运营商物联网卡的业务安全提供有力的支撑。

物联网设备准入控制实践篇

解决方案中心 张良玉

背景

近年来，物联网已被各国政府机构视为拉动经济复苏的重要动力，但安全问题成为了物联网发展的重大障碍。在物联网安全事故中，受伤最大的莫过于智能摄像头和路由器。

摄像头安全事件，如“红遍全球”的恶意软件 Mirai，它通过控制大量路由器、网络监控摄像头、DVRs、Linux 服务器以及运行有 Busybox 的 IOT 设备，使用默认密码进行登陆，一旦登陆成功，这些 IOT 设备就成为被黑客操控用于攻击其他网络设备的工具。

2016 年，德国 1127 断网事件，90 万家用路由器受攻击导致 2000 万固定用户断网后，德国电信分析确认因为家用路由器管理后台暴露，从而导致路由器受黑客控制。

从国家政策来看，国务院发布了《中国制造 2025》战略文件，其中强调工业物联网系统的安全技术也是物联网安全领域重要组成；“十二五”期间，科技部设立了国家 863 项目“物联网安全感知关键技术及仿真验证平台”；物联网安全为 2018 年科技部网络空间安全重大专项第一课题。

那么，在万物互联的网络中，IOT 资产以及业务应用又面临哪些安全风险以及对应的应对措施又如何？

安全风险及应对

目前针对物联网安全防护的解决方案中，主要还是从物联网设备准入方面入手，通过安全准入网关和监控平台来保障物联网安全。物联设备准入方面，主要的风险及应对主要有：

安全风险类型	安全问题	应对措施
设备接入安全	未授权的终端接入	终端准入控制 通过指纹精确识别终端，进行身份认证
	私接 / 共享设备	
	设备伪冒替换	
	设备恶意篡改	
终端状态安全	终端系统漏洞	设备系统版本、补丁识别和监控对开放端口、服务进行控制 应用加固
	设置不合规	
	系统补丁未安装	
	杀软未安装	
	非法软件安装	
	非法外连设备	
用户认证安全	用户越权访问	用户、角色、终端分离与绑定 用户 / 终端行为记录
	用户角色混乱	
	用户仿冒	
	认证信息追溯	
业务 / 资产安全	设备（受控）攻击物联业务	流量监控、应用识别，检测攻击行为 & 可疑事件
	设备（受控）攻击网络业务	
	设备（受控）攻击物联设备	
	外部网络攻击物联设备	

针对“设备接入安全”、“终端状态安全”以及“用户认证安全”等几方面的风险，可以通过物联网准入控制产品应对。通过对几款准入控制的产品的实践与分析，梳理了几点关键技术。

准入控制的关键技术

部署方式

由于客户实际网络环境可能是固定或者全新环境，出于对终端安全接入的安全考虑，重点关注安全准入设备的网络适应性、兼容性、安全性、故障紧急处置效率这几个方面的考虑。安全准入设备常见的主流部署包含 DHCP、旁路等，具体见下表：

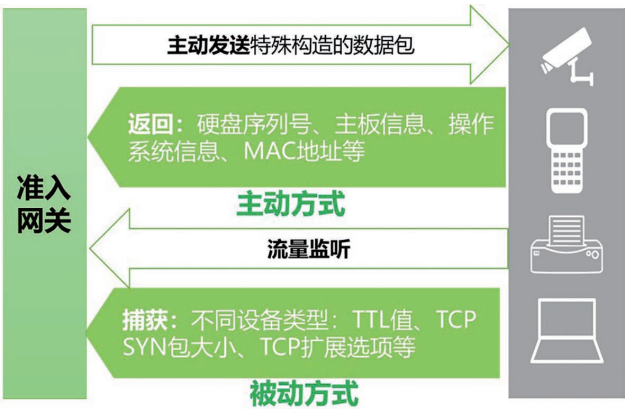
部署类型	具体描述	优劣分析
DHCP	DHCP 准入控制，适应于 2 层的网络环境，实现方式在用户进入网络之后，获取到一个隔离网段 IP 地址，通过用户认证、安全检查之后，才会分配到一个正常准入网络的 DHCP 地址。	这个场景下很好的保证了 DHCP 的安全性。
旁路镜像	旁路镜像是不会改变当前的网络环境，主要是旁挂核心交换机上，对网络改动最小，主要是通过把用户镜像到准入设备上，NAC 设备会用户发送用户认证 portal 页面，进行用户认证以及安全检查，检查之后才能够正常访问网络。	比较常见，对用户现有部署影响较小。
透明网桥	二层串联到网络，不需要对用户网络做较大改动。	容易成为单点故障

部署类型	具体描述	优劣分析
802.1x	801.x 适用于 2 层网络，是对局域网内部的设备进行身份认证。802.1x 协议采用典型的 C/S 体系架构，主要分为三部分：认证客户端、认证系统、认证服务器。	这个方案部署起来比较麻烦，需要设置客户的网络连接或第三方的认证客户端，可能与 AD 域认证等会有一定的冲突。
ARP	ARP 准入技术就通过准入设备 NAC 发送免费的 arp 报文，对未经过认证的用户进行网关欺骗，引导用户进行用户认证以及安检；适用于二层网络环境下。	如果客户端安装防 arp 防火墙就会导致 arp 准入失效的情况。
MVG/SVB	MVG/SVB 技术是国内准入厂商的私有技术，基于 cisco 的 BVI 技术的延伸，适用于二层网络环境下，通过 BVI 的思想，在用户认证通过后，进行 Vlan 标签的替换，这样能够更好的对用户进行安全隔离。	各厂商的私有技术

在考虑到对现有网络的影响、故障紧急处置效率、网络安全三个方面的考量，实际部署时多采用 DHCP 和旁路镜像两种部署模式，其中 DHCP 可以更好的保证自动接入物联网络环境的网络准入安全，旁路镜像方式则不会对现有的网络有任何影响，即使出现网络故障也不影响网络访问。

指纹识别

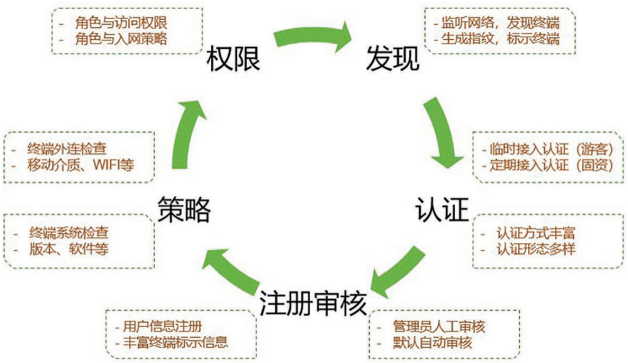
在万物互联的网络环境，各种不同类型的设备都可能进入网络，安全防护的基础应该是众多物联设备的准确识别与发现，目前主流的识别技术指纹识别。通过被动识别和主动扫描等多种方式结合，准确识别设备品牌 / 型号、系统版本 / 协议、以及对应应用和服务，进一步形成设备特征指纹，可以达到防篡改防伪造的效果。



身份认证

终端的网络行为判定会直接影响整个物联网络的门户安全，因此对终端资产的身份验证变得尤其重要。当通过唯一指纹标示终端资产的唯一性，同时基于终端资产指纹以及终端位置等信息，识别并建立不同的终端角色划分和网络准入策略，实现终端准入控制的安全闭环，极大地保证整个物联网络的安全。

通过实践，我们针对终端准入聚焦在身份认证，梳理了闭环处理流程（见下图）。按照物联终端的发现、认证、注册与审核、准入控制策略以及入网权限划分的闭环流程，针对每个环节作合规处置，保证准入控制的安全闭环。



该闭环流程为一个完整的准入控制流程，基于终端类型以及实际网络环境的特殊化，部分环节是可选的，例如摄像头，一般不需要用户认证和权限控制，重点可能在于系统版本以及漏洞的检查等，这样可以灵活实现定制化闭环流程处理。

实践分享

在内部实践过程中，我们基于物联网络的部署场景，设计内部实践环境（下图部署拓扑），对物联终端的准入控制进行了详细且细致的测试和实践。

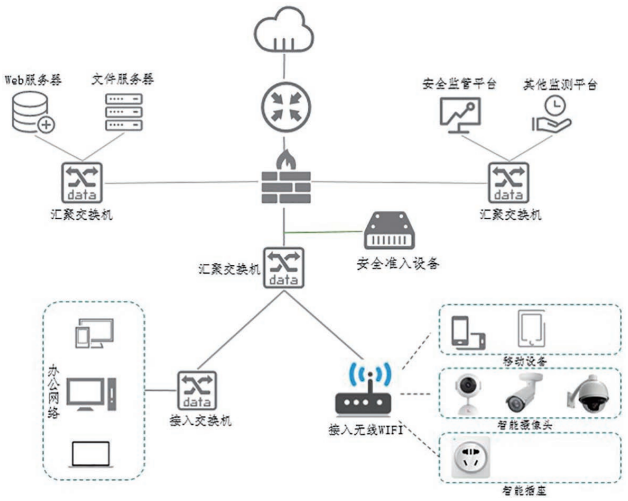
对于实践案例，我们从两个维度对物联设备的接入进行验证：

有线终端

有线终端涉及台式电脑、笔记本电脑、交换机、路由器及其他我司安全设备，安全准入设备可识别器网络信息、终端系统信息等。

无线终端

无线终端主要通过无线 Wi-Fi 接入，对手机 /iPad、智能摄像头、



智能插座的接入和控制进行实践，其中智能摄像头可识别其厂商（包含海康威视、萤石、大华、汉高邦科等）、Mac 地址并对其做准入控制。

总结

随着网络应用的普及、云计算的广泛运用以及物联网的快速发展，网络准入控制作为第一道进入网络的防护门变得越来越重要。网络准入控制对识别网络环境的资产及其合法性能够及时发现风险并对网络环境的安全保驾护航。此外，其也可以做一个探针，接入到大数据平台，同时结合威胁情报报，分析物联网整体的安全风险。网络准入设备，尤其在物联网络中的运用在当前及未来将会发挥其重要价值，为物联网络安全状态分析提供其底层资产识别和控制能力。

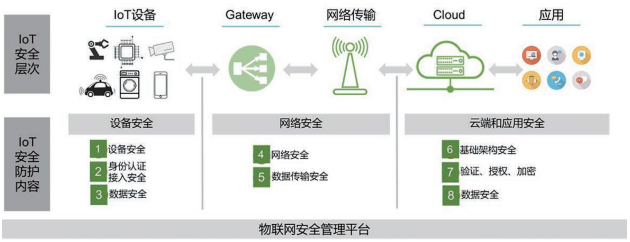
智慧城市中的物联网安全

徐翀

智慧城市，物联网是两个谈论了五六年的话题，它们二者之间到底是什么样的关系呢？如果我们尽量用一句话来概括什么是智慧城市应用的话，那就是：智慧城市应用是采集了关于城市的海量数据后，根据城市管理需求进行大数据分析，建立模型，并提供相应的智能化城市服务。

这一定义虽然不能说是最精确的，但基本涵盖了智慧城市应用的主要部分：数据采集，数据分析，依从城市管理原则，建立算法模型，提供城市级别服务。因此，数据采集就是智慧城市所有应用的基础。在数据采集来源上，智慧城市所需的所有数据只来源于两个方面：人和机器。而机器数据的采集，就是由物联网设备完成的。这些物联网设备遍布于城市各个角落，有摄像头，有地磁感应器，有气象传感设备，也有智能电表水表等入户采集设备。在智慧城市的架构中，物联网担负着数据采集的功能。因此，上传数据准确与否直接关系到智慧应用的可用性。由此可见，智慧城市中的物联网安全需求，也将会主要集中在感知层与传送层这两个层面，以确保数据准确上传，同时避免通过物联网设备数据通道对智慧城市的大数据中心进行攻击。

在智慧城市大框架下讨论物联网安全问题，其实主要需要了解的就是其与常规物联网安全、网络安全的异同。在本文中，由于篇幅的限制，我们仅仅讨论城域物联网安全的独特需求。



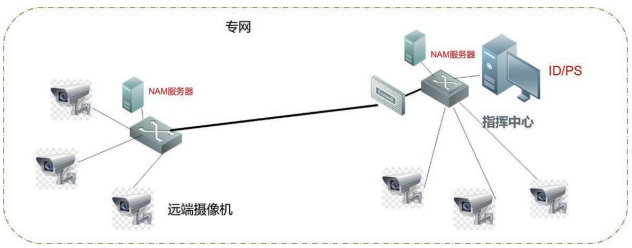
物联网安全管理体系

不同于采用 Bigzee/ 蓝牙 /Wi-Fi 等采用短距离接入手段的智能家居物联网或室内物联网，城市物联网的特点为设备分布广，设备间距大，且数目庞大。因此贴近设备部署具有加解密功能的网关设

备是不现实的。在城域物联网条件下，设备的身份认证与接入安全、设备本身的数据加解密能力，与物联网的入侵检测防护体系成了智慧城市中互联网感知层与传输层的安全需求重点。

城市物联网根据业务特点的不同，可以分为两类：一类是数据流量大，时延要求小的业务，譬如智慧交通中的视频监控业务。另一类是数据流量小，对时延要求低的业务，譬如智能电表的抄表数据业务。对于第一类业务，一般采用光纤专网构建物联网的传输层。对第二类业务，则往往采用低功耗远距离无线传输技术 NB-IoT 或 LoRa 来构建传输层。

在第一类城域物联网中，由于采用光纤专网传输，所以传输安全性较好。对物联网安全的需求多在感知层。对设备安全准入的认证，由于光纤专网良好的封闭传输性，可以放在远离设备本身的管理中心处集中部署。由于光纤带宽充足，因此，对上传数据的加密可以采用高级别加密机制，无需顾及传输效率与数据流量。以常见的智慧交通中视频监控物联网分析，可以从下图中看到准入控制设备 NAM 既可放在远端网关处，也可以放置在城市指挥中心。对设备的认证和准入控制部署较为便利。



专网型物联网安全准入控制

在第二类无线传输城域物联网中，目前国际上主要采用的是 NB-IoT 与 LoRa 两种技术。从二者的技术表现上来看差距不大，服务范围和对象也基本重叠。其主要区别在于工作频段。NB-IoT 工作于授权频谱，也就是运营商专门划分的频段。LoRa 工作于非授权频谱，也就是说，只能在某些指定的免费频段工作。因为二者对安全的需求基本一致，我们在讨论无线城域物联网的时候，以目前国内主流的 NB-IoT 网络为例。

	NB-IoT	LoRa
技术特点	蜂窝	线性扩频
网络部署	与现有蜂窝基站复用	独立建网
频段	运营商频段	150 MHz 到 1 GHz
传输距离	远距离	远距离（1-20km）
速率	<100kbps	0.3-50kbps
连接数量	200k/cell	200k-300k/hub
终端电池工作时间	约10年	约10年
成本	模块5-10$	模块约5$

表格来源：全球物联网观察

类似于一般的物联网感知层，NB-IoT 的感知层容易遭受被动攻击和主动攻击这两种性质的攻击。被动攻击指攻击者只对信息进行窃取而不做任何修改，其主要手段包括窃听、流量分析等。由于 NB-IoT 的传输媒介依赖于开放的无线网络，攻击者可以通过窃取链路数据，分析流量特征等各种手法获取 NB-IoT 终端的信息，从而展开后续的一系列的攻击。

不同于被动攻击，主动攻击包括对信息进行的完整性破坏、伪造，因此对 NB-IoT 网络带来的危害程度远远大于被动攻击。目前主要的

主动攻击手段包括节点复制攻击、节点俘获攻击、消息篡改攻击等。例如在智能电表应用中，若攻击者俘获了某个用户的 NB-IoT 终端，则可以任意修改和伪造该电表的读数，从而直接影响到用户的切身利益。

以上攻击方式可以通过数据加密、身份认证、完整性校验等密码算法加以防范，常用的密码学机制有随机密钥预分配机制、确定性密钥预分配机制、基于身份的密码机制等。NB-IoT 设备电池寿命理论上可以达到 10 年，由于单个 NB-IoT 节点感知数据的吞吐率较小在保证安全的情况下，感知层应当尽可能部署轻量级的密码，例如流密码、分组密码等，以减少终端的运算负荷，延长电池的使用寿命。

NB-IoT 改变了通过中继网关收集信息再反馈给基站的复杂网络部署，组网简洁，便于管理。但也由此带来了一些新的安全问题。

1. 管理节点接入的设备数目巨大。一个 NB-IoT 扇区理论上可以接入十万台物联网终端设备。如果能在如此庞大的设备接入点上高效完成准入认证，加密解密，是一个比较有挑战性的课题。

2. 大范围开放性网络环境。由于 NB-IoT 运行于城市蜂窝通信系统，在城市中必然会遭遇各种电磁干扰。如果遭遇人为的信号干扰活动，比如利用反无人机系统对某基站照射干扰，则必然造成数据信息的丢失。要解决这个问题，端到端的加密机制，设备与基站之间的握手机制，出现长时间电磁干扰后的告警机制，都是必须解决的问题。

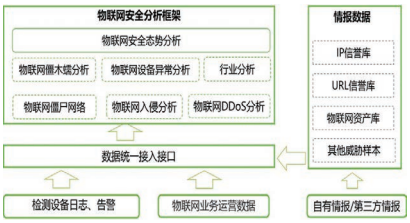
综上所述，对于城域物联网在感知与传输层面的安全防护机制，主要应包含三个方面:

1. 密钥管理。对于无线城域物联网，加密机制需要考虑到通道容量小的实际条件，采用轻量级密码技术。

2. 接入控制与身份 / 数据认证。

3. 电磁干扰环境下的数据传输机制。

如果做到上面谈到的所有机制，对于智慧城市体系中的物联网安全仅仅达到了“可用”的级别。如果要做到对城域物联网进行全方位安全管理与防护，在物联网管理层面需要进一步完善各种功能模块。对物联网的安全威胁分析体系就是其中最主要的一部分。详见下图：



安全威胁分析系统虽然不属于本次对智慧城市物联网安全的详细讨论范畴，将另有专文详述。但该系统通过大数据分析后的结果，可以被采用到智慧城市各项应用的具体运营中。也就是说，当管理者使用物联网安全威胁分析系统对城域物联网进行全方位分析与防护时，产生的分析结果与防护动作也具有城市管理职能。从这一点来看，智慧城市条件下的物联网安全威胁分析系统，已经开始脱离传统安全平台的领域，从而参与到智慧城市的应用与运营中了。

简言之，物联网是智慧城市系统获取数据的一个重要手段，而物联网安全也逐渐脱离了过去网络安全单一的防护功能。物联网安全体系在保证数据准确采集传输的同时，自身也在为智慧城市体系生产着至关紧要的功能性数据。安全即业务的时代，即将到来了。

隐藏在摄像头下的“隐匿者”

政企技术一部 王巍

引言：

在这个万物互联的物联网时代，每样家电都被赋予智能化的标签，智能、互联、可操控是物联网带给人们生活上的便利；与此同时，由互联带来安全风险也加速递增，摄像头漏洞、无人机劫持、机顶盒内容篡改等，给不法分子引进了新手段新途径，让物联网安全蒙上了一层不安全的阴影。

1. 摄像头安全预警

摄像头这一类的监控设备如今使用广泛，对于关键场所的信息记录收集、违法行为抓拍等有着巨大贡献。但是，诸如此类的监控设备却有着大大小小的各种安全漏洞，或者是摄像头采集的视频信息被泄露，引发隐私泄露事件，或者是摄像头后端的主机、数据库被入侵，形成僵尸网络。

下面是绿盟科技政企 BG 三叉戟安全团队整理收集的近几年摄像头安全漏洞。

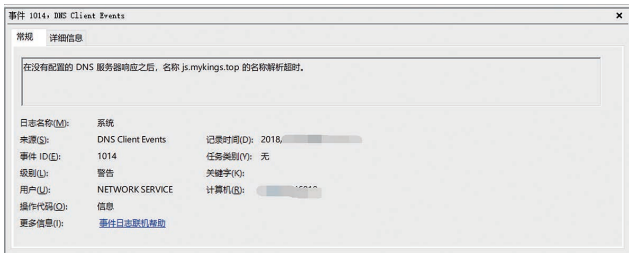
漏洞名称	漏洞详情	漏洞原因
某品牌摄像头存在后门	后门账号：默认运行 Telnet，任意用户通过以下帐号密码都能访问登陆。root:1ybdHbPDn$ii9aEIFNiolBbM9QxW9mr0:0:0::/root:/bin/sh	telnet 协议开放账号检测
预授权信息和凭证泄漏	大华等摄像头在访问服务器配置文件的时候，通过提供空白的“loginuse”和“loginpas”参数，攻击者能够绕过设备的认证程序。这样就能在不登陆的情况下，攻击者下载设备的配置文件。这些配置文件包含设备的凭证信息，以及 FTP 和 SMTP 帐号内容。	默认配置参数权限设置问题
root 权限的预授权 RCE	通过访问带有特殊参数的 URL 链接，攻击者能够以 root 用户权限绕过认证程序并在摄像头上执行各种代码。	账号权限问题
未认证情况下直播	攻击者能够通过 10554 端口访问摄像头的内置 RTSP 服务器，并在未认证的情况下观看视频直播。	端口开放问题 认证问题
Cloud 云上传问题	这些相机提供了“Cloud”功能，能够让消费者通过网络管理设备。这项功能使用明文 UDP 通道来绕过 NAT 和防火墙。攻击者能够滥用这项功能发起蛮力攻击（brute-force attacks），从而猜测设备的凭证信息。	传输协议问题 远程认证问题
信息泄露	大华部分摄像头存在读取 passwd 文件中的账号、密码进行登陆验证；可查看默认的存放账号、密码的文件。	端口探测 代码问题
缓冲区溢出漏洞	只需使用默认凭证登陆，任何人都能访问摄像头的转播画面。同时，摄像头存在的缓冲区溢出漏洞还使黑客能对其进行远程控制。	模糊攻击
默认账户	击者可以利用没有密码的 FTP 用户账号进行登录，然后激活隐藏的 Telnet 功能。或者摄像头的 80 端口管理页面是默认账户。	端口开放问题 认证问题
蠕虫专门针对海康威视相关产品进行攻击	CVE-2014-4878、CVE-2014-4879 CVE-2014-4880；目前已经有成熟的蠕虫专门针对海康威视相关产品进行攻击，通过攻击获得的大量僵尸网络被用来挖矿和 DOS。	缓冲区溢出等问题
远程命令执行	通过远程执行 URL 带参数的命令，来触发对摄像头的远程命令执行攻击，如 'http://192.168.1.107/set_ftp.cgi?next_url=ftp.htm&loginuse=admin&loginpas=admin&svr=192.168.1.1&port=21&user=ftp&pwd=$(telnetd -p25 -l/bin/sh)&dir=/&mode=PORT&upload_interval=0'	模糊攻击 代码问题

2. 惊现僵尸网络

近期，绿盟科技政企 BG 三叉戟安全团队接到某用户反馈，某关键场所的摄像头后端主机疑似被非法入侵，在我们进行问题排查的过程中，就此揭开了“隐匿者”黑客组织僵尸网络的神秘面纱。

0x01 日志分析

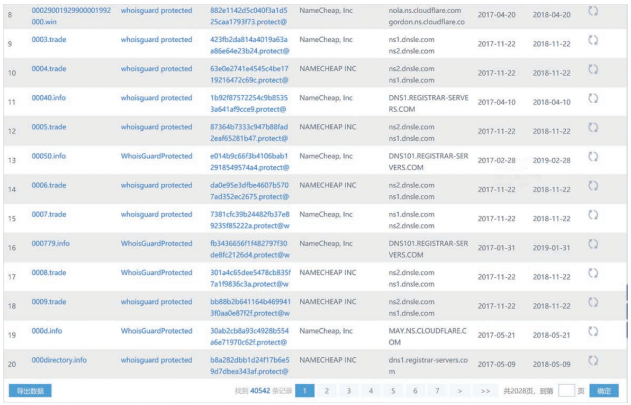
在对客户提供的 Windows Server 2003 日志进行筛选排查后发现，某个时间段内出现了多条 DNS 请求外部域名事件，该向外部请求域名较为可疑，且无法访问。



0x02 WHOIS 查询

在对此类域名进行 whois 查询后发现并无详细注册信息，注册人及联系邮箱和电话均为不可靠保护信息。

选择其中 mykings.top 域名进行电话反查，发现相同注册信息高达 4 万多条。并且多数注册域名不属于正常网站域名，多为 .trade 或 .info 非常规顶级或二级域名，注册域名数量之多，初步怀疑为僵

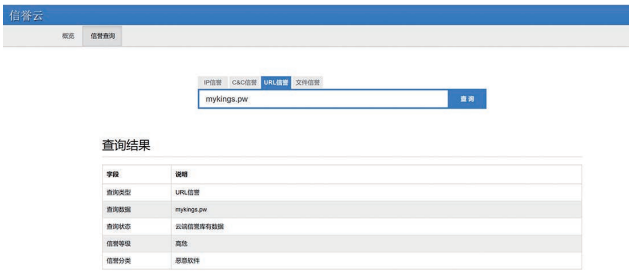


尸网络的不同控制域名。

0x03 僵尸网络

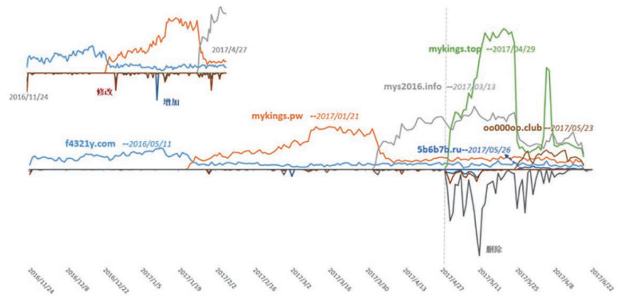
对其中 mykings.top 域名进行信誉查询发现，该域名为危险域名。通过信誉网络分析，*.mykings.top 为主控域名 *.mykings.pw 的下线。MyKings 是一个由多个子僵尸网络构成的多重僵尸网络，2017 年 4 月底以来，该僵尸网络一直积极地扫描互联网上 1433 及其他多个端口，并在渗透进入受害者主机后传播包括 DDoS、Proxy、RAT、Miner 在内的多种不同用途的恶意代码。

根据 C&C 服务器域名攻击频率的相似度分析，mykings.pw、mykings.top 等多个域名在攻击时间和爆发数量上具有相似的持续性，在近半年中，有多篇其他安全厂商报告中都曾出现过“隐匿者”的足迹。卡巴斯基实验室在 2017 年 2 月发布报告《New(ish) Mirai Spreader Poses New Risks》中也提到了前文所述的 mykings.pw 域名。



绿盟科技信誉云

如下图所示“隐匿者”对其他后门账户的操作趋势：（上方为拦截到的“隐匿者”攻击相关恶意行为爆发趋势，下方为拦截到的“隐匿者”对其他后门账户的操作增长趋势）



图取自火绒安全实验室

结束语：

入侵就在你身边，物联网的安全需求，由于分布式的特点，数量多分布零散，容易被黑客攻击组成僵尸网络；另外联网产品品牌种类多，出厂安全性标准不一致，无安全配置或弱口令等问题较多出现。故，物联网安全无小事，万物互联应安全互联。

人人都可成为“千里眼” 视频安全不容忽视

TRG产品部 李静

一部《白夜追凶》一度将黑客送上了热搜榜，而上榜的原因不是黑客盗取了多少数据赚了多少 Money，而是剧中一位黑客同学轻而易举的黑进了公安和交通视频监控系统，并进行了一系列的……(此处省略后续故事情节)，基于职业本能反应，习惯性的在互联网上输入了几个字 “视频摄像头安全漏洞”，迸出的查询结果如下：

“不要存在侥幸心理 八成网络摄像头有漏洞”

“隐私画面视频曝光 网络摄像头安全何在”

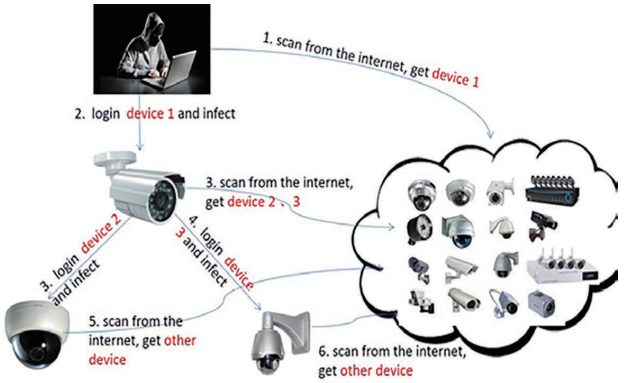
“家里的摄像头竟能被陌生人遥控 原来多个环节有入侵漏洞”

“你的摄像头安全吗? 央视曝光大量家庭摄像头遭入侵”

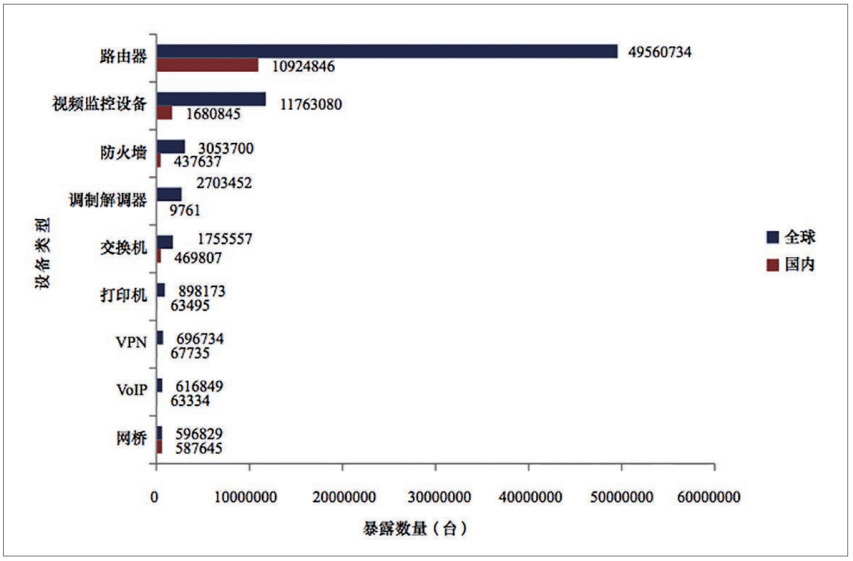
……

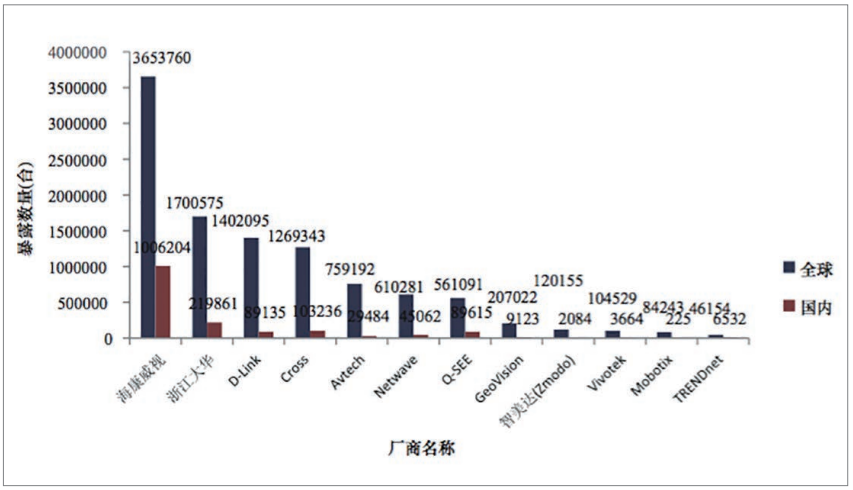
虽然视频安全的现状没有到触目惊心的 “深渊”，其未来的发展依然发人深省。网络摄像头最初仅在重要行业的安防系统使用，随着平安城市、智能交通等智慧城市建设项目的迅猛发展，视频监控已广泛应用在各行业中。在城市交通、道路布控、社区治安等环境中，视频专网建设已形成，规模也不断扩大，路口的摄像机、抓拍器、信号灯、诱导屏等设备数量和类型逐步上升，其中摄像头的数量已经扩散到了几万甚至几十万。

相对于办公网和业务网络，视频专网的网络安全级别更高、网络分支更多、视频监控接入的地址位置更为分散、导致现在视频专网网络设备和监控摄像头存在较大的安全风险，从 2015 年的 “黑天鹅”、“安全门” 事件，近期的 “mirai 蠕虫” 到由中国电信、安全帮和绿盟科技三家联合发布的《2017 年物联网安全研究报告》，报告中提到了几个很可怕的数字和现象，物联网上暴露了众多视频设备，视频监控设备在互联网的暴露数量超过了 1100 万台，高于防火墙、交换机等传统网络设备的暴露数量。从国内分布来看视频监控设备的暴露数量达到 168 万台。



视频监控设备暴露最多的服务有 4 类，分别是 HTTP 服务 (端





口 80、81、8080)、浙江大华私有协议 (端口 37777)、Telnet 服务 (端口 23) 和 RTSP 服务 (端口 554)。图中所列的设备数量仅为网络空间搜索引擎已识别出来的结果，由于部分设备暴露的端口特征不明显，实际的数量远远不止这个量级。

通过我们大量的用户调研和客户交流分析，发现视频专网的安全现状存在以下几个问题：

1. 视频摄像头为视频专网的重要组成部分，其数量庞大且位置分散，建设厂商各异，建设产权单位不同，随着物理网和大数据、IP 数字化网络的推动，其管理和监控上资源有限，无法做到持续有效的监控和统一管理，对摄像头的数量和规模做到了如指掌。

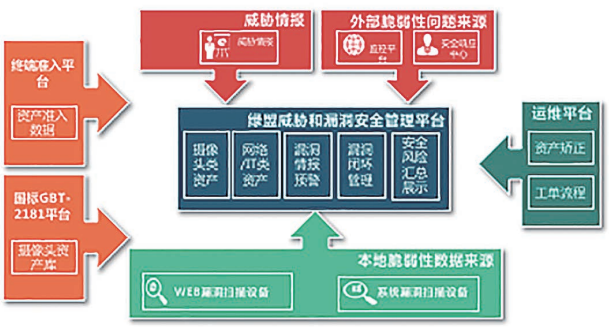
2. 在视频监控建设时，更多的考虑的是视频监控业务本身，视频专网的安全性考虑较少，简单的认为“物理隔离”可以从根源上杜绝一切安全隐患，令视频专网长时间处于裸奔状态。

3. 市场上近八成家用智能摄像头产品存在用户信息泄露、数据传输未加密、APP 未安全加固、代码逻辑存在缺陷、硬件存在

调试接口、可横向控制等安全缺陷，视频监控网络安全问题普遍存在，用户对视频安全重视程度不够，在安全了监控摄像头之后，没有对密码进行修改，很多存在弱口令等问题，系统漏洞也未得到及时修复，极易遭受黑客攻击。

4. 漏洞数量越来越多，漏洞传播已经社区化，漏洞的利用速度越来越快，漏洞的修复工作和漏洞应急响应已经显得过于缓慢。

如何保证视频专网的全程可控和全时可控，防止避免视频专网网络摄像头等设备成为僵尸设备，被仿冒甚至利用，是我们亟需解决的新安全问题。建设完善有效的设备资产全过程管控、从全局视角完成漏洞管理，利用漏洞情报信息建立快速的应急响应机制，及时有效完成漏洞治理工作是我们进行视频专网安全建设的核心思路。

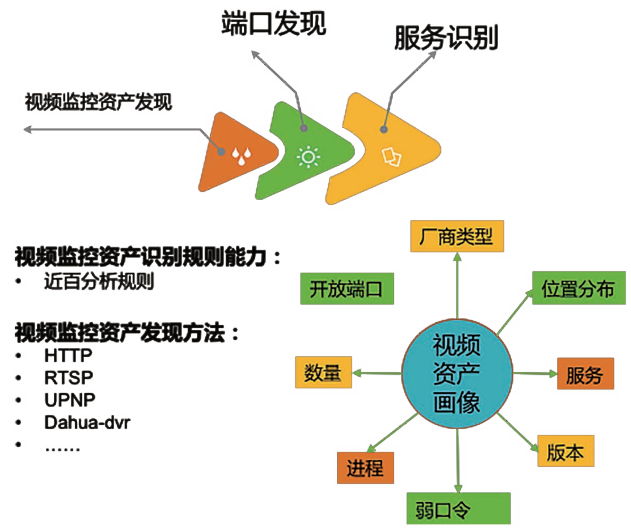


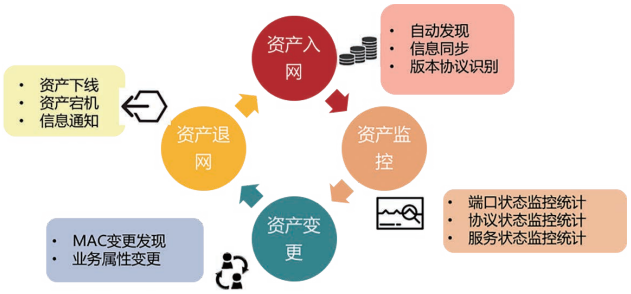
多年来，我们一直重视并致力于视频监控相关的安全建设解决方案。2017 年年初，发布了绿盟视频监控网威胁和漏洞安全管理解决方案。方案提供视频全生命周期管理和视频漏洞的全过程支撑，量化跟踪和分析流程执行情况，促进管理流程持续优化。充分利用

绿盟威胁情报中心（NSFOCUS NTI）发布的漏洞情报信息，触发视频监控漏洞管理流程，建立快速响应机制，及时有效完成漏洞修补工作。

在方案中，视频漏洞情报被应用于漏洞快速响应、漏洞风险分析和优先级分析、漏洞修复等环节，对漏洞的快速响应是漏洞管理的第一步。

通过强大的设备识别进行视频监控摄像头的主动发现，通过对视频专网内的视频监控摄像头的新增、变更、下线过程进行持续监控，同时对全网监控摄像头进行全面普查，确定网络内合法存在的资产、版本、开放的服务和端口、安全配置项目，将收集到信息将作为网络





内的资产监控基线，对于后续未经确认出现的资产变化，及时通报安全责任人，协助安全规定的有效执行。

以预防为目的的漏洞全过程管理，通过引入漏洞情报、和对资产的预先梳理和持续监控，把漏洞管理流程向外扩展了漏洞发现环节的风险预警、漏洞分析环节的漏洞修复建议、漏洞修复环节的修复方案社区，以及对整个管理过程的评估、对比和优化。

绿盟视频监控网威胁和漏洞安全管理解决方案结合当前漏洞威胁情报，结合本地风险持续监控，以及漏洞管理全流程管控能力，提供快速应急响应、风险预警触发的高效率工作模式，并且在管理流程的各环节，提供优化分析后的技术建议，最大程度加快漏洞修复效率，在漏洞被利用前完成修补。为客户漏洞管理流程提供快速响应、有序修补、持续优化的管理能力。

万物互联的网络时代已经到来，视频监控安全如果仅从硬件或者软件单一层面进行检测、管理防护，很难从根本上防微杜渐，尤其是涉及到国泰民生的企业视频监控使用，闭环安全生态需求一直都是第一要务，从底层芯片、软件系统、数据采集识别、数据存储和分析、网络传输加密到上层管理的安全链才能正中要害。

安全无止境，视频专网安全要真正实现资产理得清、风险看得见、资源管得住、责任查得出！

智能家电安全问题漫谈

北区安全服务交付部 张默

关键词：智能家电 控制终端 互联网平台 物联网模块安全

摘要：智能家电是物联网的一个具体应用，本文将智能家电架构逻辑化和通用化，从控制终端、互联网平台和物联网模块三个角度介绍智能家电典型的安全问题。

一 . 概述

“还没到家，就能让客厅的灯打开，浴室的洗澡水已经烧好，卧室空调调成最舒服的温度，电视已经自动打开你喜爱的频道……”，这句话是智能家电典型的推广用语，也为大众提供了广泛的想像空间，毕竟当年只有在电影里才是这样啊!

随着物联网的高速发展，作为其典型应用的智能家电，市场份额也迅速扩大，不论传统的白色家电厂商，还是新型的互联网公司，都纷纷推出各种各样的智能家电产品，大到空调、洗衣机、冰箱，小到咖啡机、电水壶、灯泡，种类繁多。智能家电进入了寻常百姓的家中，为大家提供了新奇和便利的体验，与此同时，这种快速增长的背后也存在着网络安全隐患，可能对智能家电用户、智能家电厂商，甚至整个互联网都带来不良影响。

二、HTTPS 的 DDoS 攻击原理

2.1 智能家电逻辑架构

智能家电逻辑架构分为三个部分，分别是控制终端、互联网平台和物联网模块。三者通过网络连接，相互传递指令和状态等数据，实现智能家电的管理、控制与状态查询。控制终端是用户与智能家电设备交互的渠道，最常见的方案是用户在手机内安装对应的 APP；物联网模块负责处理家电设备的网络通信，在家电内部与其控制电路相连，实现将网络指令和数据通过内部接口传递给家电设备。

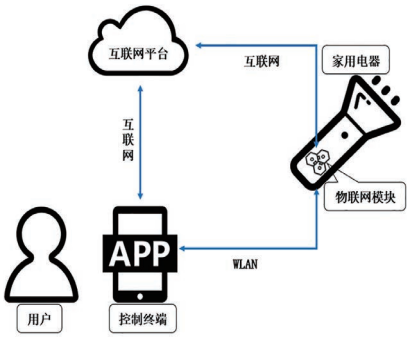


图 1 智能家电设备逻辑架构图

从智能家电设备逻辑架构可以看出，其安全性包含了控制终端、互联网平台和物联网模块三者的自身安全和相互交互安全，同时也包含使用过程中的网络接入、用户绑定和数据存储等方面的安全。下面从控制终端、互联网平台和物联网模块三者不同的角度来例举一些典型的安全问题。

2.2 控制终端典型安全问题

控制终端常见的实现方案是用户在其手机中安装 APP，那么 APP 和手机安全问题自然也就是智能家电设备控制终端的安全问题。作者不久前购买了国内某知名品牌智能家居套装、空气净化器及其生态下的飞利浦智能灯泡，通过其 APP 可实现智能化和场景化的控制，此外还购买了该厂商的智能蓝牙音箱进行语音控制，但是由于某种原因很难购买。难道就不能实现语音控制了吗? 答案当然是否定的，具体方案有很多，其中一种方案就是使用苹果的家庭 APP，通过 Siri 进行语音控制。该方案不是很复杂，可在 GitHub 下载现成的源代码，但实现控制的前提是获取该品牌各个智能设备的通信密钥，可以通过开发者模式可直接获取，而相应的净化器和智能灯泡的通信密钥获取比较复杂。此外 GitHub 上还有通过网络嗅探的方式获取密钥的源代码。

获取密钥后，通过简单的配置即可实现使用苹果的家庭 APP 来管理该品牌智能设备，通过 Siri 进行语音控制。

以上是笔者实现的通过第三方平台控制国内某知名品牌智能设备的简单过程，在过程中也存在一些安全隐患，典型问题就是通信密钥应不应该被获取，密钥被获取后能不能被第三方平台使用。如果用户的手机被攻击者植入恶意代码，或通过 Wi-Fi 破解等方式连入用户家庭网络，对于攻击者而言，获取智能设备密钥也不是难事，那么将会对用户生活或隐私带来极大困扰。

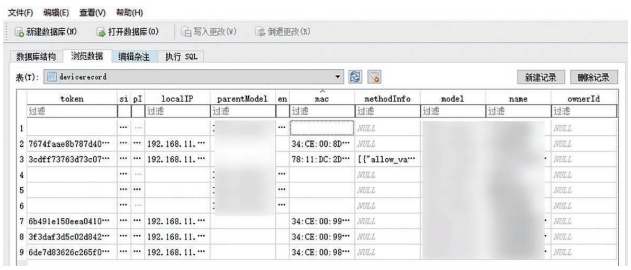


图 2 国内某知名品牌净化器和智能灯泡通信密钥获取

2.3 互联网平台典型安全问题

互联网平台安全与传统 Web 应用安全类似，典型的安全问题各厂商都已了然于胸，但也不代表不会出现“疏忽”。美诺 Miele 是创建于德国的一个百年家电品牌，2017 年一款型号为 PG8528 的联网医用清洗机 / 消毒柜被曝存在服务器目录遍历漏洞。这台设备的 Web 服务器漏洞编号为 CVE-2017-7240，漏洞可导致未经授权的入侵者访问 Web 服务器的任意目录。这样一来攻击者也就可以从中窃取敏感信息，甚至植入自己的恶意代码，让 Web 服务器执行这些

图 3 美诺 Miele PG8528 联网医用清洗机 / 消毒柜

代码。

此漏洞是由德国安全研究人员发现的，他曾在 2016 年 12 月就向 Miele 上报了此问题。不幸的是，他并未收到该公司的任何回复，所以 4 个月之后他选择直接曝光漏洞。

可能从 Miele 的角度来看，事情并没有那么糟糕，但是从另一个角度来看，这种关键的医用设备存在如此缺陷却未受到足够的关注，也没有得到及时的安全响应，这些事实就足以表明越是有把握的事更应该被关注和重视，以免出现“疏忽”。

2.4 物联网模块典型安全问题

物联网模块安全相对与控制终端和互联网平台安全，是应该更值得关注的。智能家电等物联网设备应用刚刚开始全面普及，很多物联网模块安全隐患尚未充分暴露，易造成大规模影响。2016 年 10 月 21 日，美国东海岸地区遭受大面积网络瘫痪，其原因为美国域名解析服务提供商 Dyn 公司当天受到强力的 DDoS 攻击所致，其中部分重要的攻击来源于物联网设备，经过分析确认，攻击流量的来源之一是感染了名为 Mirai 物联网恶意软件的设备。其实 Mirai 感染和传播的原理并不复杂，主要是利用了物联网设备的固件漏洞和弱口令，正是由于物联网设备的加速普及和封闭性的特点，其自身安全未得到足够重视，而这两个问题也是智能家电等物联网设备的痛点。

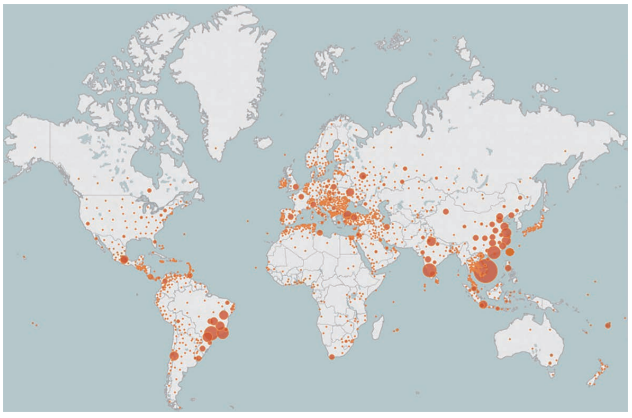


图 4 Mirai 全球感染和传播示意图

随着物联网的热潮，芯片厂商针对各种生活场景提供有针对性的整套设计方案，降低了进入该领域的门槛，制造商可以快速的利用芯片厂商提供的解决方案，定制化硬件设备产品，自己可以不关心硬件集成的问题，只需要利用芯片厂商提供的 SDK 开发平台开发自己的上层应用即可。正是由于这种模式，导致大量物联网设备固件开发仓促，未充分考虑安全问题，可能造成通用的安全风险。

除了物联网设备厂商原因产生的安全隐患，用户在购买和使用物联网设备时安全意识也有待提高。用户购买产品后，往往按照说明书向导式的联网、绑定和配置后就开始使用物联网设备，而忽略了最基本的口令安全，尤其是商用大批量采购集中部署。2015 年，某省公安厅发布了“关于立即对全省某品牌监控设备进行全面清查和安全加固的通知”的文件。文件称，近期，该省各级公安机关使用的该品牌监控设备，“存在严重安全隐患”，“部分设备已经被境外 IP 地址控制”。据此，文件要求，“各地对使用的某品牌设备进行全面清查，并开展安全加固”。而其原因是该省互联网应急中心通过网络流量监控发现部分在互联网上的该品牌设备因弱口令问题（弱口令包括使用产品初始密码或其他简单密码，如 123456、888888、admin 等），

图 5 大量视频监控设备暴露在互联网上

被黑客攻击。

智能家电等物联网设备使用时，终端绑定也是个有趣的逻辑问题。漫步于某个大型停车场，使用手机搜索附近的热点，会发现很多行车记录仪可以连接，密码可能也是前面提到的弱口令，是不是就可以随意连接并下载其中的视频呢？显然不是这么简单。原来，手机和行车记录仪连接时，需要进行绑定，绑定的最后步骤是按压行车记录仪的物理按键进行确认，以此保证不被恶意绑定。但实际上，并不是所有的智能家电设备都必须通过物理按键确认绑定，这也可能产生恶意绑定等不必要的隐患。

三 . 总结

以上从智能家电逻辑架构的控制终端、互联网平台和物联网模块三个角度例举了一些典型的安全问题，有些问题是由于厂商设计开发原因导致的漏洞，有些问题则是用户在使用过程中由于安全意识不足导致。

建议智能家电厂商：

扎实做好安全开发，建立全面的开发过程规范，在关注物联网模块安全的同时，不忽略控制终端和互联网平台的安全问题；

制定合理的安全策略，采取适度的开放原则，对涉及用户隐私和可能影响用户生活的安全隐患保持关注；

使用通用设计方案时应格外谨慎，防范连带风险；

重视各种途径反馈的安全问题，并及时修改。小的安全问题如能关联起来也将产生严重后果；

做好用户的安全引导和安全设计，如说明书和配置向导中提升口令等意识安全、用户首次登陆强制修改默认密码、不允许设置简单密码等。

建议智能家电用户：

不要盲目 root 或越狱手机，从正规应用商店下载 APP；

加强家庭无线网络安全设置，使用 WAP 2.0 协议，设置复杂密码并定期更换；

尽量避免使用第三方开源平台控制智能家电；

修改智能家电默认口令，并设置复杂口令。

相信随着物联网应用快速普及和大众对网络安全的重视程度逐步提高，以等级保护物联网安全扩展要求发布为契机，物联网安全将会获得较大幅度提升。

四 . 参考文献

http://www.freebuf.com/news/130561.html

http://www.freebuf.com/articles/terminal/117927.html

https://jaq.alibaba.com/community/art/show?articleid=90

http://tech.163.com/15/0228/14/AJI19QG8000915BD.html

物联网设备安全评估的七种武器

威胁情报与网络安全实验室 李东宏

物联网发展迅猛，正加速渗透到生产、消费和社会管理等各领域，物联网设备规模呈现爆发性增长趋势，自 2015 年至 2020 年，物联网终端年均复合增长率为 33%，安装基数将达到 204 亿台，其中三分之二为消费者应用。在联网的消费者和企业设备的投资为 2.9 万亿美元，年均复合增长率高达 20%，将超过非联网设备的投资。物联网设备已经逐步渗透到人们生产生活的方方面面，为人们及时了解自己周围环境以及辅助日常工作带来便利。但随着互联紧密度的增高，物联网设备的安全性问题也逐渐影响到人们的正常生活，甚至生命安全，物联网设备安全不容小觑。

由于物联网的迅速发展，以及物联网设备呈现出来的低成本、低安全的趋势导致黑客将目标从传统的 IT 设备转移到物联网设备。

针对物联网设备的安全评估，这里总结七种评估方式，从七个方面对设备进行安全评估，最终形成物联网设备的安全加固方案，提升黑客攻击物联网设备的成本，降低物联网设备的安全风险。

第一种武器：硬件接口

通过对多款设备的拆解发现，很多厂商在市售产品中保留了硬件调试接口。例如一般为 10 针、14 针和 20 针的可以控制 CPU 的运行状态、读写内存内容、调试系统代码的 JTAG 接口以及一般为 4 针的可以查看系统信息与应用程序调试的串口，俗称 COM 口。通过这两个接口访问设备可以获取到系统最高权限。例如研究人员可以通过串口访问 LG home-bot 的文件系统以及在安全评估，针对这些硬件接口的利用主要是为了获得系统固件以及内置的登陆凭证。

第二种武器：弱口令

目前物联网设备大多使用的是嵌入式 linux 系统，账户信息一般存放在 /etc/passwd 或者 /etc/shadow 文件中，攻击者拿到这个文件可以通过 John 等工具进行系统密码破解，也可搜集常用的弱口令列表，通过机器尝试的方式获取系统相关服务的认证口令。臭名昭著的 Mirai 和 Rowdy 恶意代码中就存在弱口令列表，一旦发现认证通过，则会进行恶意代码传播。弱口令的出现一般是由厂商内置或者用户不良的口令设置习惯两方面造成的。

第三种武器：信息泄漏

多数物联网设备厂商可能认为信息泄露不是安全问题，但是泄露的信息极大方便了攻击者对于目标的攻击。例如在对某厂商的摄像头安全测试的时候发现可以获取到设备的硬件型号、硬件版本号、软件版本号、系统类型、可登录的用户名和加密的密码以及密码生成的算法。攻击者即可通过暴力破解的方式获得明文密码。

第四种武器：未授权访问

攻击者可以不需要管理员授权，绕过用户认证环节，访问并控制目标系统。主要产生的原因如下：

厂商在产品设计的时候就没有考虑到授权认证或者对某些路径进行权限管理，任何人都可以最高的系统权限获得设备控制权。

开发人员为了方便调试，可能会将一些特定账户的认证硬编码

到代码中，出厂后这些账户并没有去除。攻击者只要获得这些硬编码信息，即可获得设备的控制权。

开发人员在最初设计的用户认证算法或实现过程中存在缺陷，例如某摄像头存在不需要权限设置 session 的 URL 路径，攻击者只需要将其中的 Username 字段设置为 admin，然后进入登陆认证页面，发现系统不需要认证，直接为 admin 权限。

第五种武器：远程代码执行

开发人员缺乏安全编码能力，没有针对输入的参数进行严格过滤和校验，导致在调用危险函数时远程代码执行或者命令注入。例如在某摄像头安全测试的时候发现系统调用了危险函数 system，同时对输入的参数没有做严格过滤，导致可以执行额外的命令。

第六种武器：中间人攻击

中间人攻击一般有旁路和串接两种模式，攻击者处于通讯两端的链路中间，充当数据交换角色，攻击者可以通过中间人的方式获得用户认证信息以及设备控制信息，之后利用重放方式或者无线中继方式获得设备的控制权。例如通过中间人攻击解密 HTTPS 数据，可以获得很多敏感的信息。

第七种武器：云（端）攻击

近年来，物联网设备逐步实现通过云的方式进行管理，攻击者可以通过挖掘云提供商漏洞、手机终端 APP 上的漏洞以及分析设备和云端的通信数据，伪造数据进行重放攻击获取设备控制权。例如 2015 年 HackPwn 上公布的黑客攻击 TCL 智能洗衣机。

上面总结了七种物联网安全设备的评估方法，识别出物联网设备的安全弱点，最终目的是要通过各种加固方式消除安全隐患。

为了降低物联网设备受攻击的概率，可以通过如下的手段进行安全加固。

1) 物联网设备在设计之初就需要考虑硬件、应用和内容可信，保证攻击者无法获取以及篡改相关资源。

2) 在物联网设备中确保没有后门指令或者后门代码。针对用户认证，需要设计成在第一次配置和使用设备时由用户进行自行设置并需要设置强口令策略。在发行版本中去除调试版本代码，将 JTAG 接口和 COM 口进行隐藏，同时关闭例如 SSH，Telnet 等不安全的服务。

3) 产品开发过程中需要遵循安全编码规范，减少漏洞产生，降低潜在风险。

4) 物联网设备需要以全局唯一的身份加入到物联网中，设备之间的连接需要可信认证。

5) 在通讯过程中或者数据存储过程中需要使用强加密算法（例如 AES）进行数据加密和认证（例如 SHA256 签名算法）。密钥使用非对称加密进行传输。

6) 在设备上市前进行专业的产品安全测试，降低物联网设备安全风险。

7) 内置安全机制，增加漏洞利用难度，厂商可以通过增量补丁方式向用户推送更新，用户需要及时进行固件更新。

8) 用户处建议部署厂商提供的安全解决方案。

记一次物联网安全测试的经历

NS-SRC 马良 李东宏

关键词：物联网 渗透 安全测试 通信 串口 固件提取

摘要：本文对一次物联网安全测试过程做了一个简单的总结，对物联网安全测试的方法和思路进行了一个简单的介绍。对物联网设备安全测试中常见的攻击方法进行一个简单的梳理。

一：任务的领取

两年前的某一天，我所在研究院的院长说有一个某厂家的物联网方面的安全测试项目，问我和钊谁想去。测试的时间比较紧张，是因成本问题 (按照测试的天数 / 时间收费)，客户想在 3-4 天内完成两个设备的安全测试。

我和钊的技术背景不同：钊擅长信息安全方面；我擅长硬件破解和固件安全。

虽然我们之前在实验室做了一些物联网设备方面的安全研究，掌握了安全测试的基本要领；但是，当时是我们第一次去厂商那里做设备方面的安全测试，对那么短的测试时间，再加上客户测试什么设备现场随机指定，心里确实没有太大的把握。

我和钊合计后问院长：可不可以两个人一起去。院长联系了市场部同事后，得到的答复是可以两个人一起去。感谢院长和市场部同事，我们争取到第一次宝贵的项目经验。后来发现，在物联网安全发展初期，项目经验不多时，两个人一起出去是对的，知识和技能可以互补。所有的经验都是从无到有，慢慢积累起来的。

现在，钊已经成为公司物联网安全方面的专家。内部称号“钊神”。

出发前，我特意带齐了硬件电路拆解和调试常用的各种小工具，准备好可能用到的软件，准备随时召唤神龙。经过一晚上的火车，我们来到了厂家所在的 A 市。

第二天上午，我们要先选取要进行安全测试的物联网设备。选取设备的时候，我们顺便参观了企业的展厅，物联网展厅的设备很多，大到洗衣机这种大家伙；小到摄像头和小小的传感器。可以说该企业的物联网产品品种十分丰富，可以看出厂家是真心要在物联网方面发力。但厂家可能在安全方面的经验有所欠缺，所以，需要我们发挥安全的长处，帮助厂商发现设备存在的安全漏洞。

厂家代表带指定了本次要进行安全测试的设备：两台安全路由器。也说明了为什么选择这两款设备的测试理由：路由器是家庭接入互联网的入口。厂家在安全方面本来就做了一些努力。希望我们能帮助找出这两款路由器存在的安全隐患。本次厂家给的包装和说明书都很全。企业代表很重视路由器的安全情况，因为很多物联网设备的联网都依赖与路由器。**两款路由器有一款是自己的研发团队设计的，细节自己**

可以把控；另外一款是外包出去的，具体细节不了解，借此机会正好了解一下外包产品的安全性和稳定性。由外包开发的那一个路由器，暂时无法提供固件，固件提取需要我们自己解决。

二：物联网设备安全分析与常见安全测试点

IoT 安全测试中，可以根据实际业务情况，构建一张全面的攻击面图，表示各个攻击点之间的关联关系，可以按照以下步骤执行：

第一步：全面了解 IoT 架构，包括阅读产品文档、手册、官网发布的信息等，利用一切能够查找到的资源，理清业务逻辑；

第二步：构建结构图，说明各个组件之间的关系。如果两个设备之间通过无线电通信，则使用有向线连接设备，并标注清楚所使用的通信协议。如果应用程序与云端通信，并通过 API 收发数据，则在有向线上标注清楚所使用过的 API。

第三步：完成结构图后，从攻击者的角度思考，有哪些可以利用的点，需要用到的技术，并列出测试用例。

IoT 安全测试中，常见的漏洞以及测试点如下表所示 (限于篇幅，仅列举常见的) :

漏洞	攻击面	说明
用户名枚举爆破	管理界面 Web 界面 云端界面 移动应用界面	能够收集到一系列邮箱用户名，并尝试通过绕过或爆破等技术通过验证机制
弱口令	管理界面 Web 界面 云端界面 移动应用界面	如使用 123456、admin 等弱密码
账号锁定	管理界面 Web 界面 云端界面 移动应用界面	在 3-5 次账号认证尝试失败后，依然能够继续尝试
未加密服务	设备网络服务	网络服务未加密，攻击者可以通过嗅探获取到有效信息
双因素认证	管理界面 云端界面 移动应用界面	缺乏双因素认证机制，如安全 token 或指纹扫描
弱加密	设备网络服务	虽部署加密服务，但未正确配置或未及时更新，例如，使用 SSL V2
更新未加密	更新机制	设备更新通过网络明文传输，未使用 TLS 加密，更新文件本身也未做加密
更新路径可写	更新机制	更新文件存放路径写权限未做限制，固件程序存在被篡改并分发给所有用户的风险
DoS	设备网络服务	服务存在 DoS 攻击风险
移除存储介质	设备物理接口	存储介质可以从设备上移除
无手动更新机制	更新机制	无法手动强制更新设备
缺乏更新介质	更新机制	未提供更新接口，设备无法更新
固件版本或最近更新日期	设备固件	固件当前版本以及最新版本未知
固件提取	官网下载 更新拦截 JTAG/SWD/eMMC SPI Flash/eMMC 芯片提取	固件程序包含很多有用信息，包括源码、服务二进制程序、预设密码、ssh 秘钥等
操作设备程序执行流	JTAG/SWD 接口 Side Channel Attack	串口 gdb 调试，改变程序执行流 Side Channel Attack 同样可以改变程序执行流或从设备中获取到敏感信息
获取控制台访问权限	串口 (SPI/UART)	通过连接到串口，可以通过控制台访问设备通常的安全措施包括自定义 bootloader，防止攻击者进入单用户模式，但该方案同样可以被绕过

三：固件提取

首先，我们一边对这两款路由的说明书进行熟悉。一边进行硬件拆解，希望找到可以提取固件的方法。我们看过厂家的网站后，发现厂家不提供此路由器的固件下载。

下面是常见的固件获取方法和提取思路

1、官网或联系售后索取升级包

2、在线升级，抓包获取下载地址

3、逆向升级软件，软件内置解包和通讯算法

4、从硬件调试接口：JTAG/SWD，利用调试工具的任意地址读取功能

5、拆 Flash、Sd 卡、TF 卡、硬盘等，用编程器或对应设备读固件

6、用硬件电路的调试串口和固件的 bootloader 获取固件

7、通过利用网页和通讯漏洞获取固件敏感信息

8、用逻辑分析仪监听 flash，ram 获取信息

9、从硬件串口获取系统权限后，用 tar、nc、dd、echo、vi 等命令提取固件

注：本次提取固件用了 2、6 和 9 的方法。

第一款路由器固件提取：在我们在拆机后，按照以往的经验找到了设备预留的开发调试串口，把串口线焊接出来，接入电脑可以看到系统开机后打印设备信息。因为厂家当时没有进行串口登陆认证，我们从串口获取到了系统的操作权限。这次我们的运气特别好，直接就获取到了路由器系统的 root 权限。但是，发现 busybx 进行了严重的裁减，例如 tar、dd、nc 等命令都不可用，没有办法直接提取固件。后来，我们通过串口发送拷贝命令的方式，通过 U 盘备份的方式，把固件完整的备份到了 U 盘，算是提取了第一款设备的固件。

第二款路由器的固件提取：在试用该路由器的手机端控制软件后，发现可以通过厂家 APP 在线升级路由器的固件。这就带给我们一个思路：通过抓抱获取路由器的固件下载地址。

但是这次的工具准备中，我们少带了一个设备：HUB。因为 HUB 早就淘汰了，向厂家没有借到。出去买的话，又耽误了测试时间。经过网上搜索，我们用 360 随身 Wi-Fi 和笔记本电脑结合，通过劫持通过 Wi-Fi 的流量解决了抓包问题。固件的升级包地址被我们抓到了。

于是，我们圆满获得了两款设备的固件。提取固件花费了我们一天半时间。在剩下的两天时间里，我们能找到固件的漏洞吗？

四：找固件漏洞

提取到路由器的固件后，我们对固件用 binwalk 进行了解包，获得了固件的完整文件系统的还原。

```
racted/cpio-root# ls -l
total 56
drwxr-xr-x  2 root root 4096 Feb 15 21:48 bin
drwxr-xr-x  3 root root 4096 Feb 15 21:08 dev
drwxr-xr-x  2 root root 4096 Feb 15 21:08 etc
drwxr-xr-x 10 root root 4096 Feb 15 21:46 etc_ro
drwxr-xr-x  2 root root 4096 Feb 15 21:08 home
lrwxrwxrwx  1 root root   11 Feb 15 21:08 init -> bin/busybox
drwxr-xr-x  4 root root 4096 Feb 15 21:08 lib
drwxr-xr-x  2 root root 4096 Feb 15 21:08 media
drwxr-xr-x  2 root root 4096 Feb 15 21:08 mnt
drwxr-xr-x  2 root root 4096 Feb 15 21:08 proc
drwxr-xr-x  2 root root 4096 Feb 16 10:23 sbin
drwxr-xr-x  2 root root 4096 Feb 15 21:08 sys
drwxr-xr-x  2 root root 4096 Feb 15 21:08 tmp
drwxr-xr-x  5 root root 4096 Feb 15 21:08 usr
drwxr-xr-x  2 root root 4096 Feb 15 21:08 var
```

经过两天的安全测试，我们发现固件中都存在厂家后门密码，并且密码为明文硬编码。最坏的情况是，固件默认开启了远程 Telnet 登陆服务，用户无法关闭这个服务。也就是说，任何人只要通过固件获取了厂家的后门密码，就可以远程控制这两款路由器，进行更危险的操作，比如，监控用户的上网情况。

另外，还发现一个从路由器的 WEB 页面中远程代码执行漏洞。同样可以通过远程网络获取代码执行权限。还有其他影响范围小一

点的信息安全问题。最后，我们在每个路由器发现了十几个漏洞。两款路由器总共发现二十多个漏洞。

幸亏发现这个问题的是安全测试人员而不是黑客，没有对用户和企业的声誉产生影响。所有漏洞我们直接提交给了厂商的安全部。

五：其他收获

到了 A 市，发现此次任务还有一个工程的同事 H，H 负责对整个企业的业务进行安全测试，顺便测试物联网平台的安全漏洞 (WEB 端)。测试时间也是 3-4 天。测试结束后，发现 H 同事是一个真正的渗透测试大牛。

H 这次的收获很大：发现了物联网控制的平台的几个系统权限漏洞，如：普通用户修改管理员密码漏洞，任意账户遍历控制所有设备漏洞等权限问题。

最让厂商安全接口人震惊的是：H 同事在对企业进行渗透测试时，从外网 WEB 端渗透进入了企业内网。企业的安全接口人员一开始不敢相信这是真的，一连说了好几个“不可能”。直到 H 大牛提供了相关进入的证据。

原来：部分人员违反信息安全规定，使用了跳板机。导致渗透测试进入了内部的重要网络。

我们把这次的安全测试情况和测试方法，写了详细的测试报告。交给厂商的的安全业务负责人。厂商的负责人对我们的工作进行了肯定，在我们临走前请我们吃饭，我们就物联网设备目前存在的安全问题提出我们的看法和改进意见。

最后，任务圆满完成了，回来的路上感觉很轻松，我们积累的技术经过了实战的检验，感觉以前所有努力都是值得的！

六：总结

在这次渗透测试过程中，我们相互配合，交流各自的思路。我向钊学到了很多信息安全方面的思路和技能；我也给钊展示了硬件设备的固件提取方法和分析思路。

通过此次安全测试，我们的技能和项目经验都有了提高。顺利的完成了物联网设备的安全测试，在安全行业，快速学习能力也是必备的技能。

假如本次的安全测试没有发现漏洞，说明厂商在安全方面做的好，大的方向和思路上没有问题，安全工作做的很到位，厂商应该高兴和自豪。

如果在安全测试中发现了严重的安全问题，厂家更应该高兴，因为有人帮他们发现了设备存在的安全问题，帮助厂家解决了用户的安全隐患，避免了厂家因为安全问题带来的经济和声誉损失，提高厂商的客户对该品牌的认可和厂商的知名度；同时，我们测试结束后都为厂家提供详细的测试过程文档，文档记录了我们的测试思路和测试工具、测试步骤。通过安全测试，厂家的安全意识提升，厂家也可以了解到更多的安全测试思路，对以后展开安全工作起到了积极的作用。

当然，本次测试能顺利发现多个严重漏洞也有运气成分。也说明当前的物联网厂商开发人员的安全意识不高，主要实现设备的功能性了；没有考虑设备的安全性，存在很多安全问题，甚至存在严重漏洞，在安全方面很有很长的路要走。

物联网设备安全测试中常见的攻击面分析

NS-SRC 马良 李东宏

关键词：物联网 渗透测试 安全测试 通信串口 固件提取 APP 分析

摘要：本文总结了物联网安全测试思路，包括物联网设备的通信设备之间的关系，分析流程和安全分析步骤，以及常见的物联网安全漏洞，并对物联网设备安全测试中常见的攻击面和攻击方法进行简单的梳理。

因为业务需要经常要进行物联网设备的安全测试，所以，将一些常见物联网设备的测试点进行了总结。限于版面，这里重点介绍思路。不对测试点进行罗列。

一：物联网设备通信过程分类

物联网技术设施分为以下部分：

(1) 嵌入式设备（智能设备）

(2) 云端服务和组件

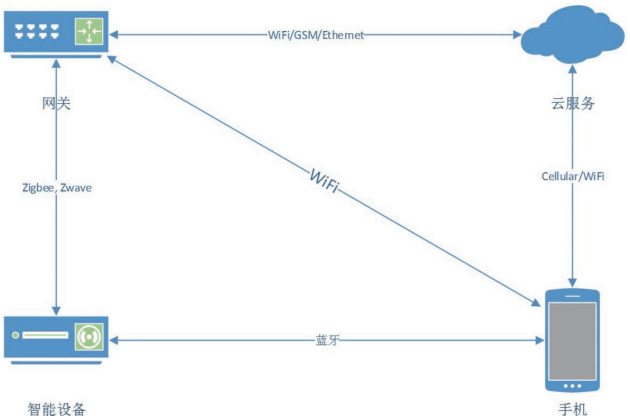
(3) 通信网关

(4) 客户端（手机等）

嵌入式设备

设备是 IoT 架构中的关键组成部分，包括一切硬件设备（网关、传感器等）。

例如，多数智能家具应用中，包括智能网关和操作设备，网关



是所有其他设备的中心连接点，操作设备负责完成实际的操作，如摄像头负责图像监控，智能洗衣机完成洗衣指令。

设备漏洞包括串口访问、固件提取、WEB 端越权、固件执行、后门密码漏洞等。

云服务与云 API 组件

软件与云组件包括以下元素：

(1) 设备固件

(2)Web 应用

(3) 移动应用，通常用于控制、配置以及监控设备

无线电通信

无线电通信负责设备与设备、设备与 APP 之间的通信，常见的无线电通信包括 Wi-Fi, BLE, Zigbee, ZWave, 6LoWPAN 以及蜂窝网等。

网关设备

常用于物联网设备指令的转发等，可以是传统的路由器，也可以是新型智能设备。

例如：小米智能网关。是一种智能家居设备的新形态。主要完成多种设备和协议的转换和接入问题，降低了单个传感器设备的功耗和复杂度，间接降低了整个系统的设计和安装成本。

二：物联网设备的分析流程

理解业务，确定攻击面

首先，应该充分理解所要分析测试的设备业务情况，可以通过以下方式：

查询官方资料，获取官方提供的文档以及辅助程序；

浏览设备相关官方或第三方论坛；

简单使用设备，熟悉设备功能；

上网查阅其他用户使用情况，收集已在网上报告的问题。

例如，当前大部分 IoT 设备由设备硬件、移动 APP 以及云端三大部分组成，根据前文介绍，需要从以下几个角度分析潜在的测试点：

(1) 设备硬件

确定设备固件版本号信息；

官网是否提供固件下载；

设备当前是否可更新固件；

设备对外开放的端口号；

设备是否可以拆解；

本地串口是否可连接，登陆是否需要密码认证；

(2) 移动 APP

移动 APP 具有哪些功能；

APP 与设备之间通信方式；

APP 与云端之间通信方式；

通信协议是否加密；

APP 是否加固，确定逆向难度；

(3) 云端

云端 API 接口，确定云端提供的服务功能；

云端与设备通信方式；

云端与 APP 通信方式；

通信协议是否加密：

云端潜在业务逻辑漏洞；

云端潜在框架、编码漏洞；

三：常见分析过程

3.1 端口扫描，确定服务

设备配置完成后，应该扫描端口，确定后台提供的服务，在后续测试中，若能发现服务漏洞，进一步利用就有可能远程控制设备。

例如，若发现设备开放了 23 端口，提供 Telnet 服务，则可以通过分析固件，找到 Telnet 用户名密码，从而作为后门利用，远程登录设备。

若发现设备开放了 80 端口，提供 HTTP 服务，则可以通过 WEB 渗透的方式，测试是否存在注入、命令执行、越权、Webshell 上传等漏洞。

3.2 通信分析

通信分析的目的是确定通信过程是否加密，是否存在劫持的可能性，以及能否实施重放攻击。

通信分析首先要确定设备、APP、云端三者之间的通信协议，判断通信是否加密，可否抓包、劫持流量等。

APP 与云端一般通过 HTTP、HTTPS 通信，分析中应判断通信流量是否加密，可否抓包劫持通信数据；

设备与云端一般采用 MQTT、XMPP、CoAP 等协议通信，也会使用 HTTP、HTTPS 通信；

APP 与设备之间通信一般采用物联网无线协议，如 ZigBee、Zwave 以及蓝牙等。

在设备创始状态下，APP 向设备下发配置信息时，需要使用设备发现相关的协议，如 UPnP、mDNS 等。

确定 APP 与设备之间的通信协议后，即可确定无线通信频段，然后借助无线设备抓取该频段的数据包，进一步分析通信行为，目前常用的方式是 SDR，外加 USRP、HackRF 等硬件设备。

3.3 串口调试

IoT 设备中有一些配置信息是写在 ROM 里头的，只有当设备通电运行后才会加载到内存中，这部分信息通过静态分析固件是获取不到的。

通过串口，可以从后台进入系统，查看系统运行后的配置信息，获取到所需要的敏感信息，如用户名密码、服务配置等。

在无法通过官网或固件更新等方法获取固件的情况下，可以通过串口提取固件。

具体的串口确定及接线可参考网络资料。

3.4 固件提取及分析

在 IoT 设备安全测试中，固件程序是最重要的分析点，应该尽最大努力获取到设备固件程序。

获取到固件后，通过 Binwalk 对固件解包，首先通过静态分析，分析系统配置文件等信息，查找是否存在漏洞或可利用后面。其次，通过 QEMU 模拟固件运行环境，使用 IDA 或 gdb 动态调试，确定漏洞，测试 poc 和 exp。

固件提取和分析可参考网络资料。

3.5 APP 分析

IoT 测试中，手机 APP 占据了很大一部分，APP 漏洞可以导致越权访问设备、恶意绑定或解绑设备、远程控制设备等严重问题。

APP 分析技术内容较多，这里就不一一赘述了。

3.6 测试云端 API 和 Web 服务

除了硬件设备、移动 APP 之外，云端 API 和 WEB 服务是 IoT 安全测试中另一个重要的组成模块，可关注的测试点有：

云端所提供的功能，判断是否存在业务逻辑漏洞；

云端与 APP 以及设备之间的通信；

WEB 渗透，测试服务漏洞。

四：物联网设备的常见安全漏洞

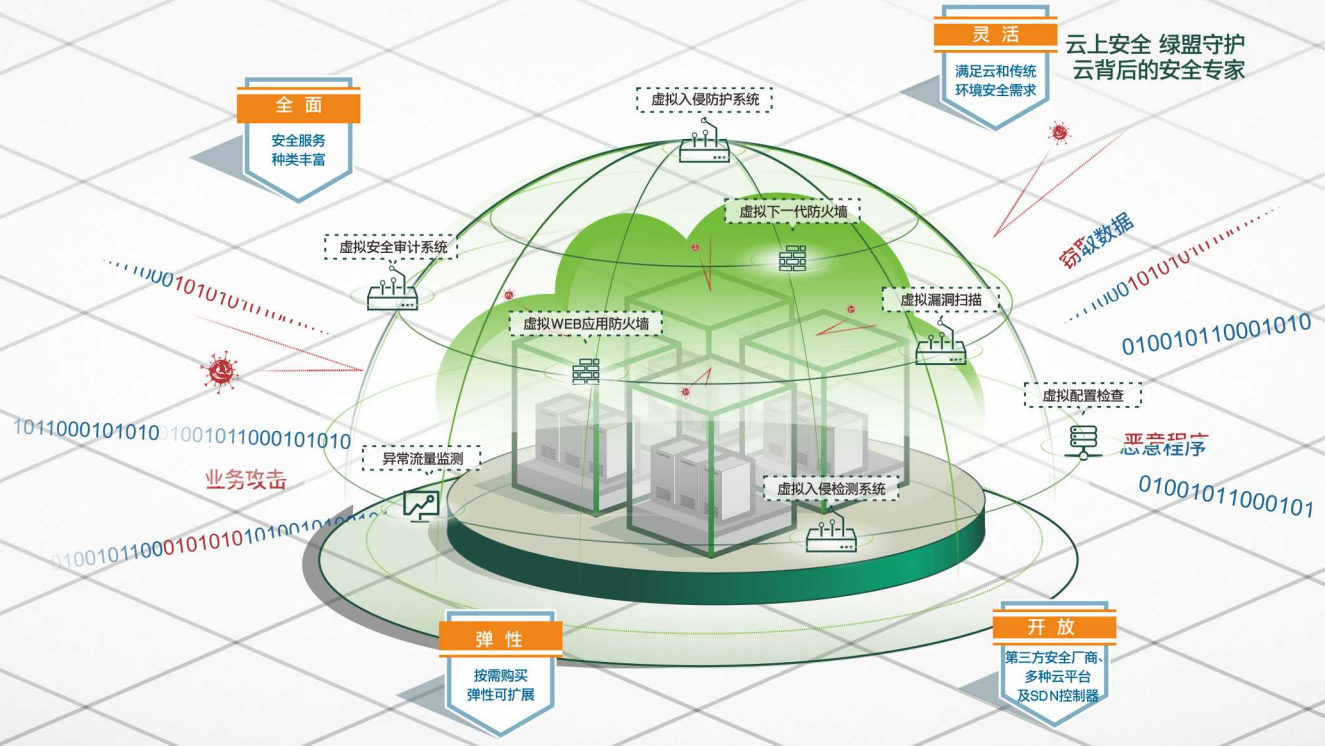
IoT 安全漏洞 Top10 如下：

编号	漏洞分类	安全评估点
I1	不安全的 WEB 接口	是否允许使用弱密码 账号锁定机制 是否存在 XSS、SQLi、CSRF 等 Web 漏洞 是否使用 HTTPS 保护传输信息 是否可以修改用户名密码修改 是否部署 waf 保护
I2	认证不足	认证要求强密码 多用户环境，具有角色隔离、权限控制功能 如可能，部署双因素认证方案 密码恢复机制 是否具有要求使用强密码选项 密码过期强制修改 是否可以修改默认用户名密码
I3	不安全的网络协议	网络服务对堆栈溢出、Fuzzing、DoS 不做响应 开发测试端口是否关闭
I4	缺乏传输加密	设备间以及设备与云端通信加密 是否使用加密方案，是否避免使用专用协议 是否有防火墙选项可用
I5	隐私	收集到的个人信息数量 个人数据是否加密保护 确保数据去掉标识或匿名化
I6	不安全的云端接口	云端安全漏洞(API 接口以及基于云的 WEB 接口) 不允许使用弱密码 具备账号锁定机制 是否使用双因素认证机制 是否存在 XSS、SQLi、CSRF 等漏洞 使用加密传输 是否具有要求使用强密码选项 密码过期强制要求修改 是否可以修改默认用户名密码

编号	漏洞分类	安全评估点
I7	不安全的移动端接口	不允许使用弱密码 具有账号锁定机制 是否部署双因素认证机制（如 Apple Touch ID） 是否使用加密传输 是否具有要求使用强密码选项 密码过期强制要求修改 是否可以修改默认用户名密码 可收集到的个人信息数量
I8	安全配置不足	是否具有密码安全选项（如密码长度要求 20 个字符以上或使用双因素认证） 是否具有加密选项（如默认使用 AES-128 的情况下，可以选择使用 AES-256） 是否具有安全日志记录机制 是否具有安全报警与通知机制
I9	不安全的软件 / 固件	具有固件更新机制，并且漏洞发现后可以及时更新 更新文件加密，更新数据传输加密 使用签名文件，安装前签名验证
I10	弱物理安全	设备使用最少数量的外部接口（如 USB 接口） 是否可以使用非预设的方法访问，例如通过不必要的 USB 端口访问 是否禁用未使用的物理接口，如 USB 接口 是否将管理员权限限制到本地接口

NSFOCUS NCSS
绿盟云安全解决方案

安全护“云”，随需而动



方式灵活	能力丰富	形态多样	开放性
提供了多种引流方式（SDN API／策略路由等）可以适用于传统和云计算网络	提供了从预防、检测、防护，到响应等丰富的安全能力	不限于虚拟安全产品，也支持传统设备	兼容云平台、SDN控制器及第三方安全厂商产品

THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

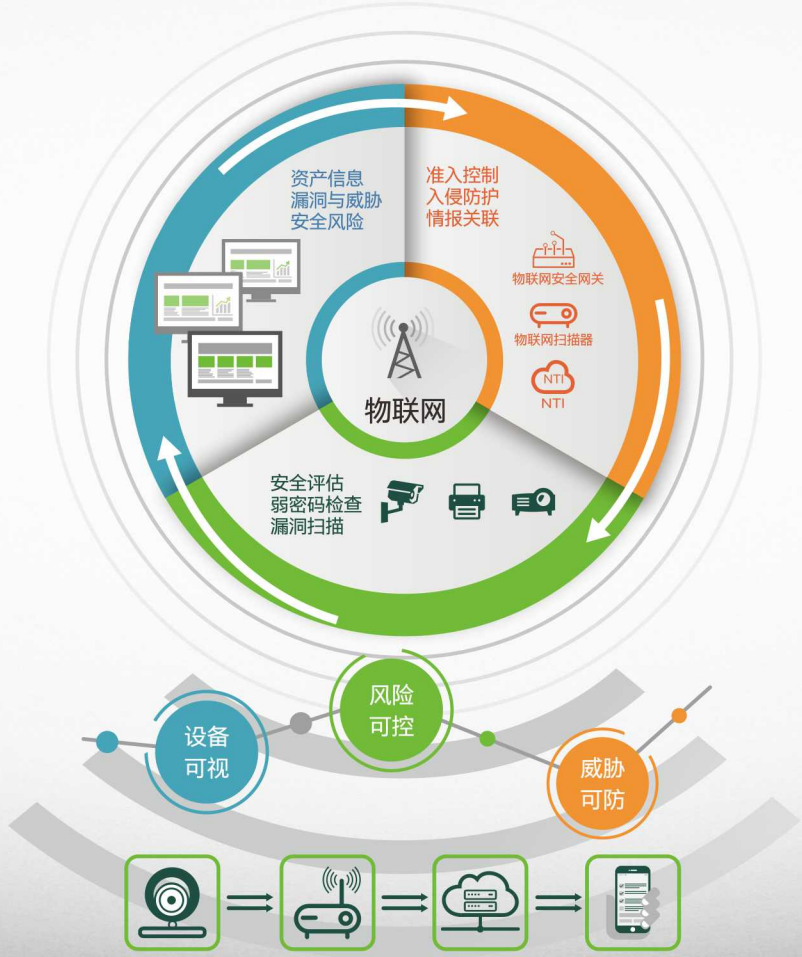
客户支持热线：400-818-6868

NSFOCUS绿盟科技

NSFOCUS IOT-AP

物联网安全分析解决方案

万物互联，安全为先



THE EXPERT
BEHIND GIANTS
巨人背后的专家

多年以来，绿盟科技致力于安全攻防的研究，为政府、运营商、金融、能源、互联网以及教育、医疗等行业用户，提供具有核心竞争力的安全产品及解决方案，帮助客户实现业务的安全顺畅运行。在这些巨人的背后，他们是备受信赖的专家。

客户支持热线：400-818-6868

NSFOCUS绿盟科技