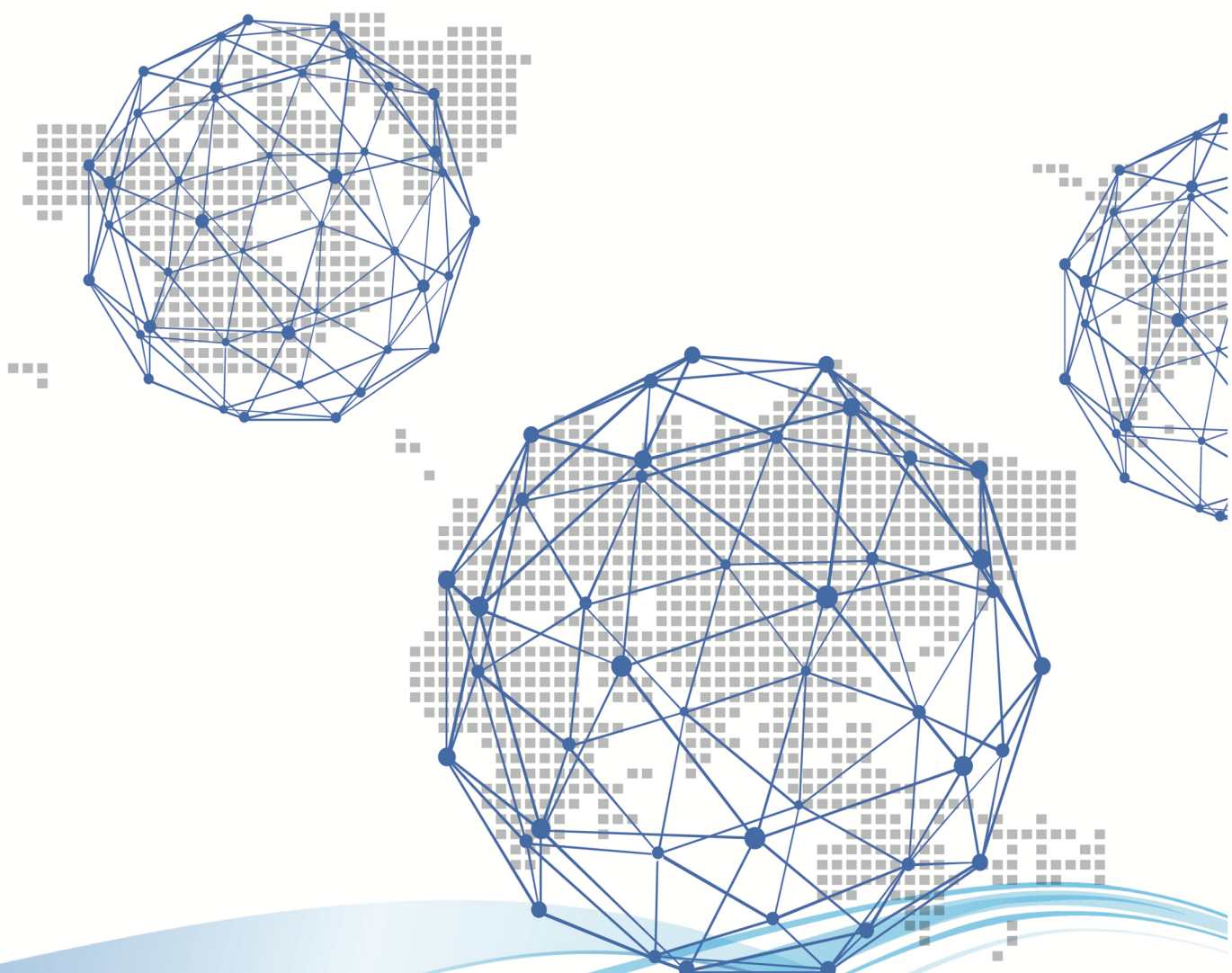
2017
物联网安全研究报告

薄明霞 唐洪玉 张星 张克雷 田金英 刘文懋 桑鸿庆 编著



中国电信 CHINA TELECOM
安全帮 anquanbang.net
NSFOCUS

中国电信
CHINA TELECOM

2017 物联网安全研究报告

薄明霞　唐洪玉　张　星　张克雷　田金英　刘文懋　桑鸿庆　编著

中国电信 CHINA TELECOM | 安全帮 anquanbang.net　NSFOCUS

联合出品

前 言

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。

物联网是继计算机、互联网之后的又一新的信息科学技术，目前，世界主要国家已将物联网作为抢占新一轮经济科技发展制高点的重大战略，我国也将物联网作为战略性新兴产业，在 2016 年国家“十三五”规划指出：要积极推进物联网发展，推进物联网感知设施规划布局，发展物联网开环应用，加快物联网基础设施建设和应用推广已经上升到了国家战略层面。

然而在物联网迅猛发展的同时，物联网安全成了产业痛点。为进一步加强物联网安全建设，向社会提供有关物联网安全状况的权威数据，中国电信安全帮携手北京神州绿盟信息安全科技股份有限公司（以下简称“绿盟科技”）联合发布《2017 物联网安全研究报告》。

报告主要包括 4 部分。

第一部分采用分层架构思想，由底而上的分析物联网安全风险，提出各层安全需求，并对物联网典型行业应用的安全风险进行分析。

第二部分针对物联网安全状况进行分析，包括物联网资产暴露情况分析、2017 十大物联网安全事件分析、2017 十大物联网恶意软件分析，揭示物联网安全防护的必要性和紧迫性。

第三部分针对物联网安全问题，提升物联网安全总体防护水平，给出物联网安全体系架构及解决方案。

第四部分从物联网安全产业发展趋势、物联网安全新技术探索两个方面对物联网安全发展进行展望，同时给出了物联网安全建设的发展建议。

本报告在编写过程中参考了大量资料，吸取了多方的宝贵意见和建议，在此深表感谢。报告的编写和发布得到相关单位的大力支持，我们在此表示衷心的感谢！欢迎广大读者批评、指正。

目 录

第一部分　物联网安全风险分析

第二部分　物联网安全现状分析

第三部分 物联网安全防护体系

第四部分 物联网安全发展展望

第一部分
物联网安全风险分析

第一章

物联网安全概述

物联网是信息技术发展到一定阶段的产物，是全球信息产业和技术的又一次飞跃。物联网的发展非常迅速，市场潜力巨大。但物联网给我们的工作和生活带来便捷的同时，也带来了风险。相比 PC 互联网和移动互联网时代，物联网应用的多样性和复杂性大大增强，而安全性和复杂性是成正比的，这也就使得物联网时代的安全问题变得更加严峻。物联网的信息安全问题是关系物联网产业能否安全可持续发展的核心技术之一，必须引起高度重视。

1.1　物联网概述

物联网是继计算机、互联网与移动通信网络之后的一个新兴网络技术，被视为继计算机和互联网之后的第三次信息技术革命。

物联网概念的正式提出要追溯到 2005 年 11 月 17 日的信息社会世界峰会上，国际电信联盟发布了《ITU 互联网报告 2005：物联网》，正式提出了“物联网”的概念。

物联网作为新技术，定义千差万别。目前一个普遍被大家接受的定义是：物联网是通过使用射频识别（Radio Frequency Identification，RFID）、传感器、红外感应器、全球定位系统、激光扫描器等信息采集设备，按约定的协议，把任何物品与互联网连接起来，进行信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的一种网络。

简而言之，物联网就是“物物相连的互联网”。这里面有两个层面的意思：第一，物联网的核心和基础仍然是互联网，是在互联网基础上的延伸和扩展的网络；第二，其用户端延伸和扩展到了任何物品与物品之间进行信息交换和通信。

与传统的互联网相比，物联网具有以下三个主要特征 [1]。

（1）全面感知

全面感知，即利用 RFID（射频识别）、传感器、二维码等随时随地获取物体的信息，RFID、传感器是物联网的主要应用工具。“感知”是物联网的核心。物联网是具有全面感知能力的物品和人所组成的，为了使物品具有感知能力，需要在物品上安装不同类型的识别装置，例如：电子标签（Tag）、条形码与二维码等，或者通过传感器、红外感应器等感知

其物理属性和个性化特征。利用这些装置或设备，可随时随地获取物品信息，实现全面感知。

（2）可靠传递

数据传递的稳定性和可靠性是保证物 - 物相连的关键。为了实现物与物之间信息交互，就必须约定统一的通信协议。由于物联网是一个异构网络，不同的实体间协议规范可能存在差异，需要通过相应的软、硬件进行转换，保证物品之间信息的实时、准确传递。

（3）智能处理

物联网的目的是实现对各种物品（包括人）进行智能化识别、定位、跟踪、监控和管理等功能。这就需要智能信息处理平台的支撑，通过云计算、人工智能等智能计算技术，对海量数据进行存储、分析和处理，针对不同的应用需求，对物品实施智能化的控制。

物联网作为战略性新兴产业，在各国政府的大力推动下，正在迎来建设高峰，许多国家都分别制定了具体的发展计划，并制定了相关政策。到 2016 年，物联网产业的发展已经超越国家边界，在很大程度上是一种全球行为。

物联网技术正在尝试将生活中的每一件物品，大到电视、冰箱，小到镜子、水杯，甚至汽车都可以联网，越来越多的医疗器械和其他设备也开始嵌入互联网功能。物联网应用逐步渗透到各行各业，智能交通、智能家居、智能物流、环境保护、农业生产、工业监控、医疗保健、政府工作、公共安全等。物联网在加速落地、快速成熟，万物互联的时代正在到来。

1.2 物联网架构简介

物联网是一个非常复杂、融合了多种技术的网络，根据信息生成、传输、处理和应用的原则，可以将物联网的层次结构自下而上划分为 4 层，即感知层、网络层、平台层、应用层。在某些框架中，尽管平台层与应用层可能被视为同一逻辑层进行处理，但从信息处理的角度考虑，将应用层独立出来更容易建立合理架构，特别是越来越多的公有云服务商提供了面向物联网应用的物联网平台服务。

感知层是物联网发展和应用的基础，负责信息的感知和采集，感知节点可为 RFID 装置、传感器、图像捕捉装置、GPS 或智能手机、激光扫描器等，尤其以 RFID 阅读器和传感器为主。多个传感器节点之间还能形成无线传感器网络（Wireless Sensor Network，WSN）。

网络层主要通过移动通信网、互联网、卫星网等网络基础设施，实现对感知层信息的接入，并将数据传输到物联网平台服务。

平台层由多个具有不同功能的处理平台组成，负责根据应用需求从感知数据中挖掘用于控制和决策的数据，并转化成不同的格式，便于多个应用系统共享。数据处理过程具有智能性和协同性。

应用层是物联网系统和用户的接口，负责向用户提供个性化业务、身份认证、隐私保护和向处理层提供用户操作指令。物联网的应用覆盖智能交通、智能家居、智能物流、环境保

护、农业生产、工业监控、医疗保健、政府工作、公共安全等行业和领域。

1.3　物联网安全概述

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。物联网将许多原本与网络隔离的设备连接到互联网中，大大增加了设备遭受攻击的风险。其次，不同类型的物与物之间是可能存在联系的，攻击某一节点，就可能会殃及另一个节点，将影响转移、扩大。最后，物联网安全的棘手不仅在于“大”，还在于“多”和“杂”。诸多物联网设备每天生成的海量数据对大规模数据处理提出了很大的挑战；不同的物联网设备的处理性能、网络协议、电池续航和生产厂商都有很大差别，很难应用统一的安全防护措施。

物联网安全事件从个人、家庭、社会到国家层出不穷。物联网设备、网络、应用面临严峻的安全挑战。例如，很多网络摄像头、路由器等物联网设备直接暴露在互联网上，这些设备可能存在弱口令、漏洞等安全风险，因此可能被恶意代码感染，成为僵尸主机（Bot）。这些受感染的设备一方面会继续感染其他设备，构成僵尸网络（Botnet）；另一方面，接受C&C 控制端的指令，在某刻发动大规模 DDoS 攻击，造成很严重的破坏和影响。近几年接连出现了多个此类僵尸网络，如 Mirai、Hajime、Remaiten、Persirai、IoT_reaper 等。2016 年 9 月 20 日，Mirai 僵尸网络针对法国网站主机 OVH 的攻击打破了 DDoS 攻击记录，其攻击流量达到 1.1Tbit/s，最大达到 1.5Tbit/s；2016 年 10 月 21 日，美国域名服务商 Dyn 遭受大规模 DDoS 攻击，其中重要的攻击源确认来自于 Mirai 僵尸网络，美国东海岸地区遭受大面积网络瘫痪；2016 年 11 月 28 日，德国电信遭遇断网时间，攻击源来自 Mirai 僵尸网络的新变种。相比于 Mirai 主要借助设备的弱口令进行传播，2017 年 9 月出现的 IoT_reaper 则不再依赖于破解设备的弱口令，而是对物联网设备的漏洞进行攻击，使得入侵几率大大提高。虽然到目前为止，IoT_reaper 构成的僵尸网络并未发动大范围的攻击，但其存在的威胁让人担心。

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，考虑到物联网覆盖的领域之广、接入设备器件的之海量、应用地域和设备供应商标准之分散，物联网时代的应用多样性和复杂性已大大增强，而安全性和复杂性也是呈正比增长，这就使得物联网时代的安全问题变得更加严峻。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。种种安全风险提示我们：万物互联，安全先行。

第二章

物联网安全风险分析

为了更好地阐述物联网安全特性，首先需要对物联网进行安全风险分析，在分析物联网的安全性时，对应物联网的 4 个逻辑层，即感知层，网络层、平台层、应用层，探讨物联网各层次面临的安全问题。

2.1 感知层安全风险及需求分析

物联网感知层的主要功能是实现对信息的采集、识别和控制，由感知设备以及网关组成。感应设备包括型设备包括 RFID 装置、各类传感器 (如红外、超声、温度、湿度、速度等)、图像捕捉装置 (摄像头)、全球定位系统 (GPS)、激光扫描仪、可能融合部分或全部上述功能的智能终端以及网关设备等。感知层是物联网信息和数据的来源，达到对数据全面感知的目的。相对互联网来说，物联网感知层是新事物，而且数量、种类众多，感知节点呈现多源异构性，通常情况下功能简单、携带能量少，相对于传统移动网络而言，物联网中的终端设备往往处于无人值守的环境中，缺少了人对终端节点的有效监控，终端节点更具有脆弱性，将面临更多的安全威胁。

（1）感知层面临的安全挑战 [2]

- 终端在户外、分散安装、易被接触到又没有纳入管理，导致物理攻击、篡改和仿冒；
- 终端驱动的不可信，可能会泄密和被控制；
- 操作系统或软件过时，漏洞无法及时修复；
- 考虑成本问题，终端资源、计算能力受限，防病毒等传统的保护手段和高安全技术可能无法应用。

（2）感知层的安全威胁

针对物联网感知层的攻击越来越多，包括物理攻击、伪造或假冒攻击、信号泄露与干扰、资源耗尽攻击、隐私泄露威胁等。

物理攻击，攻击者对传感器等实施的物理破坏，其使物联网终端无法正常工作，攻击者也可能通过盗窃终端设备并通过破解获取用户敏感信息，或非法更换传感器设备导致数据感

知异常，破坏业务正常开展。

伪造或假冒攻击，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、发起 DoS 攻击等。

信号泄露与干扰，攻击者对传感网络中传输的数据和信令进行拦截、篡改、伪造、重放，从而获取用户敏感信息或者导致信息传输错误，业务无法正常开展。

资源耗尽攻击，攻击者向物联网终端发送垃圾信息，耗尽终端电量，使其无法继续工作。

隐私泄露威胁， RFID 标签、二维码等的嵌入，使物联网接入的用户不受控制地被扫描、定位和追踪，极容易造成用户个人隐私泄露。

（3）感知层的安全需求 [3]

针对上述的挑战，感知层的安全需求可以总结为如下几点。

- 物理安全防护

需要采取措施保护终端避免失窃，或被攻击者物理上获得或复制。针对有卡的设备，需要采取措施防止将 UICC 或者 SIM 卡非法操作。针对无卡的设备，需要采取措施防止信任状非法操作。当末端节点和卡的物理安全防护被破坏后，应无法正常使用。

- 访问控制

需要采取访问控制的方式，防止终端被逻辑攻破，泄露用户或终端信息。

- 认证

物联网终端、物联网接入网关需要支持物联网网络 / 平台层的认证功能。

- 不可抵赖性

物联网终端在读写数据时要提供记录，以便识别用户或其他设备访问或使用了网络或业务。

- 机密性

终端所存储的数据或所传送的数据要加密。

- 数据完整性

需要采取措施防止终端数据被篡改。

- 可用性

需要防病毒软件，防火墙等措施，使终端不会因为攻击导致无法工作。

- 私密性

需要保护终端所存储的用户隐私，并防止用户信息泄露。

2.2　网络层安全风险及需求分析

万物互联意味着网络要支撑多样的业务和庞大的流量，需要用到各类通信技术，目前应

用于物联网的网络层的通信技术包括 Wi-Fi、RFID、蓝牙、ZigBee 等短距离无线通信技术和传统的互联网、移动通信网、以及近年来发展起来的低功耗广域网（LPWAN）。物联网的网络层主要是将感知层采集的信息通过传感网、移动网和互联网进行信息的传输，由于物联网中采集的信息需通过各种网络的融合，将信息实时准确地传递出去，物联网的传输网络是一个多网络叠加的开放性网络，传输途径会经过各种不同的网络，会面临比传统网络严重的安全问题。

（1）网络层面临的安全挑战 [2]

- 无线协议本身缺陷，如缺乏有效认证，可能导致接入侧泄密。
- 封闭的物联网应用 / 协议无法被安全设备识别，被篡改和入侵后无法及时发现。
- 未加密的通信过程容易发生劫持、重放、篡改和窃听等中间人攻击。
- IP 化后面临 IP 体系的安全问题，如来自互联网的攻击和入侵。

（2）网络层的安全威胁

物联网的网络层面临的主要威胁包括以下方面。

网络层协议漏洞，网络层功能本身的实现中需要的技术与协议（网络存储、异构网络技术等）存在安全缺陷，特别在异构网络信息交换方面，易受到异步、合谋攻击等。

海量终端设备的威胁，随着物联网业务终端的日益智能化，物联网应用更加丰富，同时也增加了终端感染病毒、木马或恶意代码所入侵的渠道，这些病毒可通过接入层进入传输网络，增加网络层的安全风险。此外，物联网中的设备传输的数据量较小，一般不会采用复杂的加密算法，保护数据，从而可能导致数据在传输的过程中遭到攻击和破坏。

异构网络融合问题，物联网的承载网络是一个多网络叠加的开放性网络，随着网络融合的加速及网络结构的日益复杂，网络层中的网络通信协议不断增多。当数据从一个网络传递到另一个网络时会涉及到身份认证、密钥协商、数据机密性与完整性保护等诸多问题，因而面临的安全威胁将更加突出。

无线传输问题，物联网大量使用无线传输技术，数据传输面临更大的威胁。攻击者可随意窃取、篡改或删除链路上的数据，并伪装成网络实体截取业务数据及对网络流量进行主动与被动的分析。

DDoS 攻击问题是网络安全未来核心，全 IP 化的移动通信网络和互联网及下一代互联网将是物联网网络层的核心载体。对于一个全 IP 化开放性网络，将面临 DDoS 攻击、假冒攻击等网络安全威胁，且物联网中业务节点数量将大大超过以往任何服务网络，在大量数据传输时将使承载网络堵塞，产生拒绝服务攻击。假冒基站攻击即攻击者通过假冒基站骗取终端驻留其上，并通过后续信息交互窃取用户信息。攻击者在攻破物联网网络之间的通信后，窃取用户隐私及敏感信息造成隐私泄露。

（3）网络层的安全需求 [3]

- 总体安全需求

物联网的通信网络的总体安全需求不得低于一般通信网络的安全需求。

- 机密性

需要保证物联网通信网络的信令的机密性，可以保证物联网通信网络的数据的机密性。

- 完整性

需要保证物联网通信网络的信令的完整性。

- 隐私性

需要保证物联网通信网络用户身份、物联网终端位置等的隐私性。

- 认证的一般需求

物联网终端和网络的相互认证可以采用多种认证方式。

- 组认证

物联网终端可以基于组的形式进行认证，来避免大规模终端认证造成的网络信令拥塞并防止可能的 Dos 攻击；

群组设备的认证可以通过认证代理来完成，如物联网接入网关或主设备。

- 密钥的一般需求

物联网终端 / 物联网接入网关和网络侧实体可以根据组认证来共享某些密钥。

物联网终端 / 物联网接入网关和网络侧可以根据不同的协议层共享相应协议层的密钥。

用多种鉴权物联网终端 / 物联网接入网关可以生成全部协议层的密钥，也可以只生成部分协议层的密钥。

- 可用性

确保物联网通信网络的信息和服务在任何时间都可以提供给合法用户，可通过数据备份等实现。

2.3　平台层安全风险及需求分析

物联网是一个规模庞大的信息计算系统，这个系统需要一个强有力的平台提供计算和存储服务支撑其应用需求。物联网平台能够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。

平台层由多个具有不同功能的处理平台组成，负责根据应用需求从感知数据中挖掘用于控制和决策的数据，并转化成不同的格式，便于多个应用系统共享。数据处理过程具有智能性和协同性，物联网平台从底层到高层可分为 4 大平台类型：终端管理平台、连接管理平台、应用开发平台、业务分析平台。

终端管理平台（DMP）：对物联网终端进行远程监控、系统升级、故障排查、生命周期管理等。

连接管理平台（CMP）：负责对物联网连接配置和故障管理、网络资源用量管理、连接

资源管理、套餐变更、号码 /IP 地址 /MAC 资源管理等。

应用开发平台（AEP）：提供应用开发和统一数据存储的 PaaS 平台，提供应用开发工具、中间件、数据存储、业务逻辑引擎、对接第三方 API 等。

业务分析平台（BAP）：对业务数据进行分类处理、分析并提供视觉化数据分析结果，通过实时动态分析，监控设备状态并予以预警，或通过机器学习，对业务进行分析预测。

平台层融合了更多的先进技术，包括云计算、大数据、人工智能等，以满足对整个庞大的物联网进行信息运算和交互的需求。平台层承上启下，是物联网产业链枢纽，物联网的大规模、分布式、多业务类型使物联网平台层安全面临新的挑战。

（1）平台层面临的安全挑战

- 平台层所管理的设备分散、繁多，设备的升级过程和安全状态等难以管理；
- 新的通信协议可能带来平台层的安全问题和漏洞，比如畸形攻击、泛洪攻击等；
- 新平台自身漏洞和 API 开放等容易引入新的风险；
- 越权访问导致隐私和安全凭证等重要数据有被泄露的风险；
- 应用丰富、数据中心出口多，DDoS 等网络攻击风险高。

（2）平台层的安全威胁

物联网平台层面临的威胁非常广泛，基本上互联网、云计算、大数据等所面临的威胁都会被物联网平台层系统继承。主要安全威胁包括以下方面。

- 平台易遭受攻击的问题

物联网的各种应用数据分布存储在云计算平台、大数据挖掘与分析平台、以及各业务分析平台中进行计算和分析，由于其用户信息资源的高度集中，容易成为黑客攻击的目标，容易导致数据泄露、恶意代码攻击等安全问题。

- 虚拟化安全问题

物联网平台通过在其部署的服务器、存储、网络等基础设施之上搭建虚拟化软件系统以实现高强的计算能力，虚拟化和弹性计算技术的采用，使得用户的边界模糊，带来一系列比在传统方式下更突出的安全风险，如虚拟机逃逸、虚拟机镜像文件泄露、虚拟网络攻击、虚拟化软件漏洞等安全问题。

- 平台系统可用性问题

用户的数据和业务应用处于云平台中系统中，其安全性依赖于平台的可用性，对平台的服务连续性、SLA 和 IT 流程、安全策略、事件处理和分析等提出了挑战。另外，当发生系统故障时，如何保证系统快速恢复也成为一个重要问题。

- 平台漏洞问题

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。

- 数据安全问题

用户的数据存储、处理、网络传输等都与云计算系统有关，包括如何有效存储数据以避免数据丢失或损坏，如何对多租户应用进行数据隔离，如何避免数据服务被阻塞等，以及发生故障后，数据能快速恢复。此外，黑客可能向物联网的大数据平台注入脏数据，导致系统误判，产生数据污染问题。

（3）平台层的安全需求

- 基础环境安全

保障物联网平台的基础环境安全包括以下几类。

物理安全。物理安全是指云计算所依赖的物理环境安全。云计算在物理安全上面临多种威胁，这些威胁通过破坏信息系统的完整性、可用性或保密性，造成服务中断或基础设施的毁灭性破坏。

计算环境安全。计算环境安全是指构成云计算基础设施的硬件设备的安全保障及驱动硬件设施正常运行的基础软件的安全。

存储安全。数据集中和新技术的采用是产生云存储安全问题的根源。云计算的技术特性引入了诸多新的安全问题，多租户、资源共享、分布式存储等这些因素加大了数据保护的难度，增大了数据被滥用和受攻击的可能。因此，用户隐私和数据存储保护成为云计算运营者必须解决的首要问题。

虚拟化安全。重点应考虑虚拟化软件和虚拟服务器安全，多租户环境下相互隔离防止未经授权访问。

- 系统可用性

平台发生故障，不影响服务的正常提供，并且可以对应用故障进行安全隔离。

- 接入安全

对接入平台的用户具备严格身份鉴别和访问控制；支持设备接入过程安全传输的能力；并能够阻断异常接入。

- 数据安全

物联网中的应用都是数据密集型的，传感设备与云平台之间、用户与云平台之间和用户与传感设备之间时刻都在进行数据交互，一旦数据丢失和损坏都将造成难以预料的后果。物联网云端保存着所有终端搜集上来的信息数据，以及据此分析获得的新数据信息。云平台必须采取适当的安全策略保证物联网中数据的完整性、保密性和不可抵赖性。

- API 安全

保证 API 的安全，防止非法访问，保证第三方插件安全，保证 API 软件的完整性。

2.4 应用层安全风险及需求分析

应用层为用户提供丰富的服务，应用领域覆盖智能交通、智能家居、智能物流、环境保护、农业生产、工业监控、医疗保健、政府工作、公共安全等行业和领域。应用层直接接触外界，因此是最敏感的地区，具有大量隐私信息，因此也是风险较严重的地带。

（1）应用层面临的安全挑战

- 如何实现用户隐私信息的保护，同时又能正确认证用户信息；
- 不同访问权限如何对同一数据库内容进行筛选；
- 信息泄露如何追踪问题；
- 恶意代码以及各类软件系统自身漏洞、可能的设计缺陷、黑客、各类病毒是物联网应用系统的重要威胁；
- 物联网涉及范围广，目前海量数据信息处理和业务控制策略方面的技术还存在着安全性和可靠性的问题。

（2）应用层的安全威胁

应用层威胁主要包括下面几种形式：病毒、蠕虫、木马、不受欢迎应用程序、远程攻击、人员威胁等。

- 病毒、蠕虫和木马

感染后，破坏应用系统正常运行的程序，使之无法正常使用。

- 不受欢迎应用程序

Rootkit：Rootkit 是一种恶意程序，它能在隐瞒自身存在的同时赋予 Internet 攻击者不受限制的系统访问权。

广告软件：广告软件是可支持广告宣传的软件的简称。

间谍软件：此类别包括所有在未经用户同意 / 了解的情况下发送私人信息的应用程序。潜在的不安全应用程序。许多合法程序用于简化联网计算机的管理。但如果使用者动机不纯，它们也可能被恶意使用。

- 远程攻击

DoS 攻击：DoS 拒绝服务攻击，是一种使计算机资源对其目标用户不可用的攻击。受到 DoS 攻击的计算机通常需要重新启动，否则它们将无法正常工作。

DNS 投毒：通过 DNS（域名服务器）投毒方法，黑客可以欺骗任何计算机的 DNS 服务器，使其相信它们提供的虚假数据是合法、可信的。然后，虚假信息将缓存一段时间。

端口扫描：通过端口扫描控制网络主机上开放的计算机端口。

TCP 去同步化：TCP 去同步化是 TCP 劫持攻击中使用的技术。

SMB 中继：SMBRelay 和 SMBRelay2 是能够对远程计算机执行攻击的特殊程序。

ICMP 攻击：ICMP（Internet 控制消息协议）是一种流行且广泛使用的 Internet 协议，它主要用于联网计算机发送各种错误消息。

（3）应用层的安全需求

应用层安全需求存在共性及差异。应用层个性化的安全需求还需针对各类智能应用的特点、使用场景、服务对象及用户特殊要求进行有针对性的分析研究，共性的安全需求包括以下几点。

身份认证：物联网服务器或者末端节点的真实身份的认证，防止身份伪造和末端节点克隆等攻击。

业务认证：物联网应用服务器对末端节点之间需要进行业务认证，为防止假冒用户使用未授权的业务或者合法用户使用未定制的业务，用户请求使用业务前必须经过严格的业务认证。

组认证：物联网应用通常对应大量的末端节点，这些末端节点可能构成一个组，物联网应用服务器需要提供对这些末端节点进行组认证的能力。

隐私保护：保护行为或者通信信息不泄密，这些信息包括通信内容、用户地理位置和用户身份等。

完整性：考虑到网络中恶意末端节点可能注入、篡改应用层消息。因此，物联网应用层需要避免未授权的删除、插入和复制操作。由于物联网需要通过多种异构网络进行通信，这些网络间的安全机制相互独立且并不一致，因此需要为应用通信提供端到端的完整性保护。

机密性：在物联网网络中各种数据和消息只能让授权用户查看，机密性保护可以避免非授权访问和应用层数据内容非授权阅读。由于物联网需要通过多种异构网络进行通信，这些网络间的安全机制相互独立且并不一致，因此需要为应用通信提供端到端的机密性保护。

密钥的安全性：采用动态下载密钥参数与动态更新登录密码的方式来实现。

防抵赖：提供不可抵赖性机制，保证通信各方对自己行为及对行为发生的时间的不可抵赖性。例如通过进行身份认证和数字签名、数字时间戳等机制避免对行为发生的抵赖。

抗重放：提供抵御重放攻击的机制。

可用性：确保物联网应用层的信息和服务在任何时间都可以提供给合法用户，可通过数据备份等实现。

2.5　物联网典型行业应用风险点简析

物联网应用涉及国民经济和人类社会生活的方方面面，主要对物联网典型应用的安全风险进行分析，主要典型应用涉及以下 8 个方面：车联网、智能家居、智能监控、智能物流、智能穿戴、智慧医疗、智慧能源和智能路灯。

2.5.1 车联网

车联网（Internet of Vehicles）是以车内网、车际网和车载移动互联网为基础，按照约定的通信协议和数据交互标准，在车 -X（X：车、路、行人及互联网等）之间进行无线通信和信息交换的大系统网络，是能够实现智能化交通管理、智能动态信息服务和车辆智能化控制的一体化网络，是物联网技术在交通系统领域的典型应用，如图 2-1 所示。

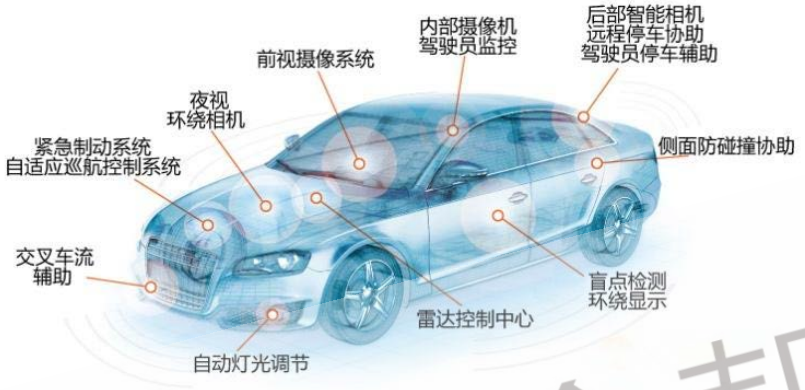


图 2-1 车联网

车联网涉及较多行业，整个产业链包括汽车车厂、电信、互联网、汽车经销商、电子元器件厂商以及保险公司等，可分为 4 大环节：零配件，基础软件供应商提供包括触控屏、芯片、传感器、地图等零配件，软件包括底层地图数据、语音库、操作系统等；车载智能设备供应商整合零配件及软件，供应车载智能设备；移动互联网通信运营商提供车联网通信服务；平台运营商提供包括导航、应急救援、娱乐、汽车维护保养等服务。

从 2013 年至今，BAT 纷纷完成移动端的地图应用布局，以此为入口，进入车联网，进一步引爆国内车联网市场。

车联网可以通过碰撞预警、电子路牌、红绿灯警告、网上车辆诊断、道路湿滑检测为司机提供即时警告；可以通过城市交通管理、交通拥塞检测、路径规划、公路收费、公共交通管理，改善人们的出行效率；可以为人们提供餐厅、拼车、社交网络等娱乐与生活信息服务 [4]。

随着车联网技术的逐渐普及，车载系统越来越受到消费者的青睐，但随之而来的安全隐患也初露端倪，部分车载系统遭到入侵与干扰。例如：

美国菲亚特克莱斯勒汽车公司的召回事件。黑客利用互联网技术，侵入一辆行驶中切诺基吉普车的“Uconnect”系统，远程操控了该车的加速和制动系统、电台和雨刷器等设备。

宝马 Connected Drive 数字服务系统遭入侵事件，黑客能够利用该漏洞以远程无线的方式侵入车辆内部，并打开车门。

特斯拉 Model S 遭入侵事件，网络安全专家通过 Model S 存在的漏洞打开车门并开走，同时还能向 Model S 发送“自杀”命令，在车辆正常行驶中突然关闭系统引擎。

此外，奥迪、保时捷、宾利和兰博基尼等大众旗下品牌的 Megamos Crypto 防护系统也

遭到攻破。

总结来看，车联网系统有如下几个点容易受到攻击。

- 汽车端：信息娱乐系统、T-box、内部 CAN 网络、外部的钥匙；
- 手机、手表上的 APP；
- 与 CAN 网络连接的 OBD 设备；
- TSP 后台所在的云端服务器；
- 通信过程，包括从车机、T-box 到后台的通信，APP 到后台的通信等。

车联网的未来发展趋势是不可逆的，当车联网成为未来汽车市场的主流产品之后，由此带来的安全问题恐怕会更频繁出现。车辆的安全直接关乎我们的生命安危，所以说车联网安全问题不容忽视。

2.5.2　智能家居

智能家居（Smart Home）是以住宅为平台，利用综合布线技术、网络通信技术、安全防范技术、自动控制技术、音视频技术将家居生活有关的设施集成，构建高效的住宅设施与家庭日程事务的管理系统，提升家居安全性、便利性、舒适性、艺术性，并实现环保节能的居住环境，如图 2-2 所示。

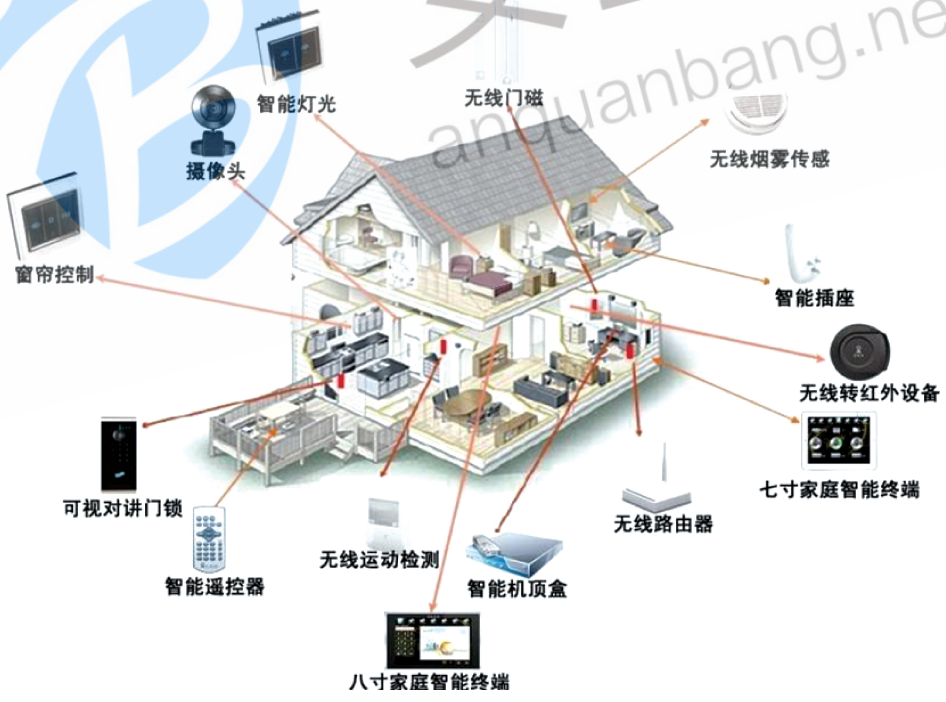


图 2-2　智能家居

智能家居是在互联网影响下物联化的体现。智能家居通过物联网技术将家中的各种设备（如音视频设备、照明系统、窗帘控制、空调控制、安防系统、数字影院系统、影音服务器、影柜系统、网络家电等）连接到一起，提供家电控制、照明控制、电话远程控制、室内外遥

控、防盗报警、环境监测、暖通控制、红外转发以及可编程定时控制等多种功能和手段。与普通家居相比，智能家居不仅具有传统的居住功能，兼备建筑、网络通信、信息家电、设备自动化，提供全方位的信息交互功能，甚至为各种能源费用节约资金[5]。

智能家居最初的发展主要以灯光遥控、电器远程控制和电动窗帘控制为主，随着行业的发展，智能控制的功能越来越多，控制的对象不断扩展，控制的联动场景要求更高，其不断延伸到家庭安防报警、背景音乐、可视对讲、门禁指纹控制等领域，智能家居目前几乎可以涵盖所有传统的弱电行业，市场发展前景诱人[6]。

随着智能家居使用度的提高，对于智能家居存在的问题也越来越多，尤其是物联网设备的“隐私安全”问题越来越突出。例如：小米某智能家电存在漏洞可被渗透导致整个智能家居网络沦陷，当前智能家居产品作为智能硬件，之所以会被攻击或远程控制，主要有两大原因：

（1）智能硬件大多通过无线 Wi-Fi 连接，给黑客入侵设备提供了渠道；

（2）智能硬件系统普遍存在安全漏洞，黑客可以利用漏洞夺取硬件控制权。

2.5.3 智能监控

智能监控是嵌入式视频服务器中，集成了智能行为识别算法，能够对画面场景中的行人或车辆的行为进行识别、判断，并在适当的条件下，产生报警提示用户，如图 2-3 所示。

图 2-3 智能监控

智能行为识别包括物体识别、越界识别、轨迹跟踪、遗留或丢失物体识别、车速测量、车牌识别、流量统计、逆行告警、涂鸦行为识别、打架等反常行为视频等。

智能监控主要包括视频监控，通过获取监控目标的视频图像信息，对视频图像进行监视、记录、回溯，并根据视频图像信息人工或自动地做出相应的动作。

从功能上讲，视频监控可用于安全防范、信息获取和指挥调度等方面，可以提供生产流程控制、大型公共设施的安防，也能为医疗监护、远程教育等提供各种服务。

从应用领域上看，视频监控在各行各业都得到了广泛的应用，除了档案室、文件室、金库、博物馆等重要部门的监视和报警，在公共场所进行安全监控，在其他经济和生活领域进

行管理和控制也是必不可少的[7]。

具体应用实例有以下领域。

金融领域：营业大厅监控、金库的监控、自动提款机及自助银行监控等。

电信 / 电力领域：交换机房、无线机房、动力机房等的远程监控、变电站、电厂等的远程无人值守监控。

商业市场：商场的保安监控、超级市场的出入口监控、码头、货柜、大型仓库的监管等。

军事领域：基地安防、公安侦破、监狱法庭管理等。

交通领域：高速公路收费管理、交通违章和流量监控、公共交通车辆牌照管理、公路桥梁铁路机场等场所的远程图像监控等。

社区物业管理：住宅小区、办公室的安全防范、智能大厦、停车场的无人监控等。

家庭应用：只需在现有的家庭微机上增加 USB 摄像头和相应的软件系统，就可实现数字化家庭监控系统。

由于摄像头的直观可视性和低成本，很多家庭用户和企业用户都安装了大量摄像头用于视频监控。然而，在以开放分享为特征的互联网环境下，由于视频监控系统的漏洞和个人、企业自身安全防护技术的缺失，企业和家庭极易遭受黑客的非法攻击进而引发数据和隐私的泄露，由此造成巨大的经济损失。目前，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。

2.5.4　智能物流

智能物流是利用条形码、射频识别技术、传感器、全球定位系统等先进的物联网技术，通过信息处理和网络通信技术平台，广泛应用于物流业运输、仓储、配送、包装、装卸等基本活动环节，实现货物运输过程的自动化运作和高效率优化管理，提高物流行业的服务水平，降低成本，减少自然资源和社会资源消耗，如图 2-4 所示。

图 2-4　智能物流

物联网为物流业将传统物流技术与智能化系统运作管理相结合提供了一个很好的平台，能够更好、更快地实现智能物流的信息化、智能化、自动化、透明化、系统化的运作模式。

智能物流在功能上强调的是智能感知、优化决策与智能反馈。首先，智能感知主要体现在通过射频识别、卫星定位于红外线等高新技术动态获取存储包装、仓储、物流配送与车辆每一环节的数据信息，对物流对象进行跟踪、定位等。其次，优化决策主要指在物流配送与管理的过程中，应用信息处理技术与数据挖掘，分析和挖掘商品信息、物流数据与客户需求等相关信息，计算和决策仓储位置与配送的路径，实现物流存储与配送的决策智能化。智能反馈是指在物品物流配送过程中，送货方与收货方都可以在物流配送的整个过程及时了解物品的准确位置与状态。在此过程中可以应用感知网、物流管理系统与红外线客户与管理提供实时的物流运行状态的信息，进而可以获取物品在整个物流过程中每一环节的信息[8]。

随着智能物流发展，物流领域也越来越依赖网络传输信息的安全性能，物流信息在网络传输过程中存在的安全隐患主要有两方面：

（1）信息泄露，海量的快递意味着海量个人信息的流出，无论是下单还是配送单信息，都使得个人信息安全站在危险边缘；

（2）黑客攻击，黑客以各种非法手段对物流信息网络进行拦截、窃取、篡改、盗用、监听，往往会给商户带来重大损失，这也是物流信息安全的最大隐患。

2.5.5 智能穿戴

智能穿戴也称智能可穿戴设备，是一种可以穿在身上或贴近身体并能发送和传递信息的计算机设备，它可以利用传感器、射频识别、全球定位系统等信息传感设备，接入移动互联网，实现人与物随时随地的信息交流，如图 2-5 所示。

图 2-5 智能穿戴

智能可穿戴设备分为生活健康、信息咨询和体感控制类设备。其中，生活健康类的设备有运动、体侧腕带及智能手环；信息资讯类的设备包括智能手表和智能眼镜；体感控制类的设备包括 Kinect、LeapMotion 等体感控制器 [9]。

可根据穿戴部位的不同，将智能穿戴设备分为智能手表类、智能手环类、智能眼镜头盔类、智能服装类和智能鞋类。其中，手环类主要以一系列运动记录手环、臂环为主；手表类主要有 Pebble 等辅助类智能设备；眼镜类主要是以 Google Glass 等为主的新型智能终端；智能服装类主要由 Geek 开发，几乎没有正式发布的产品，例如可以通过转化太阳能为电子设备充电的比基尼、靴子等。

智能穿戴设备将人与互联网连接的更加紧密，但是和 PC 与智能手机诞生初期一样，智能穿戴设备当前也存在着许多的安全盲点，可能导致用户数据和个人隐私泄露。智能穿戴设备主要问题有以下几个。

（1）自身形态较小，安全防护性不高，易被破解。目前市面可穿戴设备普遍形态较小，功能实现主要依靠多种传感器来进行工作，没有芯片或系统层，本身在软硬件上就缺乏保护性；

（2）蓝牙和 Wi-Fi 等接口是可穿戴设备可能被攻击的突破口，由于目前可穿戴设备普遍的设计逻辑都是通过蓝牙、Wi-Fi 等接口连接智能手机，再借助 GPS 或手机端的 APP 上进行数据同步。在这其中的各个环节，都有可能造成数据的泄露以及设备被攻克。

现在，智能穿戴设备还处于发展初期，企业需要意识到，不能只看眼前利益，而疏忽对用户数据的保护，不顾长远发展。安全问题或许不是智能穿戴设备发展的绊脚石，但必将会是穿戴产品淘汰与否的重要指标。

2.5.6　智慧医疗

智慧医疗，简称 WIT120，通过打造健康档案区域医疗信息平台，利用先进的物联网技术，实现患者与医务人员、医疗机构、医疗设备之间的互动，逐步达到信息化。智慧医疗由三部分组成，分别为智慧医院系统、区域卫生系统以及家庭健康，如图 2-6 所示。

图 2-6　智慧医疗

智慧医疗是最近兴起的专有医疗名词，通过打造健康档案区域医疗信息平台，利用最先进的物联网技术，实现患者与医务人员、医疗机构、医疗设备之间的互动，逐步达到信息化。在不久的将来，医疗行业将融入更多人工智慧、传感技术等高科技，使医疗服务走向真正意义的智能化，推动医疗事业的繁荣发展。在中国新医改的大背景下，智慧医疗正在走进寻常百姓的生活。

智慧医疗的应用主要集中在三个场景。

首先，利用多种传感器设备和适合家庭使用的医疗仪器，自动或自助采集人体生命各类体征数据，在减轻医务人员负担的同时，能够获取更丰富的数据。

其次，采集的数据通过无线网络自动传输至医院数据中心，医务人员利用数据提供远程医疗服务，能够提高服务效率，缓解排队问题，并减少交通成本。

第三，数据集中存放管理，可以实现数据的广泛共享和深度利用，有助于解决关键病例和疑难杂症，能够以较低的成本对亚健康人群、老年人和慢性病患者提供长期、快速、稳定的健康监控和诊疗服务，降低发病风险，间接减少对稀缺医疗资源如床位和血浆的需求。

随着智慧医疗走入公众视野，越来越多的医疗数据实现了大数据化，但随之而来的，也带来了相应的风险。例如，美国亚利桑那州班纳健康中心（Banner Health Breach）遭到黑客入侵，370 万患者、员工及客户的个人信息数据遭到窃取。

总结来看，智慧医疗在如下几点存在安全隐患。

（1）电子病历，这是病人数据的标准，并高度简化记录存储、更新和检索。与此同时，网络犯罪领域出现了黑市，其中被盗医疗记录的售价高达每条 10 美元，这是信用卡记录价值的 10 到 20 倍。医疗记录通常包括社会安全号码，使用的药物和地址，可以帮助攻击者进行各种非法的攻击，比如勒索软件攻击；

（2）便携式设备 / 硬件，如跟踪生命体征的仪器等；

（3）医疗信息系统；

（4）对互联网开放的、可以连接到医疗机构网络系统的任何服务器（网络服务器、FTP 服务器、电子邮件服务器等），医疗机构的公共 Wi-Fi 热点；办公室的打印机；视频监控系统；SCADA 系统控制器；用于控制建筑物机械和电气部件的自动化系统（如建筑物管理系统）。

2.5.7 智慧能源

智慧能源就是充分开发人类的智力和能力，通过不断技术创新和制度变革，在能源开发利用、生产消费的全过程和各环节融入人类独有的智慧，建立和完善符合生态文明和可持续发展要求的能源技术和能源制度体系，从而呈现出的是一种全新的能源形式。简而言之，智慧能源就是指拥有自组织、自检查、自平衡、自优化等人类大脑功能，满足系统、安全、清洁和经济要求的能源形式，如图 2-7 所示。

图 2-7　智慧能源

物联网技术使得智能能源变成可能，随着物联网技术的发展，智能水表、智能电表、智慧燃气、太阳能控制器等应运而生。

智能水表是一种利用现代微电子技术、现代传感技术、智能 IC 卡技术对用水量进行计量，并进行用水数据传递及结算交易的新型水表，除了可对用水量进行记录和电子显示外，还可以按照约定对用水量进行控制。

智能电表是智能电网的智能终端，除了具备传统电能表基本用电量的计量功能以外，还具有双向多种费率计量功能、用户端控制功能、多种数据传输模式的双向数据通信功能、防窃电功能等智能化的功能，智能电表代表着未来节能型智能电网最终用户智能化终端的发展方向。

智慧能源的应用主要有三个方向：商业客户的管理、分布式太阳能和智能家居 [10]。

随着智慧能源的发展，其背后可能蕴含的安全隐患同样不容忽视。2017 年，欧洲与北美数十家能源机构遭俄罗斯黑客组织“蜻蜓”针对性的网络攻击，旨在窃取用户敏感数据 [11]。

总结来看，智慧能源面临的攻击威胁主要包括：

（1）针对硬件漏洞展开攻击；

（2）通过发布钓鱼电子邮件等手段进行诱导欺诈攻击；

（3）大规模 DDoS 网络攻击。

2.5.8　智能路灯

智能路灯又叫智能化路灯，或者智慧路灯、智慧照明，是采用物联网和云计算技术，对城市公共照明管理系统进行全面升级，实现路灯集中管控、运维信息化、照明智能化，如图 2-8 所示。

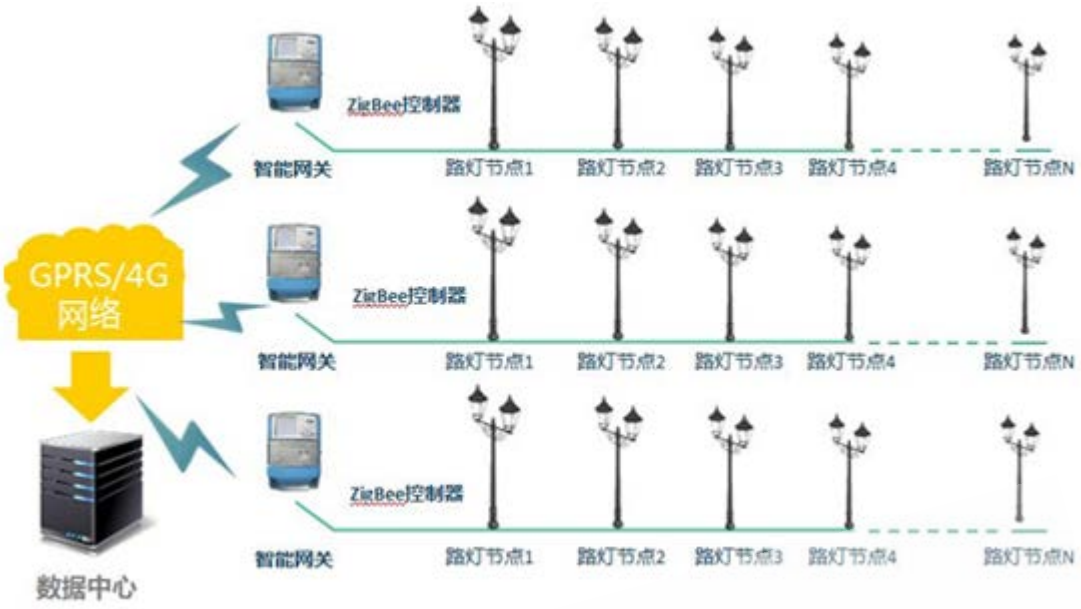


图 2-8　智能路灯

目前，根据道路照明专业委员会的统计，在全国 811 座城市中已有 263 座城市的道路灯管控采用了“无线三遥（遥控、摇信、遥测）智能化控制系统”。无论是在国家层面，还是在普通用户这里，大家对于智能控制的 LED 照明灯具的接受越来越广泛。在 LED 路灯方面，拥有智能控制系统的 LED 路灯一直是行业发展的主流方向。

路灯控制系统从最初的开关控制功能，逐渐演化到了监控节能控制功能，同时，各种新技术被用于路灯监控系统中。在路灯控制领域，主要有 PLC 技术 (电力载波通信技术)、ZigBee 无线通信技术以及 RS485 串口通信技术三种方式实现对路灯的控制 [12]。

随着物联网、下一代互联网、云计算等新一代信息技术的广泛应用，智慧城市已成为必然趋势。智慧路灯作为智慧城市建设中的重要组成部分，未来发展空间巨大，路灯的智能化改造势在必行。智能路灯给人类生活带来了各种各样的便利，但安全性问题也同样值得重视。例如，德国埃尔朗根一份最新研究报告显示，智能照明通信标准之一的 ZigBee-Light-Link（ZLL，它是 ZigBee 联盟针对照明行业开发的一种低功耗网状网无线通信技术）存在安全缺陷，该协议一旦被攻破就会导致整个照明系统被接管，智能灯泡将受攻击者掌控 [13]。

目前，物联网技术还处于初级发展阶段，并没有建立起一套完善的安全标准，同时由于网络天然的缺陷性，容易受到黑客攻击，因此集成大数据的智慧系统、智能云平台等的安全问题成为各界关注的焦点，这也是智能照明往前发展的一大绊脚石。智能系统的安全标准需要被认真看待，也需要照明企业、智能方案服务商、云平台等相关企业之间的通力合作。

第二部分
物联网安全现状分析

第三章

物联网资产暴露情况分析

智能设备的应用已经渐渐成为了日常生活不可或缺的一部分，可是在便利之余，物联网资产中暗藏的安全问题也不容小觑，物联网设备普遍存在暴露的情况。本章节概述了物联网相关的安全问题，并对暴露在互联网上的物联网资产进行了详细分析，用以揭示物联网安全防护的必要性和紧迫性，进而提高人们对物联网安全威胁的防范意识，同时也希望相关部门做好相应的安全加固并完善相应的防护机制，避免攻击者有机可乘。

3.1　概述

在物联网相关的安全问题越来越引发关注的背景下，对在互联网上暴露的物联网资产（即物联网设备与服务）进行分析和梳理是非常有必要的。一种可行的研究方法是通过网络空间搜索引擎去发现相关的物联网设备，形成面向物联网资产的威胁情报。

本章节将对全球及中国的物联网资产暴露情况进行分析，通过发布类似的报告，希望提高整个社会对物联网威胁的防范意识，也希望相关各界能提供相应的安全加固和防护机制，避免攻击者有机可乘。

需要说明的是，一个物联网设备暴露在互联网并不一定意味着这个设备存在问题，只能说明该设备存在被攻击甚至被利用的风险。比如一个设备通过用户名和密码可以被登录，如果用户使用了安全强度比较高的密码，则该设备便不存在弱口令的风险。但一旦设备暴露在互联网上，就增加了其攻击面，一旦在突发的安全事件中（如心脏出血等），其暴露的相关服务被发现存在漏洞，就有被攻破的风险。

本报告的所有数据均来自公开的网络空间搜索引擎 NTI[14]、Shodan[15] 和 ZoomEye[16]。

由于精力有限，很难保证涵盖到所有种类，对于所包含的类别，也很难保证数据百分之百的准确性。但在分析过程中，通过对三个搜索引擎（NTI、Shodan 和 ZoomEye）的数据综合分析，尽可能确保数据的全面性和准确性。希望能通过展示物联网设备在互联网的暴露情况，揭示物联网安全防护的必要性和紧迫性。

3.2 物联网设备暴露情况 分析

3.2.1 物联网设备暴露情况总览

观点 1：互联网上暴露的各类物联网设备中，路由器和视频监控设备暴露的数量最多。

智能设备的应用已经渐渐成为了日常生活不可或缺的一部分，可是在便利之余，物联网设备中暗藏的安全问题不容小觑。通过数据收集与分析，我们在图 3-1 中列出了若干暴露情况较为严重的物联网设备。

从全球分布来看，路由器暴露的数量超过了 4900 万台，远远高于其他物联网设备的暴露数量。视频监控设备的暴露数量超过了 1100 万台，高于防火墙、交换机等传统网络设备的暴露数量，仅次于路由器。打印机的暴露情况令人意外，暴露数量达到了 89 万台之多。

从国内分布来看，路由器的暴露数量达到了 1092 万台，视频监控设备的暴露数量达到 168 万台，打印机的暴露数量有 6 万台。

需要说明的是，所列的设备数量仅为网络空间搜索引擎识别出的结果，很多设备暴露出来的端口特征不明显，实际暴露的设备可能多于我们所统计结果，后面不再赘述。

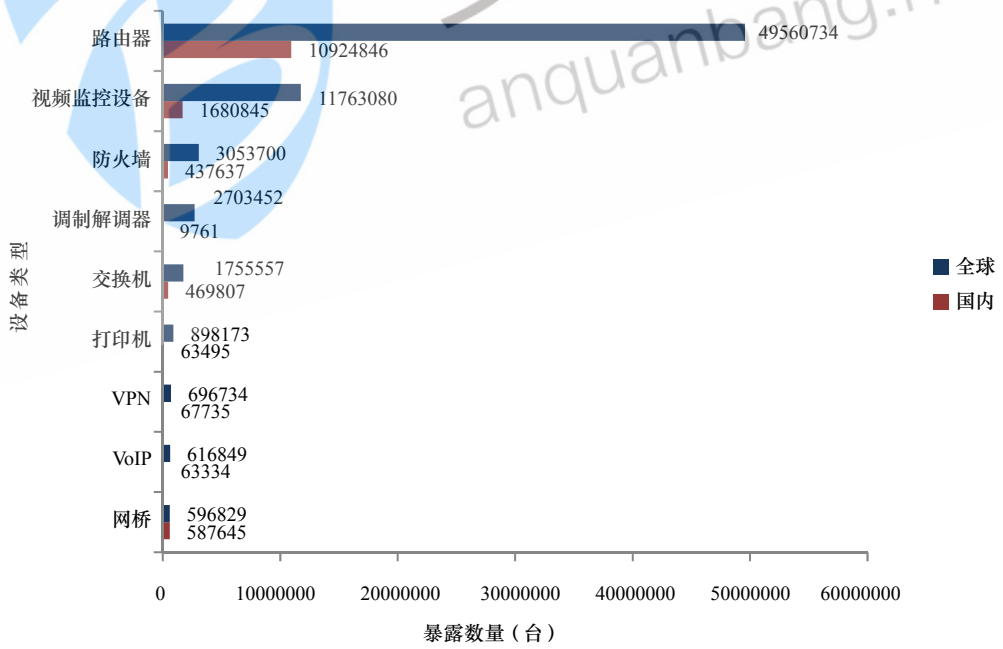


图 3-1 全球和国内物联网相关设备暴露情况

当然物联网设备不限于此。首先，有一些小众的设备（如门禁设备、恒温器和车辆调度系统等）或者某些工业控制领域的设备数量较少，图 3-1 中并未列出，我们会视情况在后续的报告中进行补充或更新；其次，有很大一部分物联网设备接入的是局域网，通过 NAT 方

式接入互联网，进而与物联网应用通信，由于这类设备隐藏在网关设备后面，不会暴露在互联网上。

接下来，我们将重点以路由器、视频监控设备和打印机为例，分别介绍这三类设备的厂商分布、地理分布和端口分布等情况，之后，会简单列举几个比较有特点的但分布数量较少的物联网设备。

3.2.2　路由器暴露情况分析

观点 2：全球范围内，华为路由器暴露的数量最多；国内范围内，水星、迅捷路由器暴露的数量最多。

在图 3-2 中，我们对路由器分厂商进行了统计。从各路由器厂商暴露在全球的设备数量来看，华为暴露的设备数量最多，占比达到 22%，AVM、MikroTik、水星和迅捷的全球暴露数量也都达到了 400 万台的规模。

从全球分布和国内分布的对比来看，华为、MikroTik、D-LINK 等在国内外均有一定的暴露，AVM 在国内几乎没有暴露。水星和迅捷路由器全球和国内暴露数量相差不大，这种情况出现的最大可能性是这两个厂商的路由器主要在国内销售。

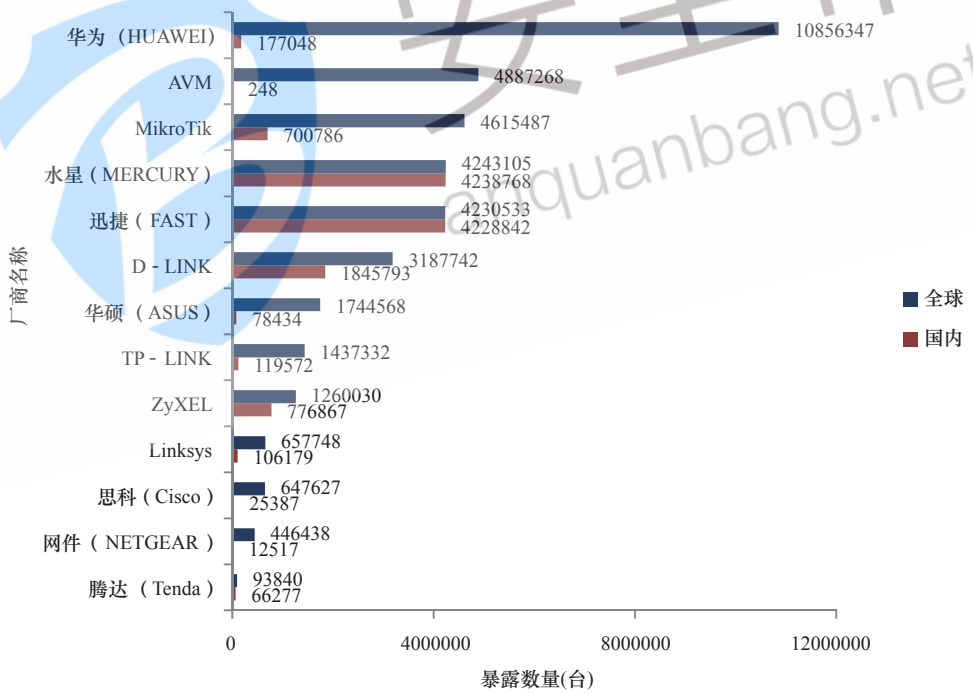


图 3-2　暴露的路由器厂商分布

观点 3：全球范围内，中国暴露的路由器数量最多；而在国内，二线城市暴露的路由器数量居多。

从全球分布来看（如图 3-3 所示），路由器类设备暴露数量最多的是中国，暴露总量超过了 1000 万台，占比达到 22%，其他国家均没有超过 500 万台。从国内分布来看（如图 3-4

所示），各城市的路由器暴露数量没有出现某个城市暴露数量远超于其他城市的情况。但是，路由器暴露数量非常多，在我们统计的城市中，暴露数量前十的城市均暴露了超过 20 万台的路由器，其中，福州、济南、长沙、郑州、南京的暴露数量超过了 50 万台。

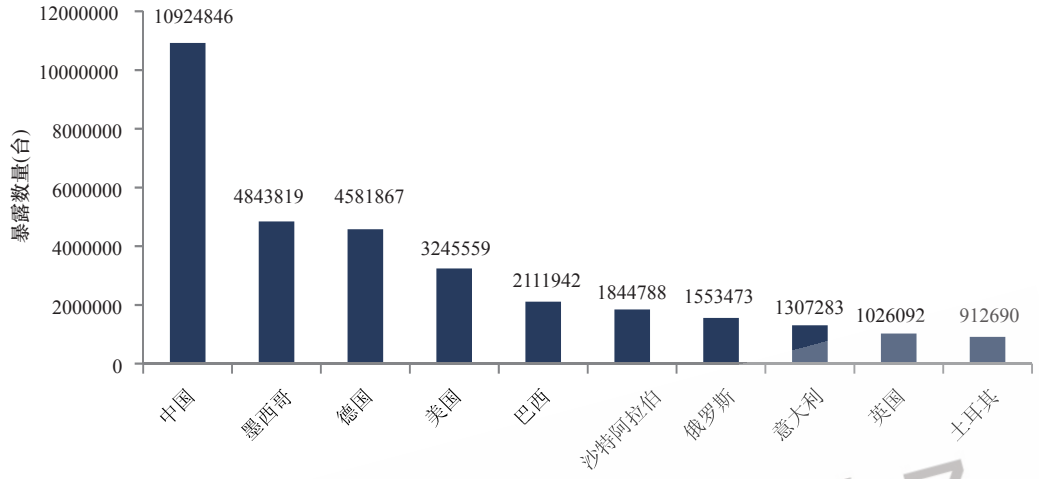


图 3-3　暴露的路由器国家分布

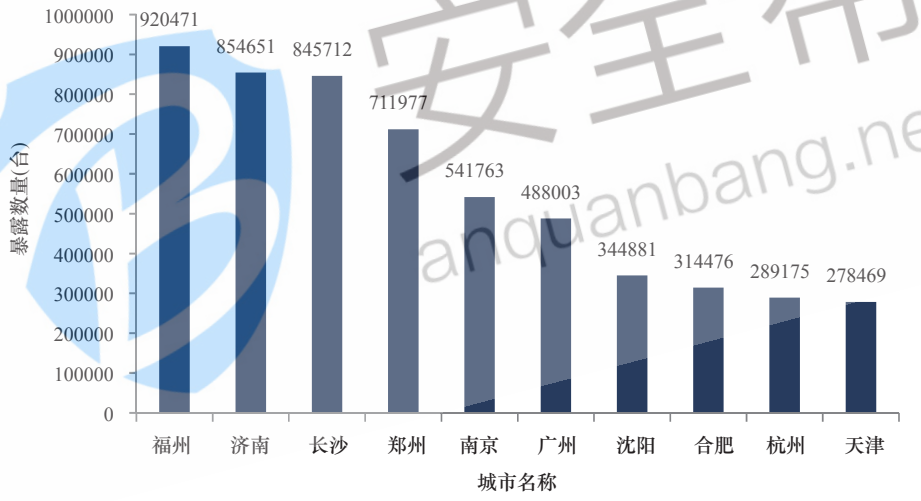


图 3-4　暴露的路由器城市分布（中国）

观点 4：全球范围内，暴露数量最多的服务依次是 HTTP、FTP、UPnP 和 TR-069；国内来看， 83% 的路由器开放了 UPnP 服务。

从全球分布来看，暴露最多的服务是 HTTP 服务，以端口 80、8080、8081 为主，暴露总量超过了 1400 万。

FTP 服务的端口为 21，暴露数量也超过了 1000 万。一般而言，FTP 服务器的配置文件中会有一个匿名登录的选项，为未登录用户提供浏览和下载服务。假设平均每个 FTP 服务开启匿名登录的概率为 1%，则超过 10 万个 FTP 服务存在信息泄露的风险；假设每个 FTP 服务提供 20GB 的空间，则意味着最多会有 2000TB 的数据暴露在了互联网上。

端口 7547 和 4567 的开放数量占路由器暴露总量的 18%，其对应的服务一般为 TR-069

协议[17]，即 CPE 广域网管理协议（CPE WAN Management Protocol，CWMP）。TR-069 定义了一套完整的网管体系结构，包括管理模型、交互接口及基本的管理参数，能够有效地实施对家庭网络设备的管理。在其网管模型中，用户终端设备为 CPE，图中开放 7547 和 4567 端口的路由器即为 CPE；此外，管理服务器称为自动配置服务器 (ACS)，负责完成对用户终端设备（CPE）的管理，如可实现远程对 CPE 的各种参数的配置修改、数据查看、固件版本升级、设备重启等。

需要说明的是，TR-069 的会话协议使用的是 HTTP1.1 协议，在关于路由器的统计分析中，为表示区分性，对于开放 HTTP 服务的路由器数量统计时，并未将开放 TR-069 服务的数量计算在内。这样区分后，路由器所开放 HTTP 服务对应的是路由器设备自身的管理平台服务，而 TR-069 服务对应的是路由器设备为便于其相应厂商管理所开放的服务。

Telnet 服务的端口为 23，提供了远程登录的功能，有将近 400 万个 Telnet 服务暴露在了互联网上。一旦攻击者通过 Telnet 服务登录到路由器，则意味着可经过该路由器连接到内部的局域网络，进而控制如智能家居中的摄像头等设备，可能威胁人们的隐私、财产和生命安全。

从国内分布来看，超过 80% 的路由器开放了 UPnP（Universal Plug and Play，通用即插即用）服务（对应 1900 端口）。UPnP 协议允许应用程序（或主机设备）自动发现前端的 NAT 设备，并根据需要自动请求 NAT 设备打开相应的端口，启用 UPnP 后 NAT 两端的应用程序（或主机设备）间可以自主交换信息，以实现设备间网络的无缝连接。当用户使用多人游戏，点对点连接，实时通信（如 Internet 电话、电话会议）或远程协助等应用程序的时候，可能需要启用 UPnP 功能。

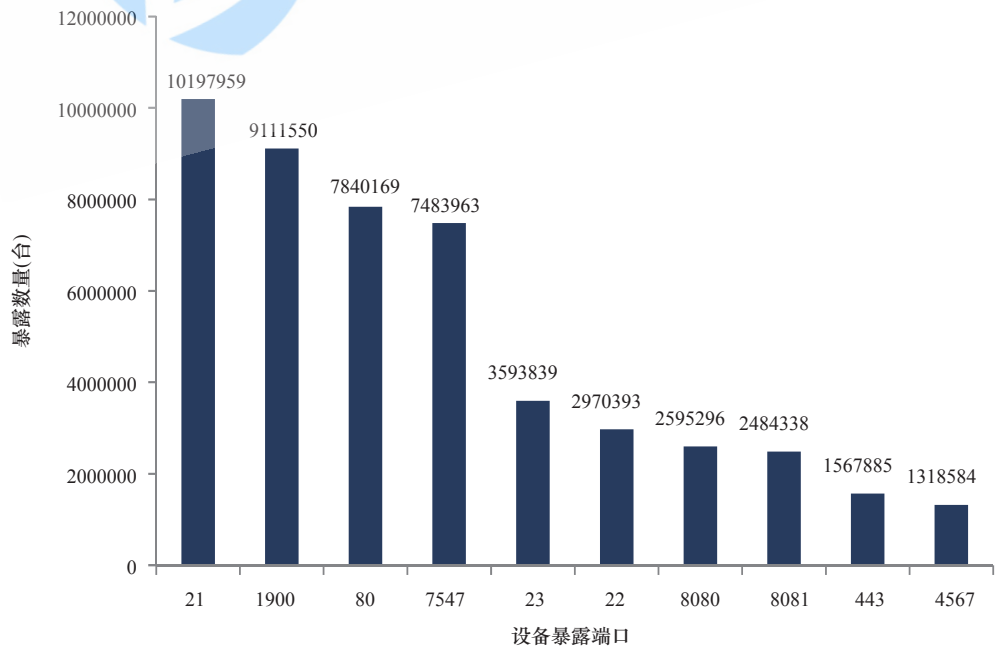


图 3-5　暴露的路由器按端口的分布情况（全球）

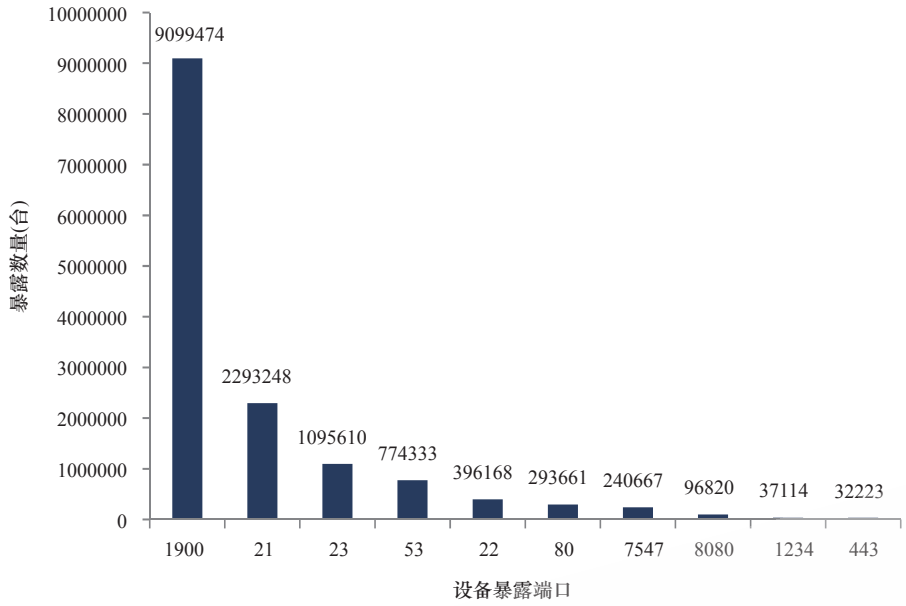


图 3-6　暴露的路由器按端口的分布情况（中国）

观点 5：全球范围内，80% 以上的暴露在互联网上的 TP-LINK 路由器开放了 HTTP 服务；国内来看，暴露在互联网的上 TP-LINK 路由器几乎全部开放了 HTTP 服务。

全球范围内，TP-LINK 路由器的暴露数量达到了 143 万台。从暴露端口的全球分布来看（如图 3-7 所示），80% 以上的路由器暴露了 HTTP 服务。在暴露出的 Top10 端口中，除端口 7547 对应的 TR-069 服务外，其余端口对应的均为 HTTP 服务。而从国内分布来看（如图 3-8 所示），TP-LINK 路由器暴露最多的端口为 80、8080 和 1080，总量达到了 3.6 万台。

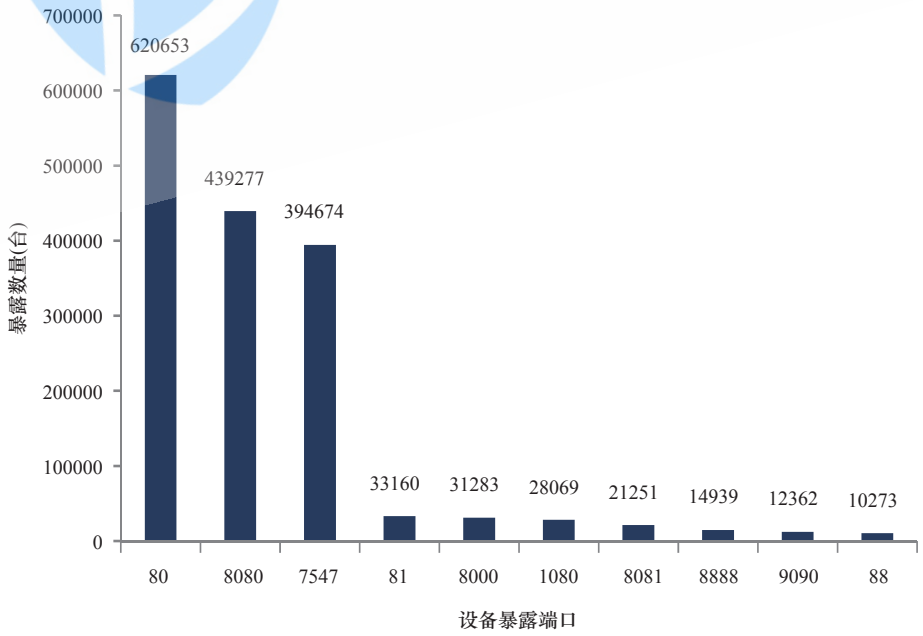


图 3-7　暴露的 TP-LINK 路由器按端口的分布情况（全球）

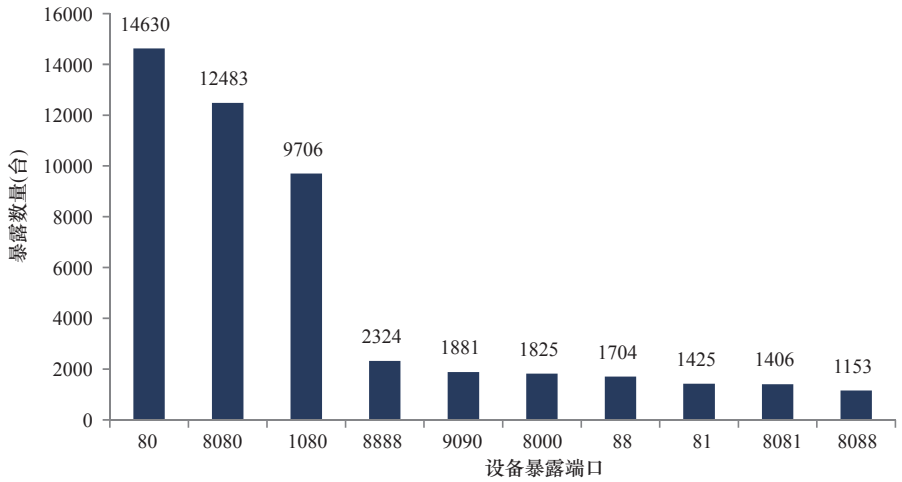


图 3-8　暴露的 TP-LINK 路由器按端口的分布情况（中国）

3.2.3　视频监控设备暴露情况分析

随着智慧城市的发展，视频监控设备应用场景愈加广泛，近年发生的一些物联网安全事件多与之有关，因而视频监控设备的暴露情况应得到足够的重视。本节主要对视频监控设备暴露情况进行统计和分析。

观点 6：海康威视和浙江大华两大厂商暴露数量较多，全球范围内，两大厂商占全球总暴露量的比例分别为 31% 和 14%；在中国范围内，该比例分别为 60% 和 13%。

图 3-9 是暴露在全球和国内的视频监控设备按厂商的分布情况。从全球分布来看，海康威视和浙江大华两家的视频监控设备暴露严重。暴露最多的视频监控设备是海康威视，总量超过了 365 万台；其次是浙江大华、D-Link 和 Cross 等厂商的视频监控设备，每家设备的暴露数量也都达到了百万量级。

从国内分布来看，海康威视和浙江大华暴露的设备多达 100 万台和 22 万台。

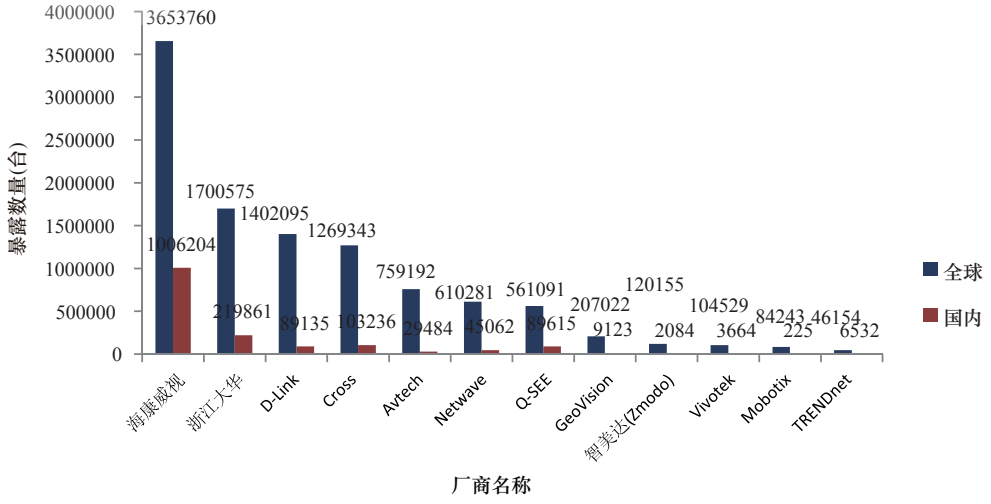


图 3-9　暴露的视频监控设备按厂商的分布情况

观点 7：全球范围内，美国和中国暴露的视频监控设备数量最多；中国范围内，暴露的视频监控设备大部分位于台湾。

从全球分布来看（如图 3-10 所示），互联网上暴露的视频监控设备主要集中在美国和中国，其次分别为巴西、越南、墨西哥等。暴露在美国和中国的视频监控设备数量，分别约占全球视频监控设备总量的 16% 和 14%。

从国内分布来看（如图 3-11 所示），互联网上暴露的视频监控设备主要集中在台湾，约占全国视频监控设备总量的 47%。

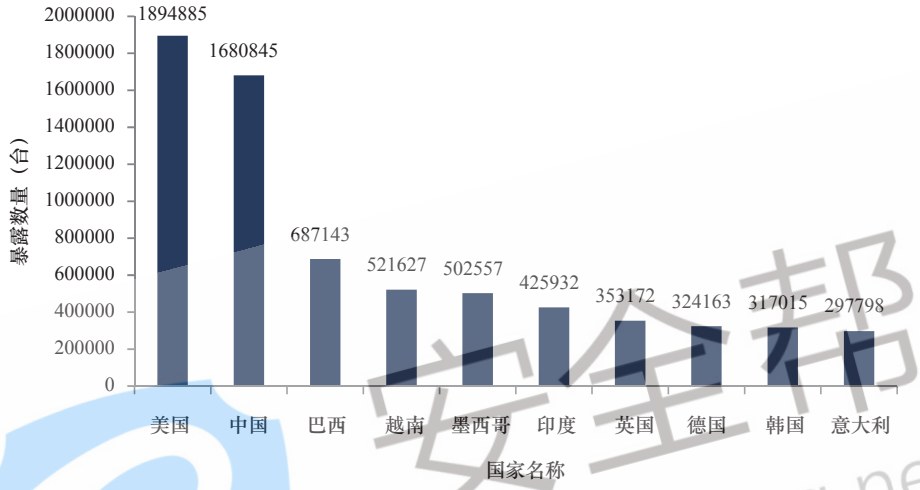


图 3-10　暴露的视频监控设备按国家的分布情况（全球）

图 3-11　暴露的视频监控设备按城市的分布情况（中国）

观点 8：视频监控设备暴露的 HTTP 服务数量最多，浙江大华私有协议、Telnet、RTSP 协议的暴露情况也比较严重。

图 3-12 和图 3-13 分别是暴露在全球和国内的视频监控设备按端口的分布情况。从服务分布上看，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）。全球范围内，HTTP 服务主要暴露在 80-82、88 和 8000 端口，这些端口的暴露令人意外，因为有安全意识的网络管理员一般会把涉及隐私和资料的 HTTP 服务开启在不常用的端口上，以防止端口扫描器探测。而这些端口的暴露数量排到了前十，事实上，视频监控设备的管理员缺乏基本的安全意识，RTSP 服务的全球暴露数量也超过了 67 万。RTSP 服务被用来实时传输流媒体，非常适合网络监控设备把视频流实时传输到前端进行实时显示，一般情况下，RTSP 服务默认开启的是 554 号端口。所以，视频监控设备在互联网上都会暴露出大量的 554 端口。

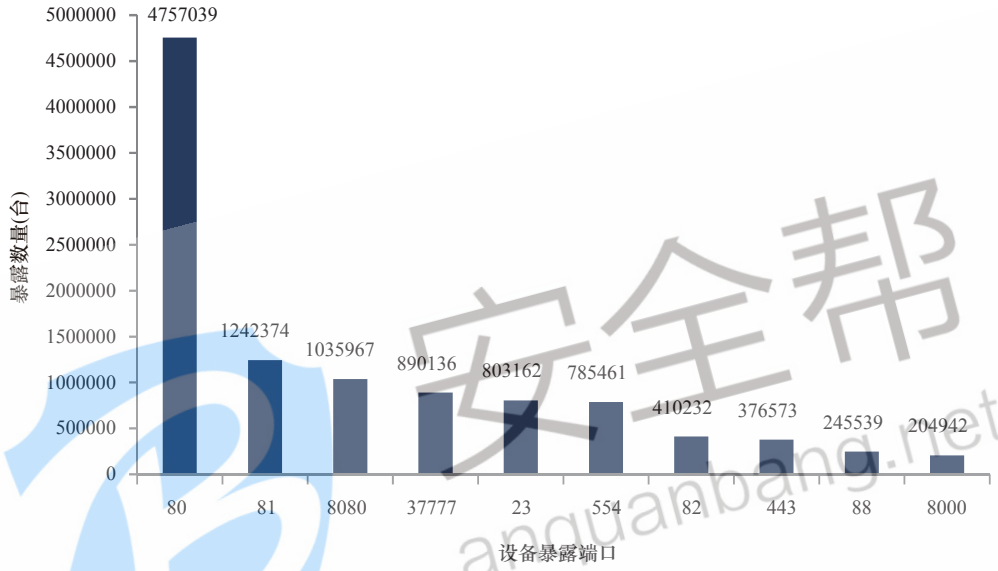


图 3-12　暴露的视频监控设备按端口的分布情况（全球）

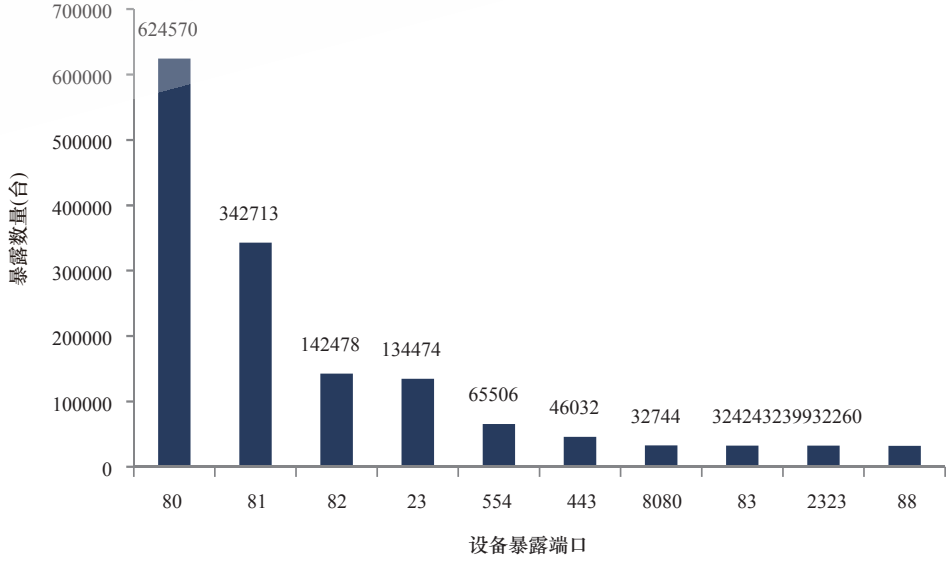


图 3-13　暴露的视频监控设备按端口的分布情况（中国）

假设来物联网设备存在弱口令的概率 P=1%（在物联网场景中，弱口令的现象比较严重，1% 其实是一个下限），那么将超过 9000 台视频监控设备存在成为僵尸主机的风险。假设每台设备可以拥有 10Mbit/s 的网络带宽，则最大可能制造出 90Gbit/s 的 DDoS 攻击。如果估计 P=10%，仅视频监控设备一类将可能制造出 900Gbit/s 的 DDoS 攻击。

3.2.4 打印机暴露情况分析

众所周知，打印机在商务、科研等场景中扮演着非常重要的作用，企业对支持移动设备打印的需求越来越大，也催生了越来越多支持 Wi-Fi 直连、NFC 打印、云打印等移动功能 [18] 的“智能”打印机。虽然打印机的攻击面较少，但同样也不容忽视。

2017 年 2 月，黑客攻入了台湾多所学校的打印机（其中惠普打印机数量占 73%，爱普生占 7%），并扬言如果学校不按照其要求付款，就发动攻击来瘫痪学校网络 [19]。事实上，有相当比例的打印机使用默认密码，部分打印机分配了外网网络地址，直接接入互联网，这些设备会直接暴露给攻击者。随着互联网 + 时代的发展，类似的安全事件会越来越多。接下来本节主要对打印机设备在互联网上的暴露情况进行统计及分析。

观点 9：互联网上暴露的打印机设备中，惠普暴露的设备数量最多，占比超过 50%。

打印机的安全问题应该受到用户和厂商的重视。前瞻产业研究院发布的《2015-2020 年中国激光打印机行业市场前瞻与投资战略规划分析报告》[20] 给出了 2015 年打印机的市场占有率，如图 3-14 所示。目前多种品牌打印机存在不同程度的暴露情况，其中惠普打印机暴露的数量最多，全球和国内占比分别为 57% 和 44%，兄弟和爱普生的全球暴露数量也超过了 5 万台，如图 3-15 所示。

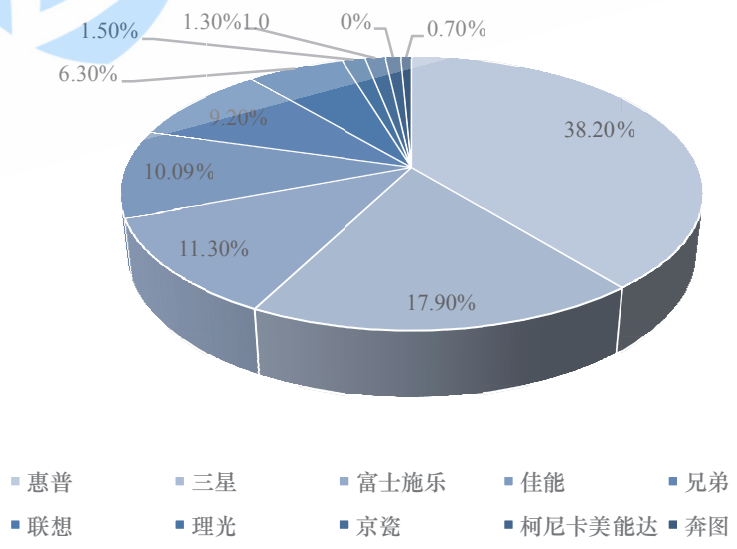


图 3-14 2015 年打印机市场占有率

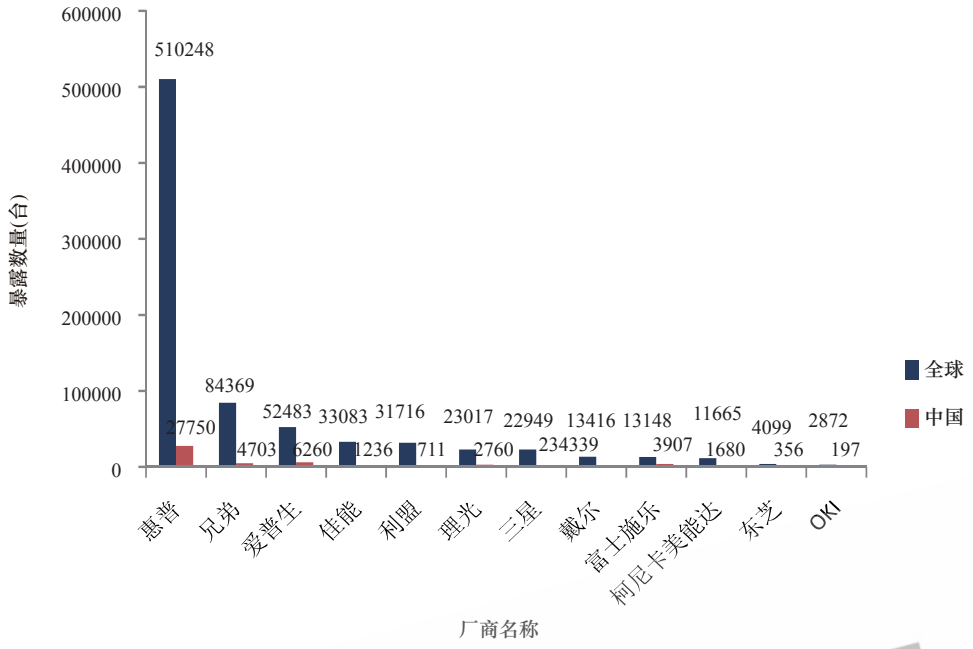


图 3-15　暴露的打印机按厂商的分布情况

观点 10：全球范围内，打印机设备主要暴露在美国和韩国；国内范围内，打印机主要暴露在港台地区，占国内暴露总量的 95% 以上。

如图 3-16 和图 3-17 所示，从全球分布来看，打印机设备主要暴露在美国，总量超过了 34 万台，占比 38%。从国内分布来看，也有超过 6 万台的打印机设备暴露在互联网上，并且主要集中在台湾，其中台北的打印机设备暴露最多，达到了 17840 台，占比 28%。

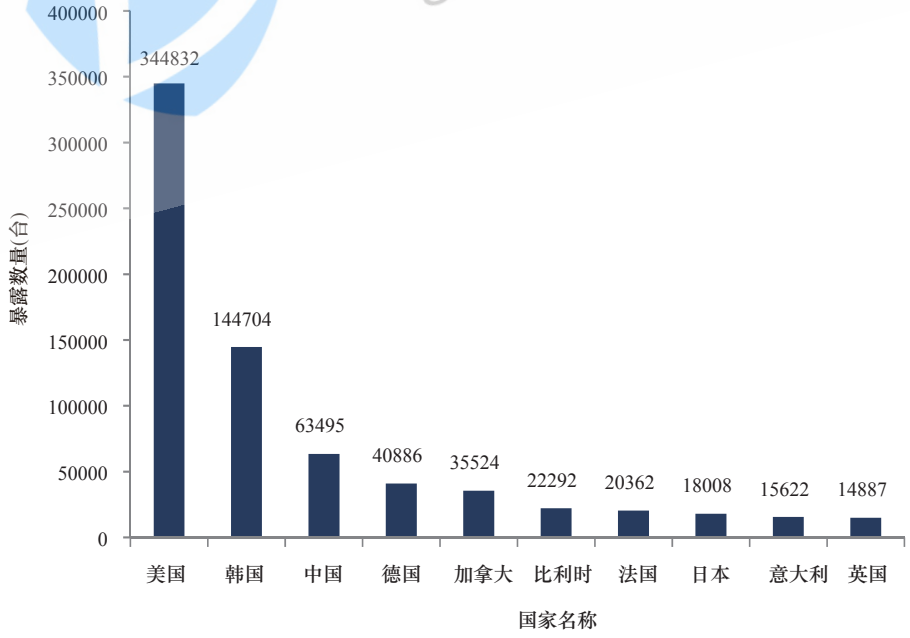


图 3-16　暴露的打印机按国家的分布情况（全球）

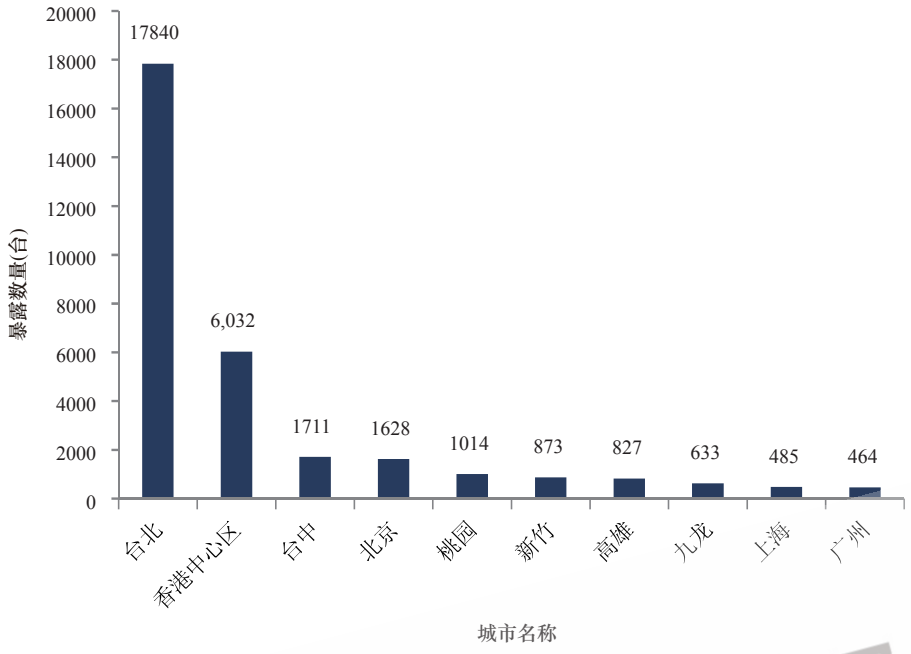


图 3-17　暴露的打印机按城市的分布情况（中国）

观点 11：惠普打印机的 HTTP 服务提供远程访问功能，但部分打印机的 HTTP 服务没有启用必要的登录认证机制。

图 3-18 和图 3-19 分别是暴露在全球和国内的惠普打印机的端口分布情况。惠普打印机暴露最多的是 HTTP 服务。从端口上看，HTTP 服务一般会开在 80、443、8080 等端口上，其中 80 端口暴露最多，全球暴露总数超过了 15 万。

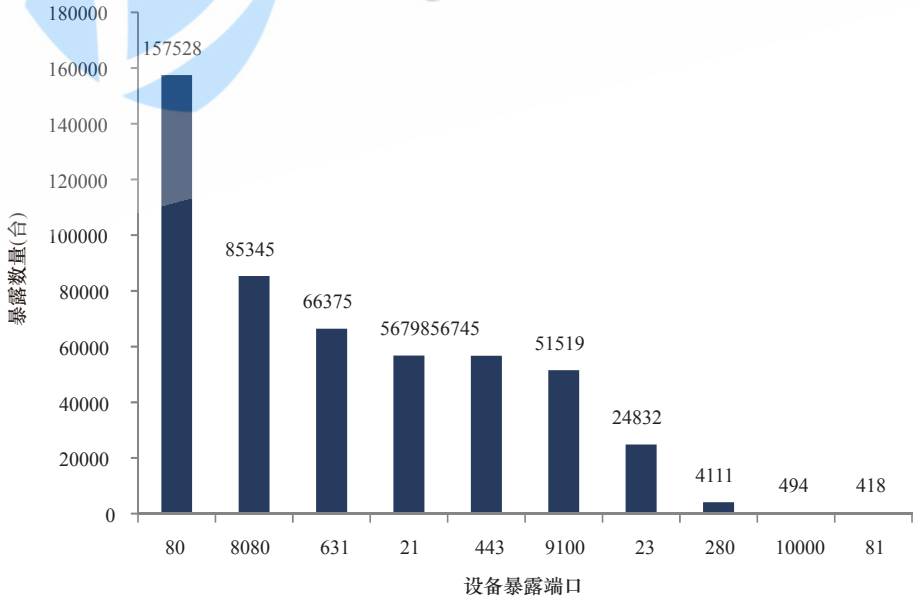


图 3-18　惠普打印机端口暴露情况（全球）

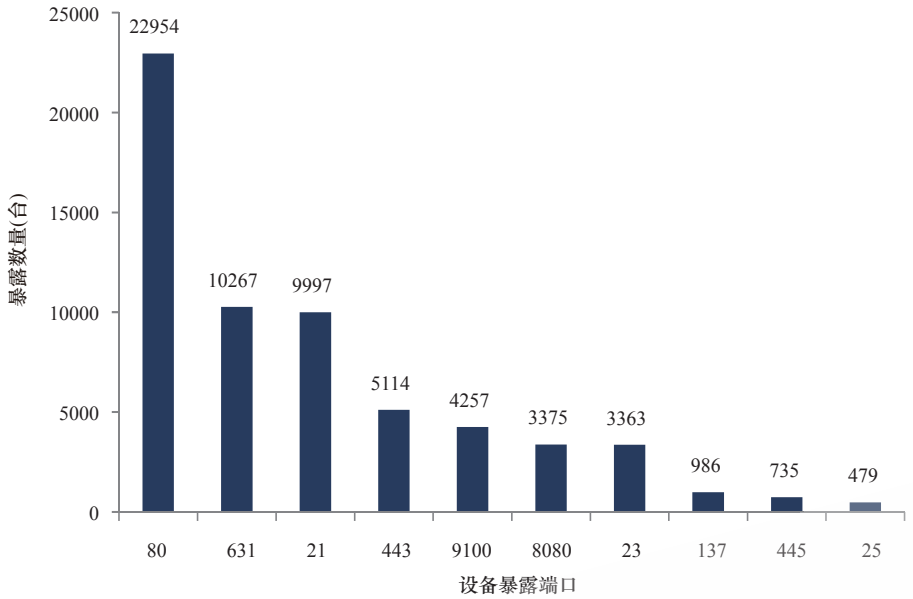


图 3-19　惠普打印机端口暴露情况（中国）

不乐观的是，很多暴露的打印机 HTTP 服务没有启用认证机制，远程用户不需登录即可进入打印机管理界面。事实上，管理员可在管理界面中设置登录密码，如图 3-20 所示，可见打印机管理员的安全意识亟待提高。

图 3-20　HP 某型号打印机管理员密码设置界面

我们上半年发布国内物联网资产暴露的报告后，惠普官方在雷锋网采访[21]中做出回应，已在 2016 年就注意到了这个现象，部分客户由于缺乏对文印安全保护的重视，没有主动部

署或者启用惠普提供的文印安全解决方案，让自己的设备和信息暴露在威胁之中。事实上，只有不到 44% 的 IT 经理人把打印机列入了安全战略，与此同时，也仅有不到 50% 的使用者会使用打印机的“管理密码”功能。也正是因为这样，全球数以亿计的商务打印机中只有不到 2% 的打印机是真正安全的。

3.2.5 其他设备暴露情况

在对暴露在互联网上的物联网资产进行分析的过程中，我们也发现了一些数量相对较少的物联网设备也暴露在了互联网上，如商用车的远程通信统一网关、网络恒温器等。这些设备的暴露，预示着随着物联网基础设施建成和新型物联网应用丰富，会有越来越多的安全问题直接在互联网上暴露出来。本章希望可以对物联网基础设施的安全建设提供一些参考。接下来，我们分别对互联网上暴露的远程通信统一网关、网络恒温器进行分析。

观点 12：数百辆商用车的远程通信统一网关暴露在互联网上，其 Telnet 登录无密码保护，存在严重的安全隐患。

远程通信统一网关（Telematics Gateway Unit，TGU），用于提供商用车（如卡车、公交等）的联网功能 [22]。这些车辆的 TGU 可以配置一个互联网地址，通过该网址可以远程监测和控制车辆。在 2016 年 3 月的一位安全研究员的博客 [23] 中就提到了一款这样的产品——Mobile Devices 公司的 C4Max。

我们按照博客中提供的方法，在网络空间搜索引擎中进行搜索，有大约 628 个 IP 被网络空间搜索引擎识别出（开放 Telnet 服务）。这些暴露出的 IP 的 Telnet 服务登录无密码保护，图 3-22 是通过 Telnet 登录 C4Max 之后在高级模式下的命令截图，可以看到登录进去后，可进行固件更新、重启等操作。

更有甚者，如果 TGU 连入了汽车动力控制系统，并且通过蜂窝网络接入互联网，就会存在暴露在互联网中的风险。在产品设计时，必须设计安全的口令和系统软件，使系统本身具备一定的安全性。否则，一旦用户使用不当，使 TGU 暴露在互联网上，那就等于把生命交到了攻击者手中。

图 3-21 Mobile Devices 公司的 C4Max 产品图片

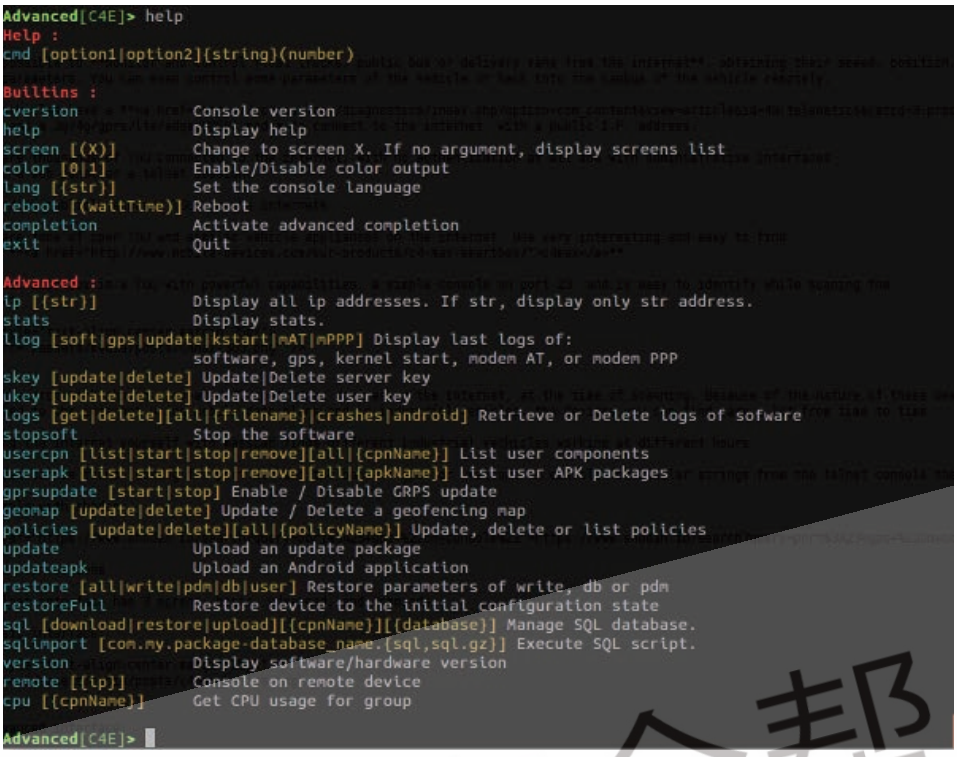


图 3-22　Telnet 登录 C4Max 之后在高级模式下的命令截图

观点 13：有近 200 个 Proliphix 公司的网络恒温器暴露在互联网上，且该网络恒温器已停产，缺乏安全维护。

在建筑设计中，HVAC（Heating Ventilation and Air Conditioning）是通风、调温的重要解决方案，使用户可以控制室内的温度。网络恒温器提供给用户远程控制的 Web 界面来控制温度，进而控制家中的 HVAC 系统。

我们在网络空间搜索引擎中发现有 165 个 Proliphix 公司的网络恒温器暴露在互联网上，图 3-23 是 Proliphix 公司的 NT20e 型号的恒温器图片。公司官网已经标注该产品已经停产，不再维护。

我们在其用户手册 [24] 中找到了该公司恒温器的默认口令及登录之后的页面截图。如果该恒温器的默认口令未修改，一旦其暴露在互联网上被攻击者利用，相当于家里的温度控制权限交到了攻击者手中，将影响到我们的日常生活，并且对我们的财产造成损失。

图 3-23　Proliphix 公司的恒温器

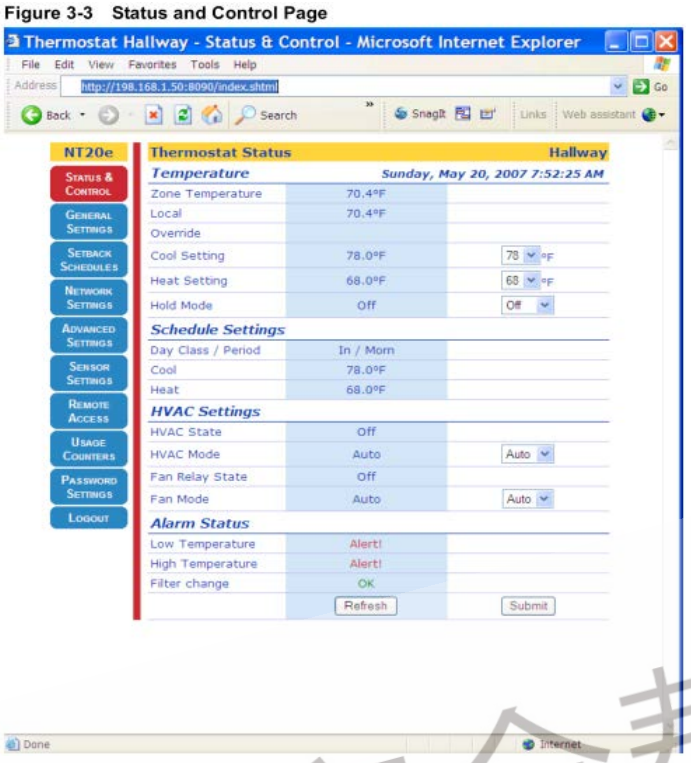


图 3-24 Proliphix 公司的某款恒温器登录之后的页面截图

3.2.6 小结

路由器、视频监控设备和打印机等物联网设备大规模的暴露，会让不法分子有可乘之机。当初的 Mirai[25] 事件就是黑客利用路由器、视频监控设备的弱口令等安全风险，对其实施入侵，并植入恶意软件构建僵尸网络，发动大规模拒绝服务攻击。此类安全事件随时都有可能发生，不仅会让这些设备失效，更重要的是，攻击者会借用这些设备发动更严重的攻击，造成破坏。

3.3 物联网操作系统的暴露情况分析

在 2016 年 12 月 8 日，工业和信息化部、财政部联合制定了智能制造发展规划（2016-2020 年）参考文献 [33]，在“智能制造关键共性技术创新方向”专栏中明确指出加快研发高安全、高可信的嵌入式实时工业操作系统。与此同时，中国信通院发布的物联网白皮书（2016）[27] 指出：物联网操作系统面向可伸缩、互通性实现创新发展。可预知的是，在 2020 年以前，物联网操作系统将在支持的无线连接类型、物联网应用层协议等功能方面得到丰富、完善，而且，物联网操作系统的安全性将进一步提高。

物联网操作系统并没有严格的定义。与传统的嵌入式操作系统相比，物联网操作系统弱化了对实时性的严格区分，增加了对物联网无线连接和协议种类的支持。在本章，我们把物联网操作系统限制为具有以下特点的操作系统。

（1）支持多种或者支持物联网专用的无线连接方式（如 NB_IoT、LoRa、ZigBee、Z-Wave 等），比如华为的 LiteOS，ThingsSquare 的 Contiki 等。

（2）支持多种物联网应用层协议，如 MQTT、CoAP，以及 Raspbian 等。

从 NTI 中，我们也搜索到了物联网操作系统，尽管这些物联网操作系统依然比较传统，但是这些物联网操作系统在应用开发方面极大地提升了物联网开发者的体验，也支持了多种无线网络协议和网络管理。如运行在智能硬件树莓派上的 Raspbian 操作系统，在支持 Node.js 的同时，加入了 MQTT 模块，使开发物联网应用程序变得像编写 PPT 一样方便。又如开源的路由器固件发行版 OpenWrt 的强大的网络管理能力体现了其成为物联网网关的潜力，基于 MT7620 等无线芯片的传统硬件解决方案，也因为 OpenWrt 在物联网方面的强大优势而逐渐被开源，极大地降低了物联网应用开发的难度。

本节将介绍暴露在互联网上物联网设备的操作系统的整体分布情况，并分别介绍暴露现象情况比较显著的 4 个操作系统的分布情况。

3.3.1　整体情况

观点 14：物联网操作系统在互联网上暴露的数量增加显著。

在 2017 年上半年，我们基于 NTI 对互联网上暴露的、搭载物联网操作系统的设备进行了端口和协议（服务）两个方面的分析，主要包含 5 个操作系统：VxWorks、uClinux、OpenWrt 系列、Raspbian 系列、Nucleus。在 2017 年下半年，我们发现，除了 Nucleus 操作系统外，其他操作系统在互联网上的暴露数量均有大幅度的增长。所以本次不再对 Nucleus 操作系统单独分析。

如图 3-25 所示，2017 年上半年，国内范围内，OpenWrt 操作系统在互联网上暴露的数量仅仅为 2136 个，下半年就增长到了 54440 个，是上半年的 25.5 倍。Raspbian 操作系统在国内暴露的数量是 1390 个，到下半年，其暴露数量增长到了 10016 个，增长了 6.2 倍。

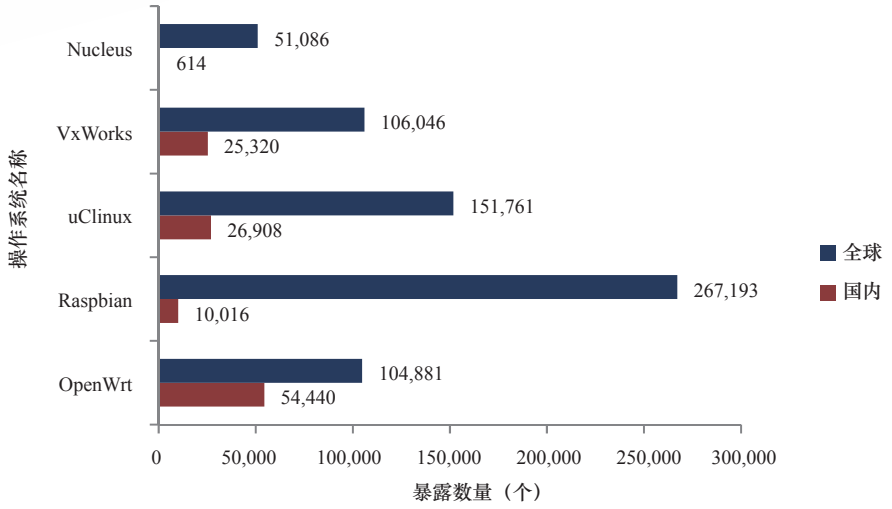


图 3-25　物联网操作系统暴露情况

接下来，我们将对 VxWorks、uClinux、OpenWrt 系列、Raspbian 系列 4 个操作系统的端口和服务的开放情况进行分析和呈现。

3.3.2 OpenWrt 暴露情况分析

Cisco / Linksys 在 2003 年发行了 Linksys WRT54G 这款路由器，由于公司欲降低成本而使用了 Linux 内核，最终迫于压力而公开了源码。此后就有了一些基于 Linksys 源码的第三方固件，后来这个固件通常被作为一个 Linux 发行版，被称为 OpenWrt。它的应用的载体通常是路由器，其中，也不能排除某些爱好者将其移植到其他嵌入式设备（如网络摄像头、机器人、开发板等）上面。

观点 15：OpenWrt 操作系统暴露的 HTTPS 和 HTTP 服务非常多，这两个服务在全球暴露总数超过 13 万个，在国内暴露总量达到了 6.7 万个。

如图 3-26 和图 3-27 所示， OpenWrt 操作系统暴露最多的服务是 HTTPS 服务和 HTTP 服务。就 HTTPS 服务而言，全球暴露了 67255 个，国内暴露了 46988 个，数量级差距并不大。除了 HTTPS 服务以外，Telnet 服务、FTP 服务和 SSH 服务的暴露数量也非常多，在全球范围内 Telnet 服务和 SSH 服务的暴露数量均超过了 1 万个，在国内，OpenWrt 操作系统开放的 Telnet 服务、FTP 服务、SSH 服务的暴露数量均超过了 3000 个。

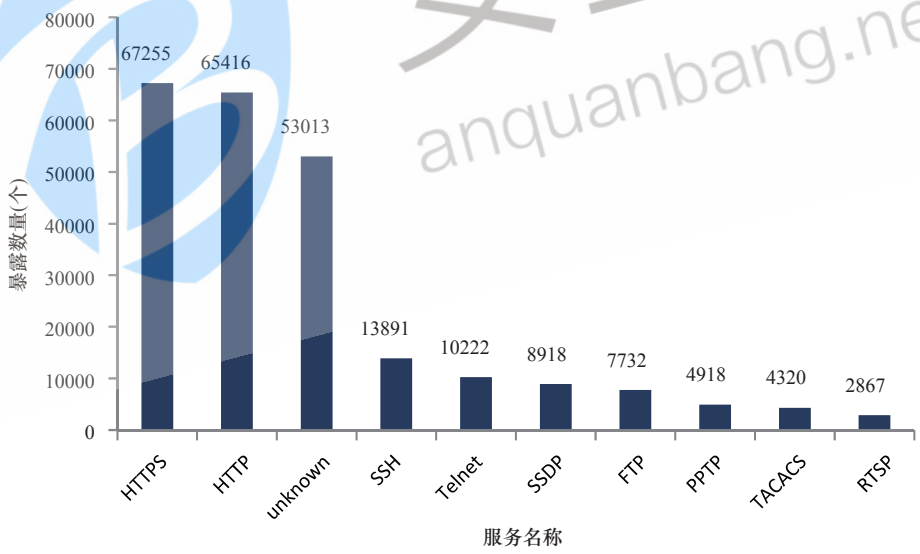


图 3-26 Openwrt 暴露的服务数量（全球）

观点 16：OpenWrt 操作系统开启的 VPN 服务比较多。

如图 3-28 和图 3-29 所示，HTTPS 服务默认开放的 443 端口暴露数量最多，全球暴露总量达到 71339 个，国内暴露的 443 端口数量达到了 49308 个。比较特别的是，1723 端口的全球暴露数量达到了 7879 个，国内暴露数量达到了 5992 个。一般情况下，1723 端口被默认配置为基于 PPTP 的 VPN 服务。这说明一部分搭载 OpenWrt 操作系统的设备被用来开启 VPN 服务。

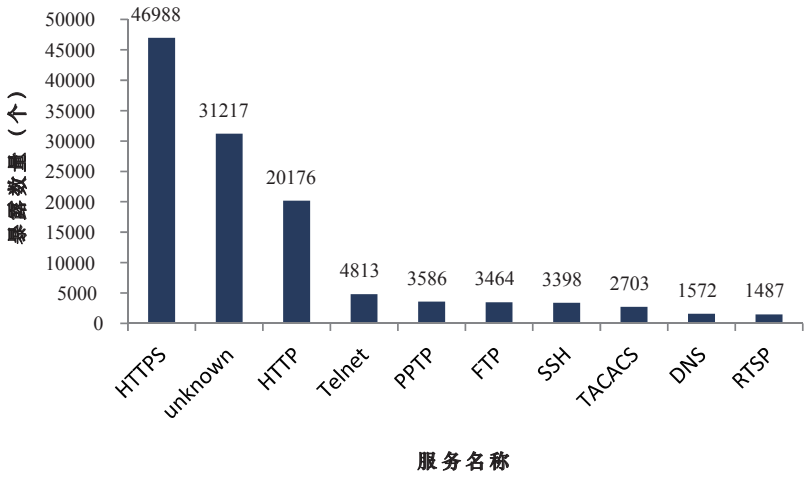


图 3-27　Openwrt 暴露的服务数量（国内）

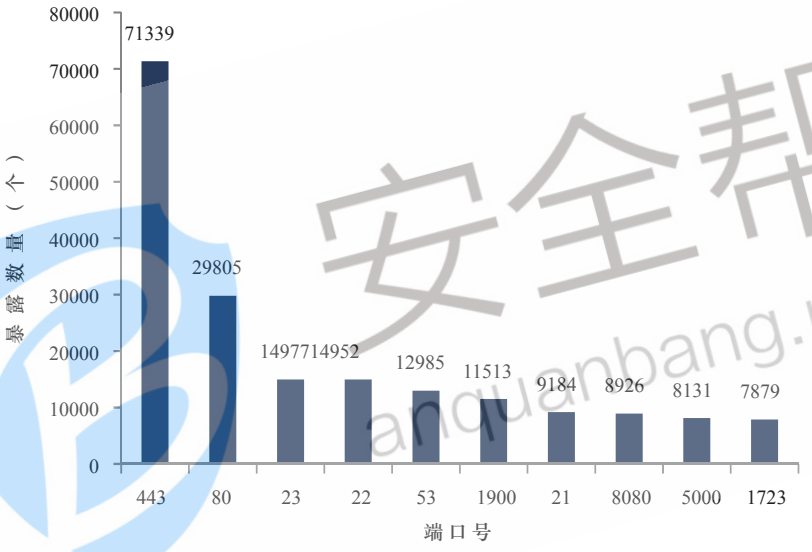


图 3-28　Openwrt 暴露的端口数量（全球）

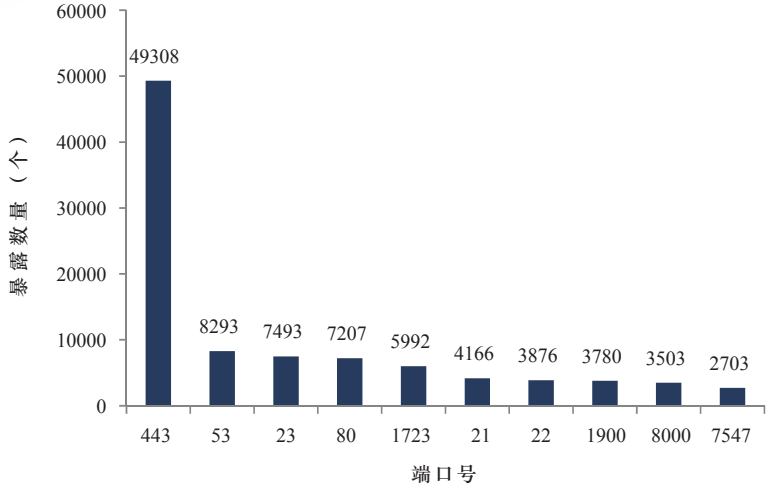


图 3-29　Openwrt 暴露的端口数量（国内）

3.3.3 Raspbian 暴露情况分析

Raspbian 一般会运行于一款名为“树莓派”的智能硬件之上。由于树莓派采用了基于 ARM Cortex-A7 的 4 核心的 CPU，RAM 达到了 1GB，性能比一般的物联网设备强劲，所以 Raspbian 操作系统与传统的嵌入式操作系统相比，会集成硬件调试、网络连接、数学计算等相关的软件包。难能可贵的是，该操作系统的安装流程得到了简化，这一点备受电子工程师和其他爱好者的好评。

观点 17：Raspbian 操作系统被安装后，一般没有被及时关闭 SSH 服务，导致大量的 SSH 服务暴露。

如图 3-30 和图 3-31 所示，在近 27 万台搭载 Raspbian 操作系统的设备中，开启 SSH 服务和 HTTP 服务的数量分别达到了 18 万台和 19 万台。说明这些设备中，有 73.3% 被用来当作 HTTP 服务器，67.6% 被开启了 SSH 服务；SSH 服务开启的原因可能有两个，其一是 Raspbian 操作系统初次运行时，默认开启了 SSH 服务；其二是管理员为了方便登录管理控制台，启用 SSH 对设备进行配置管理。

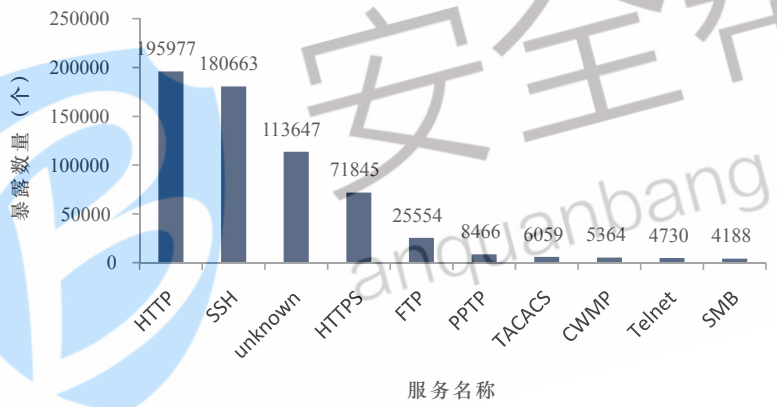


图 3-30 Raspbian 暴露的服务数量（全球）

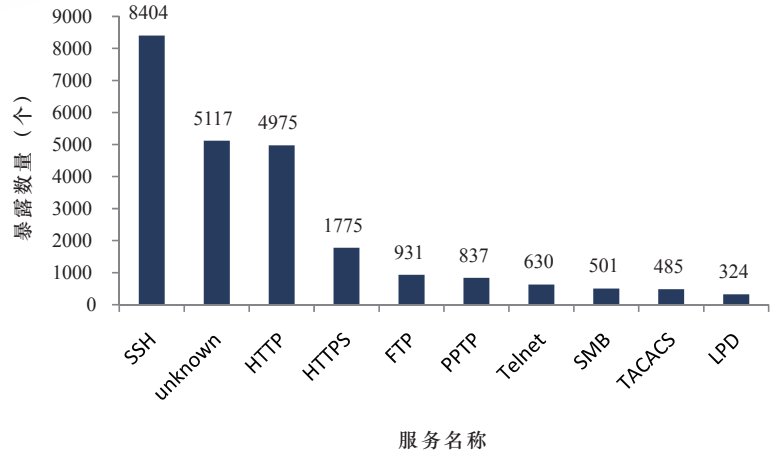


图 3-31 Raspbian 暴露的服务数量（国内）

观点 18：Raspbian 操作系统暴露的 VPN 服务比较多。

由图 3-32 和图 3-33 可以看出，不论是在看全球的端口分布还是看国内的端口分布，22 端口在所有开放的端口中开放的数量都是最多的，全球范围内，22 端口暴露数量达到了 162237 个，约占全球 OpenWrt 操作系统暴露总数的 60%；全国范围内，22 端口暴露数量达到 7859 个，约占全国 OpenWrt 操作系统暴露总量的 78%。所以，SSH 服务暴露数量多的两个原因中，前者的可能性最大。因为，有安全意识或运维经验的管理员在开启 SSH 服务时，会提前把 SSH 服务配置在不常用端口上。

和 OpenWrt 操作系统一样，Raspbian 系统也开启了很多 PPTP 服务，全球范围内，Raspbian 操作系统暴露的 PPTP 服务的数量达到了 8466 个，国内暴露的 PPTP 服务的数量为 837 个，说明管理员在这些搭载 Raspbian 操作系统的树莓派或其他兼容硬件上架设了 VPN 服务。

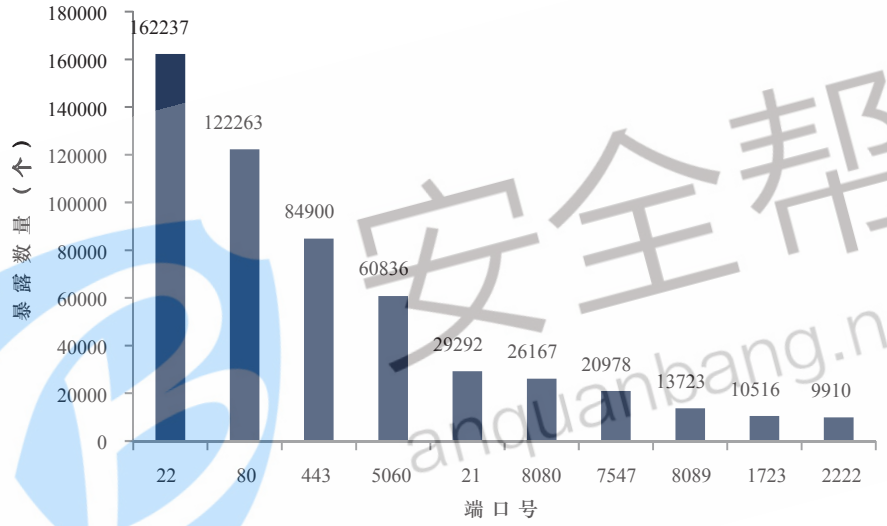


图 3-32　Raspbian 暴露的端口数量（全球）

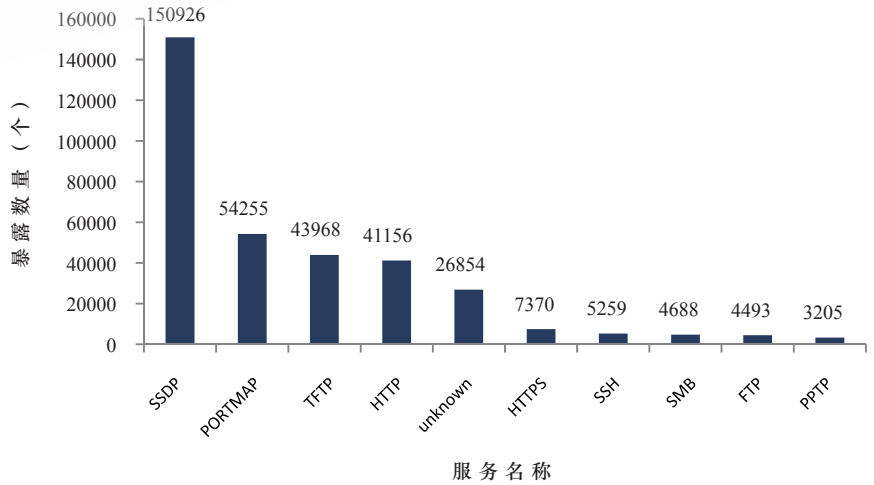


图 3-33　Raspbian 暴露的端口数量（国内 uClinux）

3.3.4 uClinux 暴露情况分析

与 Linux 操作系统相比，uClinux 采用实时存储策略，使没有 MMU（内存管理单元）的微处理器也可以被移植上操作系统，体验与 Linux 操作系统相同。目前 uClinux 操作系统已经被应用于路由器、机顶盒、视频监控等领域。

观点 19：全球范围内暴露的 151761 个 uClinux 操作系统中，开启 SSDP 服务的至少有 149773 个，约占 99%。

如图 3-34 和图 3-35 所示，搭载 uClinux 操作系统的设备，开放的 SSDP 服务的数量最多，在全球范围内，SSDP 服务的暴露数量达到了 15 万个，在国内，SSDP 服务暴露的数量达到了 25052 个。其次是 HTTP 服务、TFTP 服务和 HTTPS 等服务。

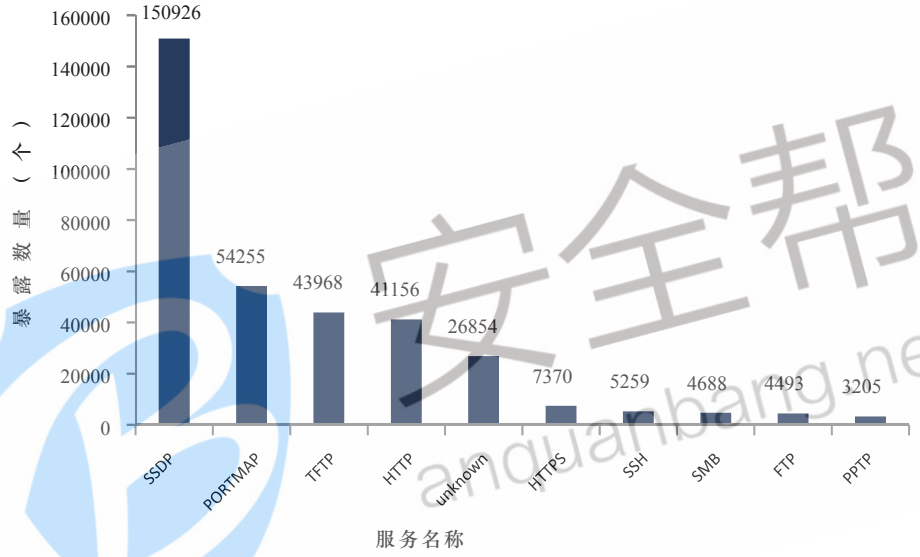


图 3-34 uClinux暴露的服务数量（全球）

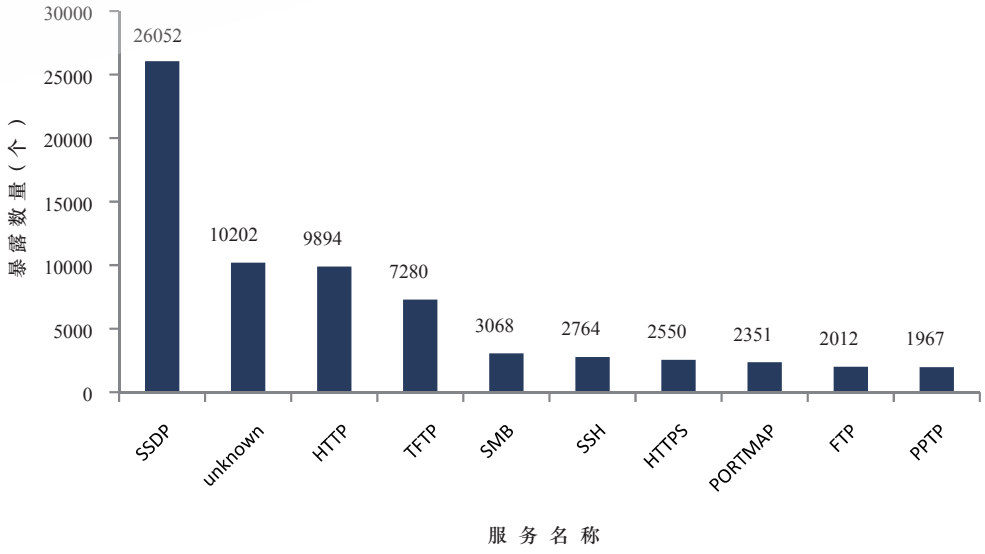


图 3-35 uClinux暴露的服务数量（国内）

由图 3-36 和图 3-37 所示，默认开启 SSDP 服务的 1900 端口暴露的数量最多，全球范围内，暴露了仅 15 万个，约占全球 uClinux 操作系统总量的 98%，全国范围内，暴露 25875 个，约占 97%。比较特别的是，69 端口暴露的数量，在全球范围内达到了 43887 个，排名第三；在国内，69 端口暴露数量达到了 7276 个，排名仅次于 1900 端口。一般情况下，TFTP 服务会默认开启在 69 端口。结合端口和服务分布情况看，搭载 uClinux 的设备极有可能同时提供了设备发现的功能和文件传输的功能。

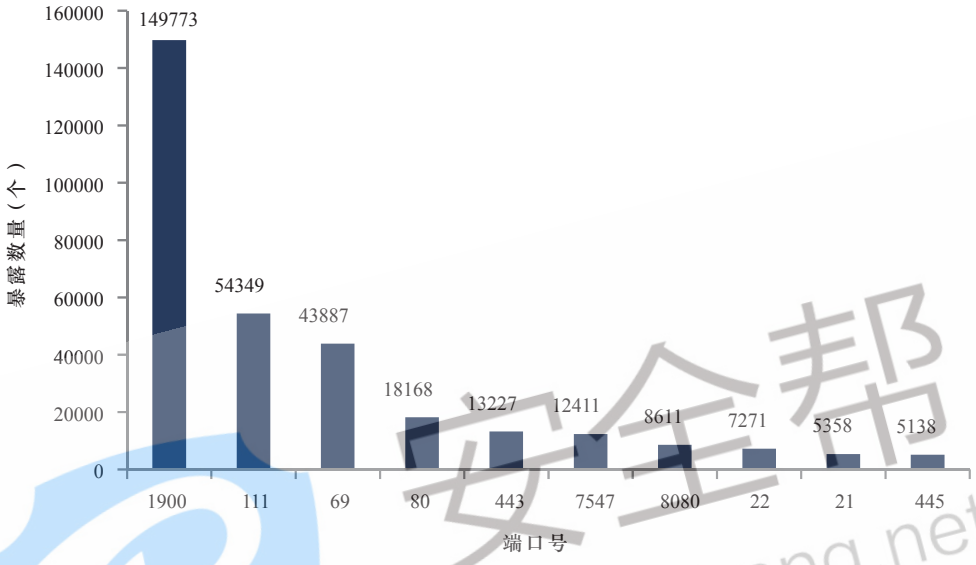


图 3-36　uClinux 暴露的端口数量（全球）

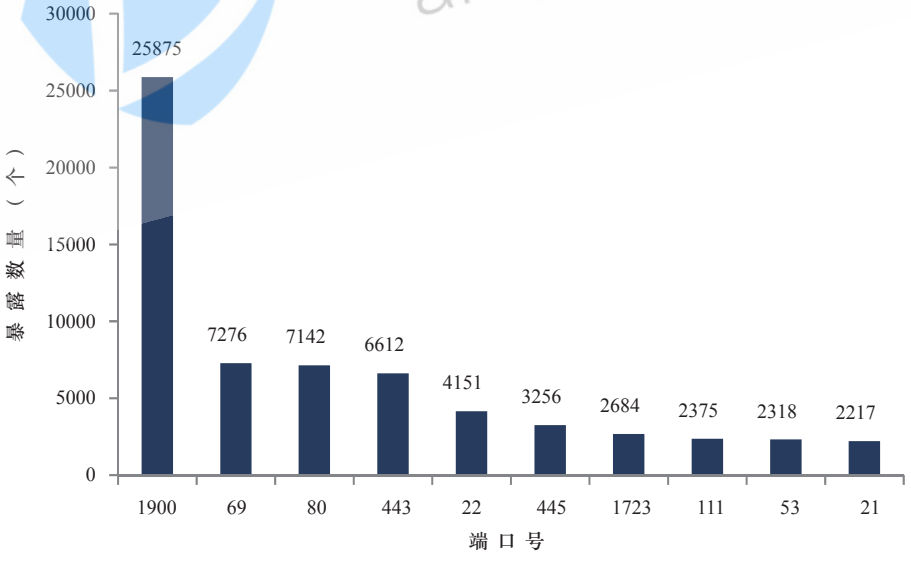


图 3-37　uClinux 暴露的端口数量 - 国内

3.3.5　VxWorks 暴露情况分析

VxWorks 操作系统是美国 WindRiver 公司于 1983 年设计开发的一种嵌入式实时操作系

统（RTOS），作为业界公认的具有高实时性内核操作系统，它的应用领域甚广，如交换机和路由器这些处理大量流量的设备，航天领域各种精密控制设备等。

观点 20：VxWorks 操作系统暴露 WDB 调试服务的现象比较严重。

由图 3-38 和图 3-39 所示，未识别的服务和 HTTP 服务的总量达到 44 万个，是全球暴露的 VxWorks 操作系统总量的 4 倍。所以，VxWorks 操作系统一般会开启多个端口，一般用于 HTTP、FTP、Telnet 等服务。

另外，WDB 调试服务暴露数量非常多。而且全球 12120 台设备，其中国内 9100 台设备都抛出了“Error in Wind River System VxWorks debug service response”的 banner 信息。在互联网上，WDB 服务提供了远程调试 VxWorks 操作系统的能力，如果被攻击者通过 WDB 调试端口获取到操作系统的调试权限，会危害到系统安全。

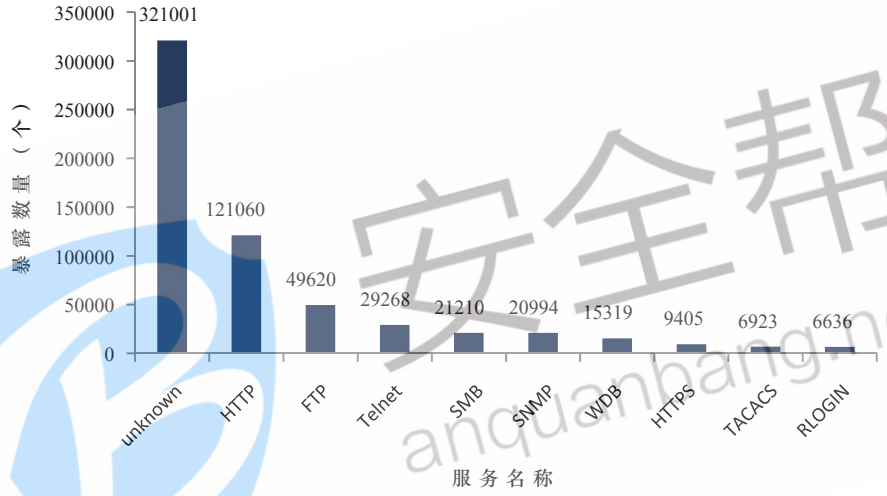


图 3-38　VxWorks 暴露的服务数量（全球）

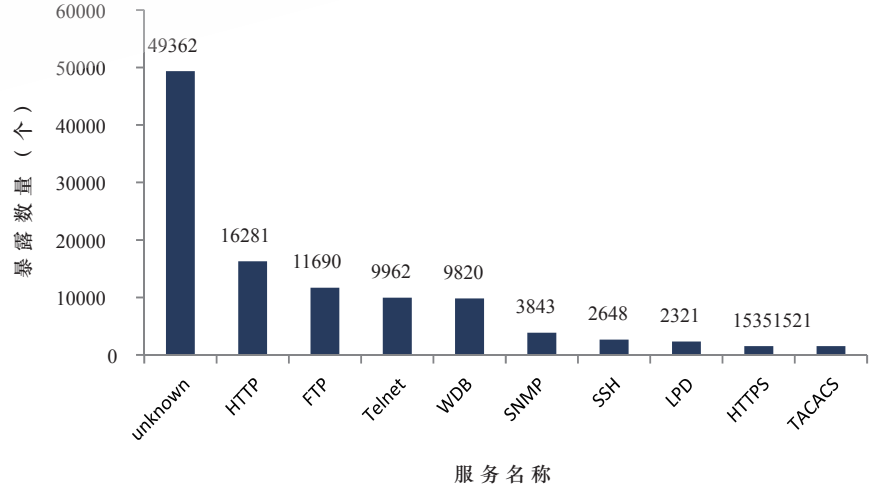


图 3-39　VxWorks 暴露的服务数量（国内）

由图 3-40 和图 3-41 所示，全球的 VxWorks 操作系统开启的 21、23、80 端口最多，均

超过了 4 万个，暴露的 111 端口暴露数量也达到 23896 个。在国内，VxWorks 操作系统暴露的 111 端口的数量最多，达到了 15952 个。其次为 21、23、80 等端口。

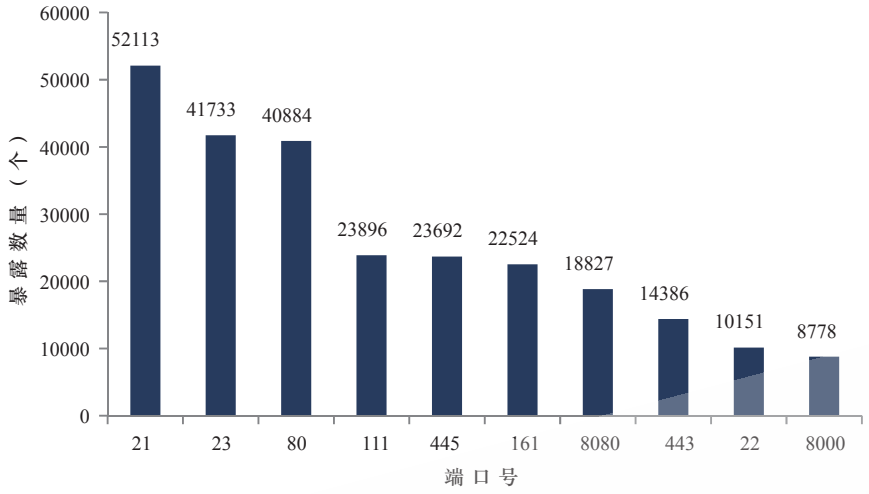


图 3-40　VxWorks 暴露的端口数量（全球）

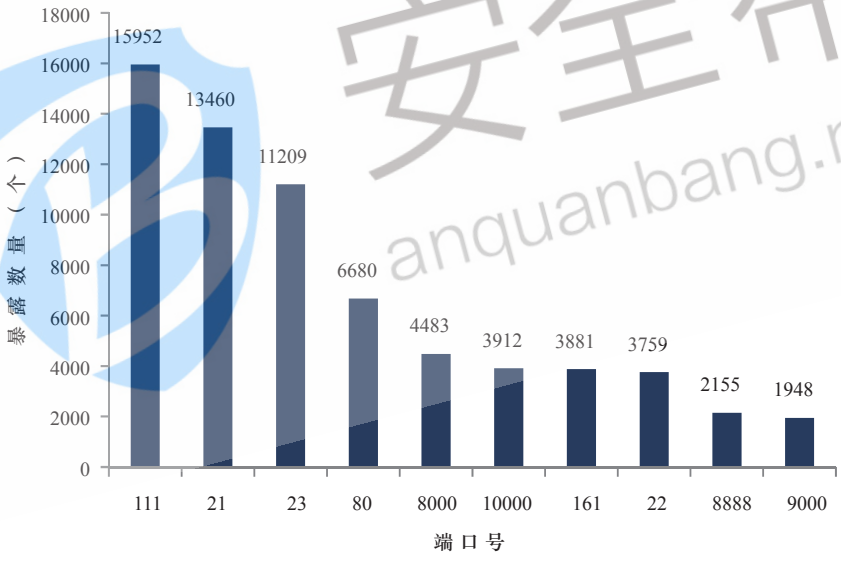


图 3-41　VxWorks 暴露的端口数量（国内）

3.3.6　小结

从 2017 年上半年到现在，除了 Nucleus 之外，其他的 4 个操作系统在互联网上暴露的数量增长幅度非常大，这一方面说明现在搭载物联网操作系统的设备日趋增长，另一方面也说明了互联网上暴露的设备信息更加全面。一般情况下，如果这些操作系统的默认配置不被改变，默认开启的服务和端口也将暴露在互联网上。在这些开放的端口和服务中，常常带有操作系统的版本信息，这样，攻击者只需要找到系统版本对应的 CVE 漏洞或默认登录口令，即可成功得到获取操作系统权限，大大降低了攻击者的攻击成本。

3.4 关键性发现

我们对常见的物联网设备和操作系统进行了分析，关键性发现如下。

（1）互联网上暴露的各类物联网设备中，路由器和视频监控设备的数量最多。

（2）全球范围内，华为路由器暴露的数量最多，占比达到 22%；国内范围内，水星、迅捷路由器暴露的数量最多。

（3）全球范围内，中国暴露的路由器数量最多；国内范围内，二线城市暴露的路由器数量居多。

（4）在视频监控设备中，海康威视和浙江大华两大厂商暴露数量较多。全球范围内，两大厂商占全球总暴露量的比例分别为 31% 和 14%；国内范围内，该比例分别为 60% 和 13%。

（5）全球范围内，美国和中国暴露的视频监控设备数量最多，占比分别为 16% 和 14%；国内范围内，暴露的视频监控设备大部分位于台湾，占比为 47%。

（6）互联网上暴露的打印机设备中，惠普设备数量最多，占比超过 50%。部分惠普网络打印机的 HTTP 服务没有启用必要的登录认证机制。

（7）全球范围内，打印机设备主要暴露在美国和韩国；国内范围内，打印机主要暴露在港台地区，占国内暴露总量的 95% 以上。

（8）商用车的远程通信统一网关、网络恒温器等在互联网上也有一定的暴露，其可能面临远程登录无密码保护、设备停产缺乏安全维护等风险。

（9）树莓派的主流操作系统 Raspbian 被安装后，SSH 服务一般没有被及时关闭导致大量暴露。

（10）约 99% 的 uClinux 操作系统开启了 SSDP 服务。

（11）一部分搭载 OpenWrt 和 Raspbian 操作系统的设备会被用来开启 VPN 服务。

（12）约 14.4% 的 VxWorks 操作系统会暴露 WDB 调试服务。

3.5 防护建议

借助于网络空间搜索引擎的资产情报，我们对暴露在互联网上的物联网资产进行了分析。分析维度分为两类，一类着眼于设备，关注于不同种类的设备在互联网的分布情况；一类着眼于物联网操作系统，关注 4 类主要的操作系统暴露在互联网上。

由于精力有限，很难保证涵盖到所有种类，对于所包含的类别，也很难保证数据百分之百的准确性。但在分析过程中，我们通过对三个搜索引擎（NTI、Shodan 和 ZoomEye）的数据综合分析，尽可能确保数据的全面性和准确性。另外，我们的目的是通过展示物联网设备在互联网的暴露情况来揭示物联网安全防护的必要性和紧迫性。从这个角度来讲，少量遗漏或噪声数据并不影响文章的观点。

结合我们的分析，下面分别从用户角度、物联网厂商和信息安全厂商角度给出一些物联网安全建议。

用户角度：

（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，如 FTP（21 端口）、SSH（22 端口）、Telnet（23 端口）等；

（3）修改默认端口为不常用端口，增大端口开放协议被探测的难度；

（4）升级设备固件；

（5）部署厂商提供的安全解决方案。

物联网厂商角度：

（1）对于设备的首次使用可强制用户修改初始密码，并且对用户密码的复杂性进行检测；

（2）提供设备固件的自动在线升级方式，降低暴露在互联网的设备的安全风险；

（3）默认配置应遵循最小开放端口原则，减少端口暴露在互联网的可能性；

（4）设置访问控制规则，严格控制从互联网发起的访问；

（5）与安全厂商合作，在设备层和网络层进行加固。

信息安全厂商角度：

- 优先关注暴露数量较多的物联网资产的脆弱性分析；
- 为物联网厂商提供设备出厂前测评服务，将设备可能存在的风险尽可能降低；
- 关注物联网设备的安全防护，推出既满足正常用户的访问，同时又可抵抗恶意攻击的安全产品及解决方案；
- 加大物联网安全宣传的力度，提高公众的信息安全意识。

第四章

2017 十大物联网安全事件分析

随着物联网的飞速发展，物联网已能够将物理设备、车辆、建筑物和一些其他嵌入的电子设备、软件、传感器等事物与网络连接起来，使这些对象能够收集和交换数据。物联网允许远端系统通过现有的网络基础设施感知和控制事物，可以将物理世界集成到计算机系统，从而提高效率、准确性和经济利益。可见，物联网已经在很大程度上融入到我们的生活中。但随着物联网的发展，其面临的安全问题也越来越凸现出来，物联网安全问题正走进人们的视线。近年来，诸多的物联网安全事件引起我们的广泛关注。本章主要对 2017 年物联网十大热点安全事件进行解析。

4.1 新路由器高危漏洞致德国百万用户断网

日期：2017 年 6 月。

事件：数百万德国网民遭遇一系列的网络中断，究其原因是一次失败的消费者路由器劫持。

德国电信（Deutsche Telekom）的 2000 万用户中有 90 万用户受到本次网络中断影响，德国电信发布的声明中表明本轮攻击主要是为了进一步扩大感染，如图 4-1 所示。

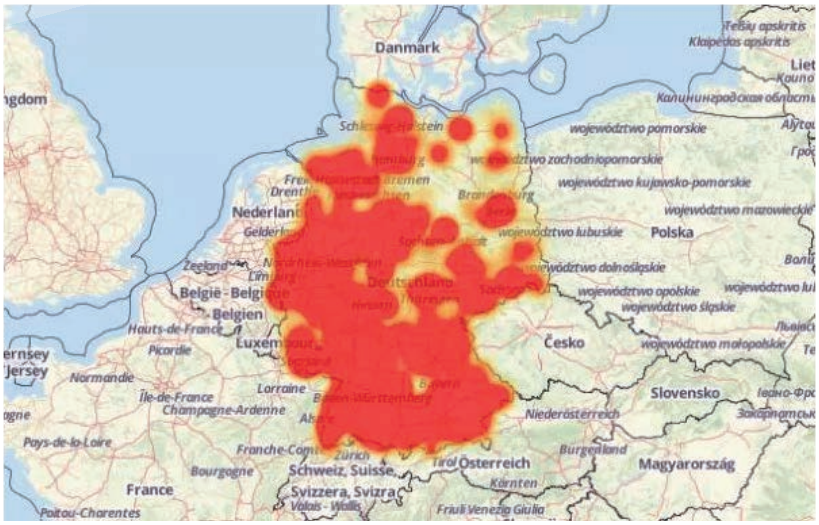


图 4-1 新路由器高危漏洞致德国百万用户断网

德国电信在声明中表示：“本轮攻击尝试通过恶意程序感染路由器，但由于失败导致 4% 到 5% 的路由器出现崩溃和受限，这导致德国电信为消费者提供的网络服务受限。”公司表明将会部署软件更新来修复这个问题，同时还推荐消费者暂时重启设备以重新启动没有恶意软件的固件。

安全研究人员发现台湾合勤科技、德国 Speedport 等公司的路由器产品存在该漏洞。这些设备被发现 7547 端口对外开放，攻击者可以通过发送基于 TR-069 和 TR-064 协议的指令利用漏洞。物联网搜索引擎 Shodan 报告有 4100 万设备开放了 7547 端口，有大约 500 万设备暴露了 TR-064 服务。在事件发生过去 24 小时内，奥地利的 TR-069 路由器流量大幅增加，开放 7547 端口的设备可以到达 53000 个。

在运营商对旧的攻击地址：l.ocalhost.host 进行了访问限制后，攻击者开始改用：timeserver.host 和 ntp.timerserver.host 这两个域名进行攻击。

这两个主机名都解析到了：176.74.176.187。

事件发生几天内，对 7547 端口的攻击大大增加。这些扫描似乎利用了流行的 DSL 路由器中的漏洞，这个问题可能已经导致德国 ISP 运营商德国电信出现严重问题。对于德国电信，Speedport 路由器似乎是这次事件的主要问题。

通过 Shodan 搜索，约 4100 万个设备开放 7547 端口。代码看起来是从 Mirai 派生的，带有对 SOAP 漏洞的附加扫描。

出售僵尸网络的两名黑客叫 BestBuy 和 Popopret，他们被认为与 GovRAT 恶意程序有关联，该恶意程序被用于从多家美国公司内部窃取数据。他们的 DDoS 租赁服务并不便宜，租赁 5 万设备组成的僵尸网络两周的费用在 3 千到 4 千美元。但是不得不说有了这样的攻击资源购买渠道，未来使用 IoT 设备进行拒绝服务攻击的事件会越来越多。

临时解决办法：

如果你怀疑你的路由器可能受到本次漏洞影响，你可以重启路由器并检查是否开放了 7547 端口，如果开放了该端口，请在路由器上对该端口进行访问限制。

但如果你的路由器已经感染，路由器将不再监听 7547 端口，你可以选择更新最新的官方固件并进行初始化操作，以免受该漏洞的危害。

总结：网络罪犯正在利用新发现的路由器高危漏洞，存在漏洞的路由器可能多达数百万部。研究发现代码看起来是从 Mirai 派生的，众所周知，Mirai 的源码在北京时间 2016 年 9 月 30 日前后泄露，随后被托管到 Github 上。自那以后，不管是黑帽子还是白帽子都对 Mirai 的源码进行了大量深入的分析。换句话说，随着时间的推移，各路新玩家终将逐渐入场，截至目前，我们的观察也印证了上述观点。我们已经发现了若干 Mirai 的新变种，例如出现了新的主控域名，或者登录界面从俄文变为英文 / 中文，也有一些明显还是新玩家摸索阶段的设定，比如将主控域名设为 8.8.8.8 或者 baidu.com。基于种种 Mirai 变种，我们推测 Mirai 家族对网络空间安全的威胁将会长期持续，周期也许会以年为单位计。尽管这个新变种有若

干变化，它仍然重用了 Mirai 的部分代码，进而顺带继承了 Mirai 代码中的缺陷，并与既有 Mirai 僵尸网络共享控制端基础设施。鉴于 Mirai 的源码已经公开，结合上述两个变种行为，我们担忧 Mirai 会成为一个 DDoS 攻击库的母体，通过对源代码部分内容进行更新，就可以随时增加对新漏洞的支持。

4.2 蓝牙协议漏洞攻击影响数十亿蓝牙设备

图 4-2 蓝牙协议漏洞：BlueBorne 攻击影响数十亿蓝牙设备

时间：2017 年 9 月。

事件：Armis Labs 披露了一个攻击向量，使得搭载主流移动、桌面、IoT 操作系统（包括 Android、iOS、Windows、Linux 系统）的设备均受其影响。

它通过空气 (Airborne) 即可传播，然后通过蓝牙 (Bluetooth) 协议发起攻击，BlueBorne 由此得名。

BlueBorne 之所以危险，是因为大多数用户都会在他们不使用蓝牙时将蓝牙打开。而 Attacker 根本不需要与 Target 设备配对（但是信号得在接收范围内），即可完全接管该设备。

Armis Labs 团队的负责人 Ben Seri 称，他们已经在实验环境下建立了一个僵尸网络，并且使用 BlueBorne 攻击安装了勒索软件。

然而，Seri 认为，即便是经验丰富的攻击者，想要在全球范围内制造一个瞄准所有平台，并且可以从一个受感染设备逐步感染周围设备，而且具有自传播功能的蠕虫也不那么容易。

Armis 总共列出了 8 个漏洞 (包括 Android、Windows、Linux 和 iOS 在内的几个操作系统中发现实施于蓝牙的 8 个漏洞，利用这些漏洞，黑客就能完全控制设备），其中 4 个是高危漏洞。

- 信息泄露漏洞 (CVE-2017-0785)

这个漏洞发生在 SDP 服务器上，攻击者可通过向 SDP 服务器发出构造的请求，然后服务器会在返回攻击者的响应中泄露它内存中的信息，这些信息可帮助攻击者识别周围的蓝牙服务，以及利用下面提到的远程代码执行漏洞。

- 远程代码执行漏洞 #1 (CVE-2017-0781)

这个漏洞发生在蓝牙网络封装协议（Bluetooth Network Encapsulation Protocol，BNEP）服务中，该服务通过蓝牙连接共享互联网（Tethering）。由于 BNEP 服务中存在缺陷，攻击者可构造非常容易利用的 Surgical Memory Corruption，然后攻击者就可完全接管设备然后执行任意代码了。由于缺乏适当的授权认证，触发此漏洞根本不需要任何用户交互、身份验证或者配对，因此 Target 用户完全无法察觉正在进行的攻击。

- 远程代码执行漏洞 #2 (CVE-2017-0782)

这个漏洞跟上一个相似，但是存在于 BNEP 服务的高层——PAN（Personal Area Networking）Profile 中，这个文件用于在两个设备之间建立 IP 网络连接。这个漏洞造成的 Memory Corruption 更大，但还是可以被攻击者利用，以获取受影响设备的完全控制权。跟上一个漏洞类似，这个漏洞无需用户交互，认证或配对即可触发。

- The Bluetooth Pineapple——中间人攻击 (CVE-2017-0783)

中间人攻击使得 Attacker 能够拦截并干扰出入 Target 设备的流量。在 Wi-Fi 环境下，要发起 MITM，Attacker 不仅需要特殊的设备，还需要有从 Target 设备发往它已经建立连接的“开放”Wi-Fi 网络（没有加密密钥的）的连接请求。攻击者必须嗅到“连接”在“开放”网络上的 Target 设备发往“开放”网络的 802.11 的 Probe Request 包，之后再伪装成这个“开放”网络，向 Target 返回 Probe Response。而在蓝牙 (Bluetooth) 中，Attacker 可以主动地使用支持 Bluetooth 的设备玩弄 Target。这个漏洞位于蓝牙协议栈的 PAN Profile 中，使得 Attacker 在受害者的设备上创建一个恶意的网络接口，重新配置网络路由，然后使设备上的所有通信流量都走这个恶意网络接口。这种攻击不需要用户交互、认证或者配对，使得实际的攻击发生于无形之中。

总结：BlueBorne 漏洞源自一个复杂协议，此协议连同两个关于蓝牙的常见误解，被研究界抛弃和忽视多年之久。第一误解是蓝牙无法进行空中拦截，第二误解是蓝牙始终需要某种用户交互。BlueBorne 漏洞证明这两种假设都是错误的，因为只要开启设备上的蓝牙，设备就极易受到攻击。与传统网络攻击不同，BlueBorne 不需要用户点击 URL 链接，或者下载恶意文件，受害者甚至根本不需要连接到互联网上，并且黑客根本就不需要与目标受害者配对，只要目标的蓝牙开关处于打开状态，黑客就可连接到这台设备，完全接管设备，还可以通过被攻陷的设备传播恶意软件，而受害者完全无法察觉。

4.3　CopyCat 病毒感染全球 1400 多万台 Android 设备

时间：2017 年 7 月。

事件：2017 年 7 月，网络安全厂商 Check Point 的研究人员表示，一种名为 CopyCat 的恶意软件已经感染了超过 1400 万台 Android 设备。CopyCat 会获取被感染手机的 Root 权限，

劫持手机应用，目前已经获得了数百万美元的欺诈广告收入，如图 4-3 所示。

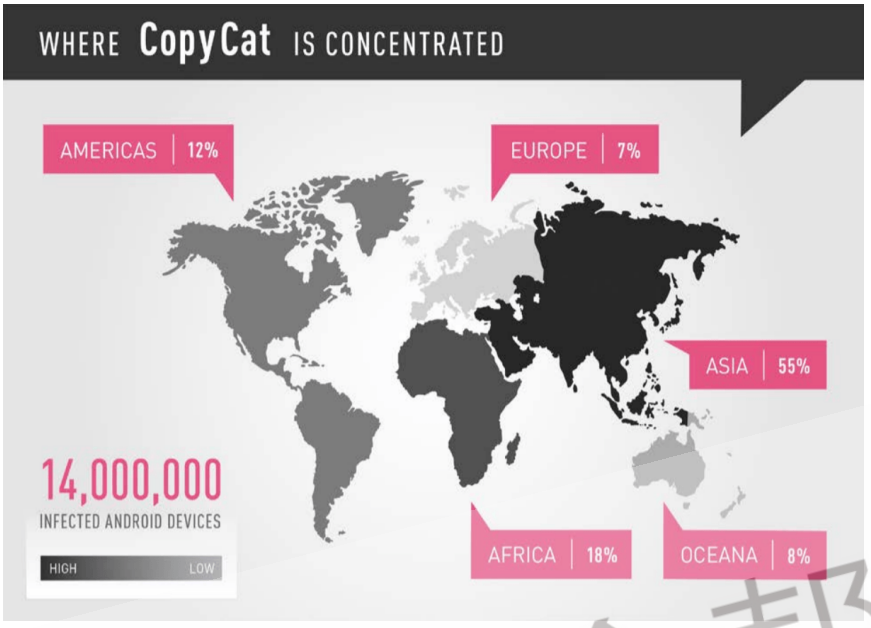


图 4-3 CopyCat 病毒感染全球 1400 多万台 Android 设备

谷歌过去 2 年一直在追踪 CopyCat，并且更新了 Play Protect，防止这款恶意软件继续感染用户的 Android 设备，但是仍然有很多的用户通过第三方应用市场下载软件和钓鱼式攻击中招。

据悉 CopyCat 的受害者主要集中在亚洲，印度、巴基斯坦、孟加拉国、印度尼西亚和缅甸是被感染比较严重的几个国家。另外，美国有超过 28 万台设备被感染，加拿大有超过 38.1 万台设备被感染。

CopyCat 是通过假冒其他流行应用来欺骗用户的。一旦用户下载了这种假冒的恶意应用软件，它就会收集受感染设备的数据，下载 Root 工具来劫持 Root 受感染的设备，从而切断其安全系统。然后，CopyCat 就可以下载各种虚假应用，劫持受感染设备的应用启动程序 Zygote。一旦它控制住 Zygote，就能知道你下载过哪些新的应用程序以及你打开的每一款应用程序。

CopyCat 可以用它自己的推荐者 ID（Referrer ID）替换受感染设备上的每一款应用程序的推荐者 ID，这样在应用程序上弹出的每一个广告都会为黑客创造收益，而不是为应用开发者创造广告收益。每隔一段时间，CopyCat 还会发布自己的广告来增加收入。

据 Check Point 介绍，CopyCat 还会检查被感染的设备是否位于中国境内，中国的用户不会受到攻击。Check Point 的研究人员认为这很可能是因为 CopyCat 背后的黑客是中国人，不攻击中国人是为了避开中国警方的打击。

总结：随着现在移动设备的快速发展，智能手机无疑是其中最大的宠儿。无论是从硬件配置还是操作系统方面都在高歌猛进中。智能手机市场也成为手机设备生产厂商的必争之地。

然而，一些黑客也早就意识到了智能手机中的商机。虽然 CopyCat 不会像 WannaCry 一样恶意加密用户资料，以删除资料威胁用户缴纳赎金，但是 CopyCat 强制获取用户设备的最高权限（Root）后，可以进行任意操作，使得用户信息泄露，设备安全受到了极大威胁。用户不得不重视移动设备安全，避免成为一些黑客的“肉鸡”，此外尽量不去下载未知来源的软件，并且及时更新安全漏洞。

4.4　BroadPwn 漏洞影响使用 Broadcom Wi–Fi 芯片的数百万台 Android 设备

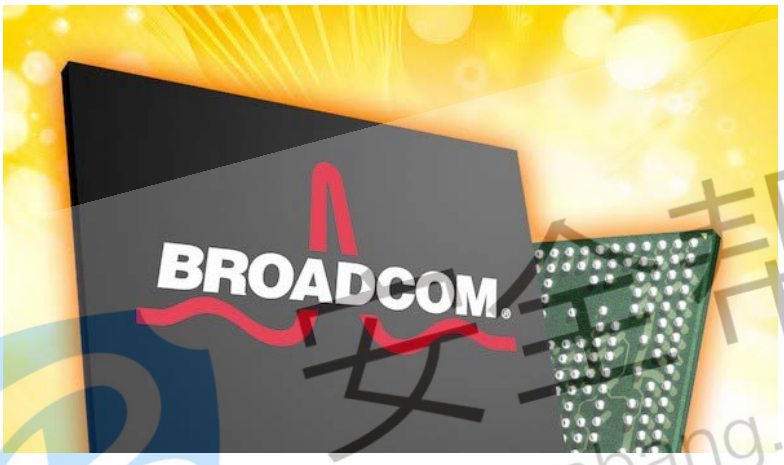


图 4-4　BroadPwn 漏洞将影响使用 Broadcom Wi-Fi 芯片的数百万台 Android 设备

时间：2017 年 7 月。

事件：2017 年 7 月，Exodus Intelligence 研究员 Nitay Artenstein 在博通 (Broadcom)Wi-Fi 芯片当中发现了一个漏洞，这个漏洞可怕到什么程度呢？只要在无线网络范围内，而且不管你是否已经连接特定的 Wi-Fi 网络，黑客就可以通过远程控制执行任意程序发起攻击，并且这个过程无需任何用户交互。谷歌也于 2017 年 7 月发布了一份关于 Android 设备的安全更新报告，警示 Broadcom Wi-Fi 芯片存在一处远程代码执行漏洞 BroadPwn（CVE-2017-3544），或将影响数百万台 Android 设备以及部分 iPhone 机型，如图 4-4 所示。

这个漏洞主要是 BCM43 系列，包括 BCM4354、BCM 4358 以及 BCM4359 Wi-Fi 芯片，除了谷歌、三星 Galaxy 从 S3 到 S8、HTC、LG 等众多安卓手机厂商外，iPhone 也难逃这个漏洞，不过好在 iPhone 7、iPhone 7 Plus 没有影响，因为它使用的是 Intel 的 Wi-Fi 芯片，截至 2017 年 7 月，估计全球至少有数百万台 Android 及 iOS 移动终端设备受影响。

据悉，Google 修补了数十个重要漏洞与 100 多个中等问题。此外，研究人员还修补了几个影响 Android Mediaserver 进程的关键漏洞，其中一些漏洞可能被攻击者远程执行恶意代码。值得注意的是，在 Mediaserver libhevc 库中存在漏洞（CVE-2017-0540）允许攻击者利用特制文件在媒体文件与数据处理的过程中损坏内存。

虽然 Google 已发布关于 Pixel 与 Nexus 设备的安全更新，但剩下的 Android 设备仍易遭受攻击。除非各原始设备制造商（OEM）能够立即检测并修复漏洞，不然无法完全解决当前问题。

总结：相比更为常见的系统（软件）上的漏洞，手机芯片暴露出的漏洞问题在严重性上要远超过前者。芯片漏洞会“潜伏”在一些软件中，趁机获取手机的 Root 权限，将用户的隐私资料进行泄露。在某些严重的情况下，甚至还有机会直接接管用户手机的所有功能，不管是 GPS、摄像头还是麦克风。而且与系统（软件）的漏洞不同，芯片漏洞更具广泛性和普遍性。比如说，某款软件被黑客植入了漏洞，但用户没有在自己的手机上安装，就可以避免受到该漏洞的攻击。但对于芯片漏洞来说，基本是百分之百“中招”。要是处理器出现了芯片级漏洞，那所有搭载这一处理器的手机都可能会受影响。芯片厂商应重视产品所出现的安全漏洞并进行积极修复，及时推出修复补丁并说明该（这些）漏洞出现的原因以及解决办法。

4.5 亚马逊 AWS S3 致 50 多万台汽车跟踪设备的登录凭证泄露

图 4-5 亚马逊 AWS S3 致 50 多万台汽车跟踪设备的登录凭证泄露

时间：2017 年 9 月。

事件： Kromtech 安全中心 2017 年 9 月发现 SVR Tracking 超过 50 万的记录暴露在网上。SVR Tracking 是提供车辆跟踪找回服务的一家美国公司，旨在提供服务帮助客户监控车辆以防被拖走或被盗。为了持续实时更新车辆位置，这家公司会在车辆不显眼的位置安装追踪设备，只是未经授权的司机不太容易注意到追踪设备。

SVR 官网的信息显示，跟踪设备持续跟踪汽车，只要用户正确登录 SVR 应用程序（笔记本、台式电脑和移动设备均可下载使用），就能清晰了解到过去 120 天车辆所在位置。

Kromtech 安全中心发现 SVR 将数据存放在公开可访问的亚马逊 S3 云存储中，包含近

54 万（540，642）个 SVR 账户的信息，包含电子邮箱和密码，车牌号和车辆识别号码（VIN）。

数据包括：116 GB 的每小时备份数据、2017 年 8.5GB 每日备份数据、339 份“日志”文件等。

SVR 密码经过哈希处理或使用其他随机数据——但使用的却是最弱的加密算法（SHA-1），这就意味着黑客无需太多时间便能破解这些密码。鉴于许多经销商或客户有大量跟踪设备，因此设备总数量可能更多。Kromtech 率先发现 SVR 数据泄露问题，并于 2017 年 9 月 20 日报告给 SVR，几小时内 SVR 关闭了这台服务器。

AWS S3 云存储成了数据泄露重灾区，Kromtech 早些时候发现时代华纳公司约 400 万条客户个人可识别信息在线泄露。安全公司 UpGuard 上月底发现全球第六大传媒公司 Viacom 也因此遭遇数据泄露事件。此外，Kromtech 还发现超过 8.86 万信用卡、护照照片和其他形式的 ID 暴露在网上。2017 年 5 月，Kromtech 宣布发现 5.6 亿多条登录凭证因配置不当的数据库暴露在网上。

总结：对于云上数据库的安全技术，数据库安全厂商可以从数据库访问、数据库加密、数据库防护墙和数据库审计 4 个方向考虑。云服务厂商如果能把这 4 种安全手段应用到用户的云数据库上，将提高云数据库的安全性。云服务虽然能带来更低的价位、更好的效率、更佳的灵活性，但安全性很可能是制约云服务厂商进一步发展的障碍。解决云上的安全问题将更有益于云厂商自身的发展，同时也是一种对用户负责的表现。

4.6　Stackoverflowin 黑客入侵 15 万台打印机

时间：2017 年 2 月。

事件：2017 年 2 月，国外一个自称“stackoverflowin”的黑客侵入了超过 15 万台打印机，被入侵的这些打印机全部都打印出了这名黑客留下的警告信息，如图 4-6 所示。

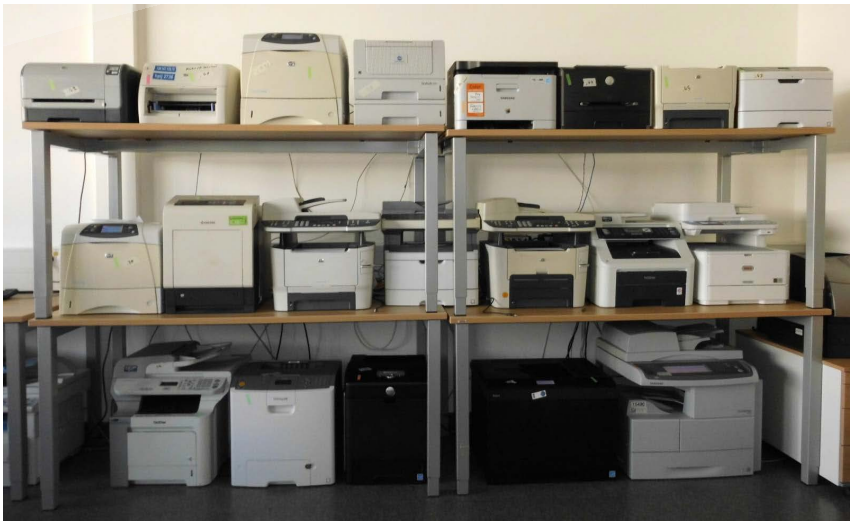


图 4-6　黑客入侵致 15 万台打印机被黑

不过据他本人声称，他控制这些打印机的目的是为了提高人们对打印机安全的认识，打印机在安全这块儿实在太薄弱了。如果你的打印机会不受控制地打印“YOUR PRINTER HAS BEEN PWND‘D’”，那就说明你的打印机已经沦陷了。

这次“攻击”其实只是个脚本，在 24 小时内，Stackoverflowin 就跑着一个他心爱的小脚本，搜索打开的打印机端口，搜索到符合条件的打印机给该打印机发送一个打印作业。大到企业总部的多功能打印机，小到餐馆收据打印机多多少少都受到了影响。

Stackoverflowin 会控制打印机输出各种信息，最新的一条是这样写的：“你们的黑客之神 Stackoverflowin 回来了，这台打印机已经是火焰僵尸网络的肉鸡之一了，想办法修好你们的打印机吧。有问题？ Twitter 找我。”

许多受害者都反映他们的打印机会打印出奇怪的内容，受到影响的品牌包括 Afico、Brother、佳能、爱普生、惠普、利盟、柯尼卡美能达、Oki 和三星。如果你发现你的打印机也开始默默打印奇怪的东西，那么可能意味着你需要关闭路由器的 9100 端口——这是黑客发出打印作业的方式。要确保打印机不会因为公开的 IP 地址而被入侵，首先要做的就是在路由设置中确立明确的规则，如白名单机制或者建立一个私有虚拟网络。

Stackoverflowin 表示，他写的脚本主要针对的目标就是那些 IPP（互联网打印协议）端口、LPD 端口和 9100 端口向外部开放的打印设备。这个脚本针对 Dell Xeon 的打印机还包含了一个远程代码执行漏洞的 Exploit。借助这个漏洞，就能注入 PostScript，完成强制远程打印工作。Stackoverflowin 解释，他所做一切都是出于好意，这些其实是他对安全工作的做法。

总结：除了让打印机打印一个鬼脸、打印不明来源的内容之外，黑客入侵还有可能的操作包括从发送打印任务、损坏存储到获取打印机内部数据、密码，甚至安装恶意程序、更新未知固件。目前打印机固件的安全性采用识别码来验证，而第三方软件则由厂商严格认证的开发者和开发环境来完成，各厂商未公开的代码认证系统保证打印机软件包的正当性。这些措施在很大程度上避免了恶意固件或软件包被安装到打印机上；然而权限管理的先天缺陷仍然让打印机的底层系统暴露在外，不排除未来遭遇新的攻击方式的可能性。

4.7 智能泰迪熊玩具泄露 200 多万条亲子聊天记录

时间：2017 年 3 月。

事件：互联网填充智能玩具 CloudPets（泰迪熊）暴露了 200 多万条儿童与父母的录音、以及超过 80 万个账户的电子邮件地址和密码。

安全研究员发现，这些用户数据存储在一个公开的 CloudPets 数据库中，没有被密码或者防火墙保护，攻击者无需身份验证即可访问。此外，有证据表明已经有攻击者访问了数据库，还删除了数据并索要赎金。研究人员还称至少联系了 CloudPets 泰迪熊智能玩具的制造商 Spiral Toys 共 4 次，告知其数据库漏洞，但没有收到回复。

图 4-7　智能泰迪熊玩具泄露 200 多万条亲子聊天记录

这已经不是第一次提到智能玩具泄露用户的隐私数据。此前，德国政府监管机构联邦网络局就发出警告，家长应尽快销毁一些为他们孩子设计的可连接互联网的智能玩具。起因就是因 My Friend Cayla 严重缺乏安全功能可被黑客控制，并泄露儿童隐私信息。

总结：随着科技和网络的发展，智能玩具越来越多的出现在市面上，随着中国儿童消费市场年增长率逐渐提升，儿童智能玩具有望形成万亿级别的市场。各大电商平台上，智能故事机、智能机器人较为常见，其中有些产品可实现远程监控，父母下载 APP 后，还能听到孩子和机器人聊天，儿童信息加工可形成详尽的“家庭档案”，玩具厂商易陷数据泄露门，需提高安全性。目前企业掌握的数据量、数据价值和数据安全防护能力之间是不匹配的，所以数据泄露的风险非常严重，当务之急，一要督促玩具厂商提高自身产品和服务的安全性；二要规范厂商收集、使用数据的行为，特别是共享和转让。

4.8　美国一大学 5000 余台 IoT 设备遭受 DDoS 攻击

图 4-8　美国一大学遭到 5000 余台校园物联网设备 DDoS 攻击

时间：2017 年 2 月。

事件：美国一大学校园网遭到 DDoS 攻击，大批学生表示网速非常慢。经校方人员调查后发现，发起 DDoS 攻击的正是校园周围 5000 多台 IoT（物联网）设备构成的僵尸网络。在这些受感染 IoT 设备中，大多是校园内的自动售货机。

威瑞森公司在其《2017 年数据泄露文摘》的前瞻报告中详细描述了这起校园 DDoS 攻击事件。

据悉，当时该大学的网速非常慢，学生们的抱怨越来越多，IT 人员立马展开了调查。调查发现学校的 DNS 服务器因为大量的流量负载而宕机。大多数流量来自于一个僵尸网络，这些流量很反常，只对二级域名发送连接请求。经过进一步调查后，发现校园周围的 5000 多台 IoT 设备遭到恶意软件感染，攻击者通过猜测默认密码的方式达到远程操控僵尸网络的目的。

最终，工作人员成功拦截了包含僵尸网络明文密码的网络数据包。在这之后他们写了一个脚本，清除了校园里所有受感染机器里的恶意软件。

总结：近年校园物联网安全事件频发，一方面是由于校园网内设备复杂，联网设备多，存在大量弱口令和漏洞威胁；另一方面这些思维活跃动手能力强的大学生们喜欢捣鼓网络。其实，这样的攻击一直都存在，只是集中爆发才被发现。另一个同样容易遭受此类攻击的就是企业。所以建议企业应该密切地关注 IoT 设备的网络设置，并尽可能将其与互联网和其他设备的访问分开。他还建议将物联网设备与常规 IT 资产清单一起使用，并使用基本安全措施，比如更改默认凭据和轮换强大的 Wi-Fi 网络密码。

4.9 “橙风单车”投用次日遭黑客攻击，5000 台车被迫停工

图 4-9 “橙风单车”投用次日遭黑客攻击，5000 台车被迫停工

时间：2017 年 8 月。

事件：2017 年 8 月，冰城市民向反映，“橙风单车”不能使用了。原来，由于这些单车投用第二天就遭到黑客攻击，导致系统瘫痪，用户无法正常使用。9 日，目前投放单车的哈尔滨市跨越科技有限公司已经向警方报案。

9 日，哈尔滨市跨越科技有限公司松北区的办公地点整齐地排列着数千辆共享单车，一位工作人员正将写着“网络故障暂停使用”字样的纸壳放在醒目位置。据该公司相关人员介绍，公司是冰城的本土企业，为响应政府号召，推行绿色出行、节能减排等出行理念，于 8 月 4 日在道里区和南岗区的繁华街路，投放 5000 台“橙风单车”。没想到， 5 日下午就有用户称单车无法正常解锁。客服立即将相关情况汇报给后台管理中心，单车生产厂商进行“会诊”后，断定车锁没有问题。于是跨越科技公司花高价对系统进行升级，谁料 7 日后事情更严重了，多个用户投诉单车无法正常使用。该公司后台同时发现，管理系统遭到大批黑客连续攻击，5000 台共享单车被迫停工。由于新用户无法注册，导致客服每天接百余个投诉电话。一些用户投诉称，打开“橙风单车”APP，新用户注册无法接收到验证信息；老用户扫码解锁后，却显示“请检查网络”，车辆无法使用。8 日夜间哈尔滨市跨越科技有限公司报警称，该公司服务器遭遇黑客攻击。由于该公司服务器在沈阳，按照规定，由沈阳警方处理后续事宜。

总结：企业要加强网络安全建设，预防黑客攻击。除了外部安全威胁，共享单车企业更要严格规范公民个人信息的收集，遵循合法、正当、必要的原则，在必要的范围内合规使用数据，落实网络安全等级保护制度，禁止数据非法出境，向他人提供数据时要注意数据脱敏清洗，尤其注意对涉及个人信息及国家秘密的地理信息的管理。

4.10　新型恶意软件 Cutlet Maker 暗网售价 5000 美元

时间：2017 年 10 月。

事件：据外媒报道，卡巴斯基实验室研究人员于 2017 年 5 月发现黑客组织在暗网论坛 ATMjackpot 出售一款新型 ATM 恶意软件 Cutlet Maker，可以通过侵入特定 ATM 供应商的 API 接口后清空设备所有现金，而无需与银行用户及其数据进行交互。目前，该恶意软件售价 5000 美元，如图 4-10 所示。

调查显示，Cutlet Maker 起先于暗网 AlphaBay 出售，但随着美国 FBI 的审核调查后，该网站于 2017 年 7 月关闭。不过，知情人士透露，该恶意软件开发人员又重新创建了一个暗网市场 ATMjackpot，专门出售 Cutlet Maker。此外，有消息指出，该恶意软件工具包除了所需设备、目标 ATM 机模型以及恶意软件操作的提示与技巧外，还提供了一份详细的手册说明以便用户轻松查看。

研究人员表示，该恶意软件可分为 CUTLET MAKER 与 Stimulator 两大模块。

CUTLET MAKER：主要负责侵入 ATM 机的 API 接口后分配资金。其程序由开发人员

采用 Delphi 编写，并利用 VMProtect 等多个应用进行包装。

图 4-10　新型恶意软件 Cutlet Maker 暗网出售，仅用 5000 美元即可掏空 ATM

Stimulator：该模块主要用于获取 ATM 机转储内容并查询设备余额，其程序也采用 Delphi 编写，并使用与“CUTLET MAKER”相同的方式进行包装。

据称，CUTLET MAKER 和 Stimulator 显示了网络犯罪分子如何使用合法的专有数据库和恶意代码从 ATM 中分配资金。不过，此类恶意软件不会直接影响到银行客户，因为它只是为了从特定供应商的 ATM 中窃取现金。目前，研究人员建议各银行供应商加强 ATM 设备的防御措施以防黑客攻击。

总结：计算机网络在大大增强了网络信息服务灵活性的同时，也给黑客攻击和入侵敞开了方便之门。不仅传统的病毒借助互联网加快了其传播速度并扩大了其传播范围，而且各种针对网络协议和应用程序漏洞的新型攻击方法层出不穷。银行的计算机网络系统已成为一些黑客侵犯的对象和渠道，不仅影响了网络稳定运行和用户的正常使用，造成重大经济损失，而且还会威胁到国家金融安全，因此网络系统的安全性和可靠性成为银行工作的重心。

第五章

2017 十大物联网恶意软件分析

早期，网络病毒、蠕虫入侵的对象只是计算机，随着物联网时代的到来，物联网恶意软件兴起，入侵的对象由电脑转向网络摄像头和路由器。物联网时代，最害怕的就是僵尸网络。由于我们网络安全意识不足和日益增长的无安全保障产品，近年来，僵尸网络危害迅速增长，本章节将对 2017 年十大物联网恶意软件进行详细解析。

5.1　Mirai

日期：2017 年 4 月 4 日。

事件：Mirai 僵尸网络新变种发起 54 小时 DDoS 攻击，最高峰值刷新纪录。

事件描述：据云安全公司 Incapsula 的监测，一所美国大学于 2017 年 4 月 4 日遭到 Mirai 变种僵尸网络的 DDoS 攻击（分布式拒绝服务攻击）。而该攻击竟然持续了 54 小时，总计产生超过 28 亿次的访问请求，严重影响了这所高校网站的正常运行。其平均攻击流量为每秒 3 万次请求，巅峰时为每秒 3.7 万次的请求，在持续 54 小时的攻击中，总计累积了超过 28 亿次的请求。此次攻击事件打破了 Mirai 僵尸网络有史以来最高记录。Mirai 的攻击方式如下：发起攻击的僵尸网络主要由闭路电视摄像机头、DVR 和路由器组成。攻击者可能利用已知 IoT 设备漏洞打开 Telnet（23）端口和 TR-069（7547）端口。Mirai 攻击频率如图 5-1 所示。

图 5-1　Mirai 攻击频率

事件总结：Mirai 新变种由源代码泄露导致。Mirai 僵尸网络之前通过网络层展开 DDoS 攻击，而新变种则利用应用层进行攻击。此次攻击中使用的 DDoS 僵尸网络采用不同的用户代理，而非曾在默认 Mirai 版本中出现的 5 个硬编码样例。在 Mirai 源代码被公布后，基于 Mirai 僵尸网络的活动就日渐猖獗。另需注意的是，原本 90% 以上针对网络应用层的攻击不会超过 6 小时，但在此次攻击中却持续了 54 小时，暴露出面向网络应用层的 DDoS 攻击已成为新趋势。分析显示，攻击流量来自全球 9,793 个 IP 地址，超过 70%的设备位于以下国家及地区：美国（18.4%）、以色列（11.3%）、台湾（10.8%）、印度（8.7%）、土耳其（6%）、俄罗斯（3.8%）、意大利（3.2%）、墨西哥（3.2%）、哥伦比亚（3.0%）和保加利亚（2.2%）。

5.2 BrickerBot

日期：2017 年 4 月 11 日。

事件描述：网络安全供应商 Radware 发现了一个名为 BrickerBot 的面向基于 Linux 的物联网（IoT）设备的新型恶意软件程序。

BrickerBot类似于Mirai，这是破坏性的恶意软件程序，它将IoT设备引入到了拒绝服务（DDoS）攻击的僵尸网络中。像 Mirai 一样，BrickerBot 会攻击未更改默认用户名和密码的不安全设备。

一旦进入不安全的设备，BrickerBot 将开始永久删除存储并撤销 Internet 访问，从而有效地杀死了设备，这是 Mirai 与 BrickerBot 的主要区别。Mirai 使用 IoT 设备，而 BrickerBot 使它们无法使用。这种攻击似乎在理论上看起来容易脱落，因为所有的攻击者都需要远程访问 IoT 设备，而许多设备通过采用糟糕的认证和加密技术的路由器连接到互联网。

事件总结：

BrickerBot 与我们以前看到的任何物联网恶意软件不同，大多数物联网恶意软件愿意囤积大量的僵尸网络设备，然后用作代理中继或发动 DDoS 攻击，这是有利可图的。而 BrickerBot 的目的是破坏。虽然不知道制作 BrickerBot 程序的幕后黑手真实目的是什么，但其无疑对物联网设备是一个巨大威胁，不仅可以瘫痪家中的家电，而且还可以让一些关键位置的监控摄像头失灵。

针对上述情况，建议物联网用户应经常更换自家系统的用户名和密码，对设备所有者而言，一旦他们的设备不够安全，他们必须重新安装固件，甚至购买新的设备。

5.3 Persirai

日期：2017 年 4 月 26 日。

事件：新型 IoT 僵尸网络 Persirai 一举攻陷 12 万台 IP 摄像机。

事件描述：僵尸网络 Persirai 利用恶意软件 ELF_PERSIRAI.A 进行不断传播感染。一个月内，多家原始设备制造商（OEM）的 1000 多种型号网络摄像头产品受此恶意网络感染。

图 5-2 是 2017 年 4 月 26 日的 Persirai 感染趋势图，从图 5-2 中可以看出，中国是该类僵尸网络感染的重灾区，仅大陆地区的感染率就高达 20.3%。

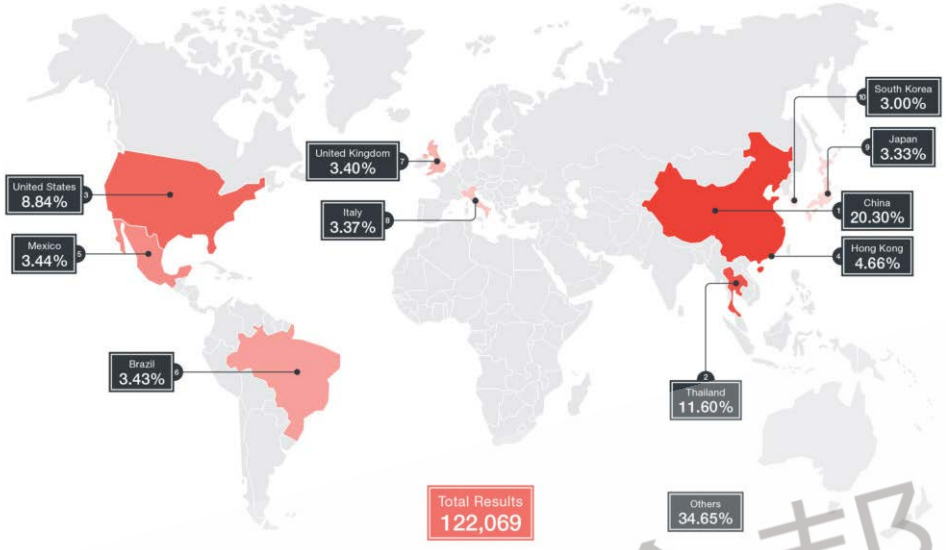


图 5-2　Persirai 感染趋势

僵尸网络 Persirai 的感染方式是这样的：通常，在用户内部网络中，网络摄像头通常可以使用路由器的即插即用协议 (UPnP) 功能进行端口映射，使得用户可以通过广域网远程访问到设备，而这也带来了感染 IoT 恶意软件的风险。Persirai 正是利用恶意软件 ELF_PERSIRAI.A，对暴露在公网的网络摄像头进行传播感染。

事件总结：在 Mirai 轰轰烈烈成为首个感染 IoT 设备的恶意软件之后，其代码的开源性特点也会成为未来 IoT 类恶意软件的可用之处。随着物联网时代的到来，网络犯罪分子将会从传统的 NTP 和 DNS 服务中脱离开来，使用 IoT 设备发起 DDoS 攻击。而对普通 IoT 设备用户来说，其对设备采取的脆弱安全性措施将会加剧物联网安全问题的严重性。

默认密码、出厂密码、弱口令都将会是攻击者进行攻击利用的途径。然而，以上分析也表明，即使是强壮口令也不能免于攻击。除此之外，物联网设备使用者应该采取多种手段来防止攻击，如禁用路由器中的 UPNP 功能以免于 IoT 设备和端口的暴露在线、及时更新固件等。当然，IoT 安全也不完全是终端用户的事，还需要设备制造商供应商在生产环节把好安全生产关，才能共筑未来物联网安全。

5.4　Hajime

日期：2017 年 4 月 29 日。

事件：僵尸网络 Hajime 实施新型攻击方式，劫持逾 30 万 IoT 设备。

事件描述：从 2017 年年初开始，被称为 Hajime 的僵尸网络成功地感染了超过 30 万种

互联网设备，这标志着制造商无法继续保护他们的网络连接设备。僵尸网络主要使用两种攻击方法，专注于强力猜测密码或利用默认密码。例如，一个模块专注于 Arris 电缆调制解调器，并使用密码根据当前算法登录到具有激活功能的设备。自 2009 年以来，该漏洞已被公认。Hajime 比 Mirai 更加复杂，实现了隐藏其活动与运行进程的更多机制。调查表明，该威胁具有允许运营商快速添加新型功能的模块化结构。分析报告显示，Hajime 并未执行分布式拒绝服务（ DDoS ）攻击或其他任何攻击代码，而是从控制器中提取语句并每隔 10 分钟在 IoT 终端上显示一次。Telnet 默认密码攻击如图 5-3 所示。

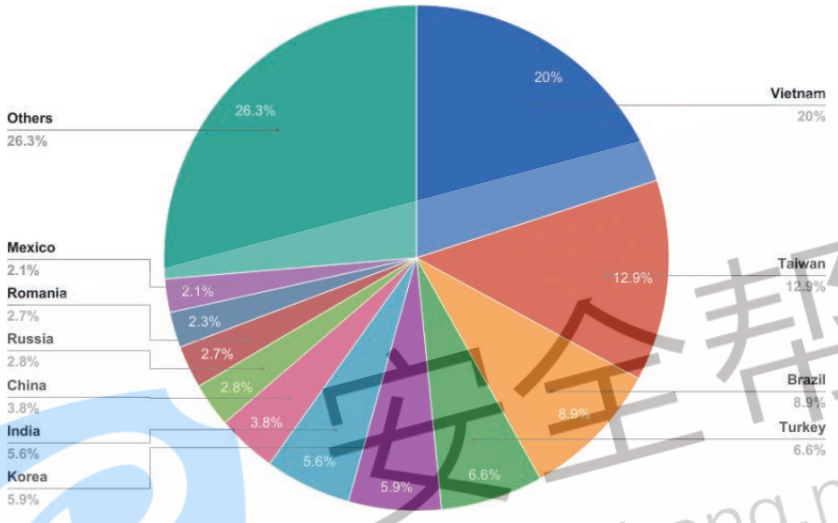


图 5-3　Telnet 默认密码攻击

事件总结：专家发现，僵尸网络 Hajime 几乎可以针对互联网上的任何设备发动攻击。在卡巴斯基研究人员看来，Hajime 最耐人寻味的在于动机。截至目前，攻击模块中引入 TR-069 协议的做法使僵尸网络规模日益扩大，但具体动机仍不为人知。尽管暂未发现僵尸网络 Hajime 被用于任何类型攻击或恶意活动，仍建议 IoT 设备用户将密码更改为难以暴力破解的形式并尽可能更新固件。

5.5　http81

日期：2017 年 5 月 8 日。

事件：http81 新型僵尸网络来袭国内超 5 万台摄像头遭控制。

事件描述：在 Mirai 僵尸网络攻击造成美国东海岸大面积断网事件之后，2017 年 4 月中旬起，国内也出现了控制大量 IoT 设备的僵尸网络。在 4 月 15 日发现 http81 僵尸网络活跃度异常增加，当日扫描事件数量比平时增长 4 倍到 7 倍，独立扫描 IP 来源增长幅度达到 40 倍到 60 倍，如图 5-4 所示。4 月 22 日，http81 活跃度更是达到高峰，扫描来源的 IP 地址超过 57,000 个。与普通僵尸网络 100 到 1000 个 IP 节点的规模相比，两周后 http81 已经成为一个巨型僵尸网络。http81 僵尸网络在中国已经感染控制了超过 5 万台网络摄像头。如果按照

每个活跃 IP 拥有 10Mbit/s 上行带宽测算，http81 僵尸网络可能拥有高达 500Gbit/s 的 DDoS 攻击能力，足以对国内互联网基础设施产生重大威胁。

图 5-4　http81 僵尸网络分布

事件总结：当 http81 僵尸网络被公开曝光后，开始变得更加低调和隐蔽。http81 控制主机域名的 IP 地址已改为私网 IP 地址，其扫描行为也明显下降，暂时停止了大规模扫描。但是由于国内的网络摄像头等设备大多缺乏安全更新维护，只要 http81 的恶意代码没有被摄像头运维人员清除，攻击者随时可以控制主机重新上线。如果任由 http81 僵尸网络扫描感染更多设备，其防御难度也会越来越高。

5.6　Stantinko

日期：2017 年 8 月 2 日。

事件：神秘僵尸网络 Stantinko 潜伏 5 年感染逾 50 万系统设备。

事件描述：僵尸网络 Stantinko 于过去 5 年内一直处于雷达控制状态，其成功感染逾 50 万台计算机设备，并允许攻击者在受感染主机上执行任意操作。自 2012 年以来，僵尸网络 Stantinko 为大规模恶意软件活动提供动力，其主要针对俄罗斯与乌克兰等国家。由于该僵尸网络具备加密代码及迅速适应能力，可规避安全软件检测。Stantinko 是一款模块化后门，其中包括加载程序执行服务器并直接在内存中发送任何 Windows 可执行文件。由于插件系统较为灵敏，攻击者可在受感染系统上执行任意代码。Stantinko 的传播方式如下：为检测受感染用户设备，攻击者使用应用程序 FileTour 作为初始感染媒介，能够在受害者设备上安装各种程序，同时启动僵尸网络 Stantinko 进行传播。Stantinko 不仅会安装浏览器扩展、执行广告注入与点击欺诈，还能在 Windows 服务中执行任意操作（例如：后门攻击、Google 搜索以及强制操控 Joomla 与 WordPress 管理员面板等）。

事件总结：僵尸网络在攻击后将会安装两款恶意 Windows 服务，每款均具备重新安装其他程序的能力，因此用户必须同时删除这两款程序才能完全去除恶意软件。目前，僵尸网络幕后黑手正试图通过多款恶意活动访问 Joomla 与 WordPress 网站管理账户，并在暗网转售账户登录凭证，或是通过与 Facebook 交互插件进行社交网络欺诈。

虽然这一僵尸网络对用户来说影响并不广泛，不太占用 CPU，但它仍是极大的威胁，因为它为网络犯罪分子提供了充足的欺诈收入来源，它为网络犯罪分子的欺诈行为带来了丰厚的金钱收入。此外，Stantinko 还存在一个功能齐全的后门程序，允许恶意软件操作人员全面监视和控制所有的受感染主机。此外，功能齐全的 Stantinko 后门还能允许攻击者监视所有受害设备。

5.7 WireX

日期：2017 年 8 月 2 日

事件：僵尸网络 WireX：黑客利用数十万 Android 设备发动 DDoS 攻击

事件描述：WireX 最早出现在 2017 年 8 月 2 日，当时发现有少数的 Android 设备受到黑客的在线攻击。之后不到两个星期，被 WireX 感染的 Android 设备数量已经多达数万台。更令人担忧的是，僵尸网络的肇事者目前还控制着酒店行业中的几个大型网站，他们给这些网站制造大量的垃圾请求，造成真正的访问者无法访问网站。攻击者利用官方应用商店传播的恶意程序创建 Android 僵尸网络发动 DDoS 攻击。据悉，被称为 WireX 的僵尸网络在其高峰时最高控制 100 多个国家逾 12 万 IP 地址。然而，当前各企业很难抵御这种 IP 地址遍布全球的 DDoS 攻击。专家通过跟踪攻击事件很快就定位出了运行 WireX 的恶意软件，它们分散在 GooglePlay 中大约 300 种不同的移动应用中，包括视频播放器、铃声或者文件管理器之类的简单工具，常见的软件名为 Network、Filter File、Storage Data、Storage Device、Analysis。Google 经证实后，紧急下架部分应用以减少目标设备沦为 DDoS 攻击的动力来源。据悉，这些应用程序多数由俄罗斯、中国与其他亚洲国家的用户下载，尽管 WireX 僵尸网络当前仅在小规模攻击活动中处于活跃状态。

事件总结：在该 Android 僵尸网络膨胀到难以控制前，包括 Cloudflare、Akamai、Flashpoint、Google、Dyn 等在内的科技公司已积极采取行动并对其进行联合打击。此外，如果用户设备运行的是 Android 操作系统的最新版本，那么该系统中包含的 Google Play Protect 功能将会自动移除已下载的恶意 WireX 应用。目前，研究人员建议用户从 Google 官方商店下载应用程序，并始终在移动设备上保持全方位杀毒软件，以便在感染设备前阻止恶意程序下载。

5.8 Rowdy

日期：2017 年 8 月 5 日。

事件：Mirai 变种 Rowdy 物联网恶意软件袭击我国有线电视网 [34]。

事件描述：我国有线电视终端设备——电视机顶盒于 2017 年 8 月受到 DDoS 攻击事件。攻击类型多样，包括 TCP Flood、HTTP Flood、DNS Flood 等。通过对攻击源 IP 进行溯源，发现攻击来自有线电视的终端设备——电视机顶盒。Rowdy 的传播机制是这样的：它一旦植入机顶盒，就立即扫描，发送大量的数据包，并不断地与控制服务器通信，发现其功能及行为特征与物联网恶意软件 Mirai 极为相似。经过对比发现，Rowdy 其 bot 上线方式与 Mirai 相同，DDoS 攻击代码一致，代码结构基本无变化，基于这些特征已经可以确定，Rowdy 样本是 Mirai 物联网恶意软件的变种，虽然入侵方式同样是破解设备弱口令，但采用加壳措施进行自我保护，并采用一定的算法隐藏控制服务器地址，通信端口 1992。

事件总结：Mirai 恶意软件经过改造后，实现了从摄像头等视频监控系统向机顶盒物联网设备的跨越，这无疑大幅度扩展了其传播范围。Rowdy 在短短数月时间已经形成了规模不小的 Bot 僵尸网络，感染的设备涉及国内 5 家厂商。国内的机顶盒使用量有多大？据国家统计局 2 月份发布的《中华人民共和国 2016 年国民经济和社会发展统计公报》显示，该设备实际用户到达 2.23 亿户，同时据奥维云网《2017 年中 OTT 运营大数据蓝皮书》显示，该设备实际用户达到 2.4 亿台。如此庞大的网络，一旦被 Rowdy 快速渗透，带来的后果不堪设想。

在跟踪调查中发现，Rowdy-Bot 僵尸网络已经开始向外发起 DDoS 攻击，监控到的国内受控制僵尸主机已达 2000 多台，如图 5-5 所示。

图 5-5　国内各地区感染情况

5.9　Linux.ProxyM

日期：2017 年 9 月 25 日。

事件：新型 IoT 僵尸网络 Linux.ProxyM 通过感染 Linux 设备发送钓鱼邮件，开展 DDoS

攻击活动。

事件描述：

从 2017 年 5 月起，僵尸网络 Linux.ProxyM 异常活跃，迄今为止已感染设备 1 万多台，如图 5-6 所示。

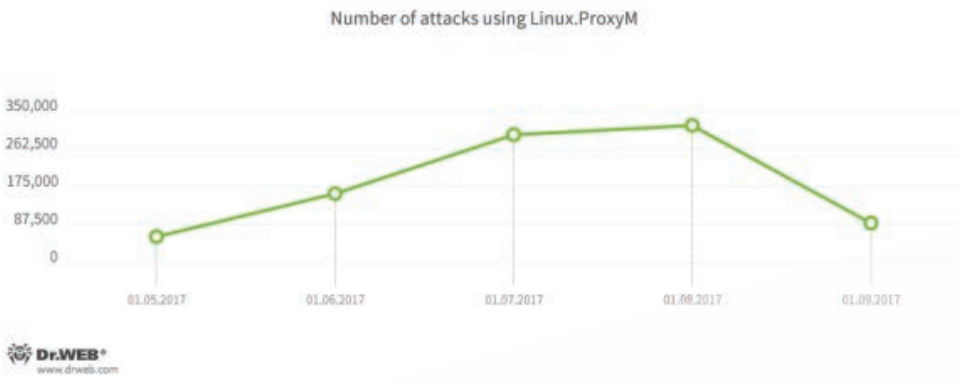


图 5-6　Linux.ProxyM 攻击次数

Linux.ProxyM 感染设备的方式是这样的：通过分发钓鱼邮件引导诱导用户运行其中涵盖的恶意软件，一旦点击，僵尸网络 Linux.ProxyM 所分发的恶意软件能够在任何 Linux 设备（包括路由器、机顶盒与其他设备）上运行、同时还可以可规避安全检测。当一台设备被感染后，它都能够连接至命令与控制服务器，并下载两个互联网节点域名。如果用户在第一个节点提供登录凭证，那么跳转至第二个节点时将通过服务器发送一个包含 SMTP 服务器地址命令，用于访问用户登录凭据、电子邮件地址和邮件内容。此外，据相关数据显示，每台受感染的设备平均每天可以发送 400 封这样的钓鱼邮件。

僵尸网络 Linux.ProxyM 感染范围很广，巴西被僵尸网络 Linux.ProxyM 攻击的比例最高，同时，美国、俄罗斯、印度、墨西哥和意大利等国家都受到不同程度的影响，如图 5-7 所示。

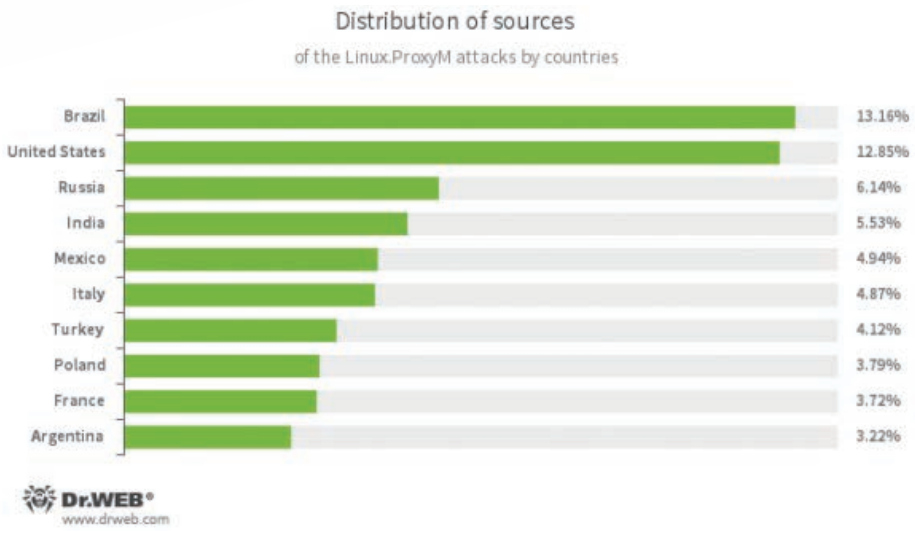


图 5-7　感染国家分布情况

事件总结：截至目前，尚不了解黑客攻击的真正意图是什么，但随着物联网的发展，针对物联网的攻击活动逐渐成为网络犯罪攻击的焦点，因此，黑客可能会继续扩展 Linux 木马执行的范围，开展 DDoS 攻击。

5.10　IoTroop（Reaper）

日期：2017 年 10 月 23 日。

事件：CheckPoint：新 IoTroop 僵尸网络恐带起另一波风暴。

事件描述：新的僵尸网络 IoTroop 正在快速增长，在过去的一个月里已经感染了 100 万家企业和机构，其中包括医院，国家运输系统，通信公司和政治机构，将带来超过 Mirai 的安全威胁。IoTroop 属于锁定物联网（IoT）装置的僵尸网络，它透过同样的恶意程序感染全球的 IoT 装置，让黑客自远端控制这些大量的 IoT 装置，并执行分散式阻断服务攻击（DDoS），攻击对象从医院、运输系统到政治组织不等。IoTroop 控制的 IP 增长趋势如图 5-8 所示。

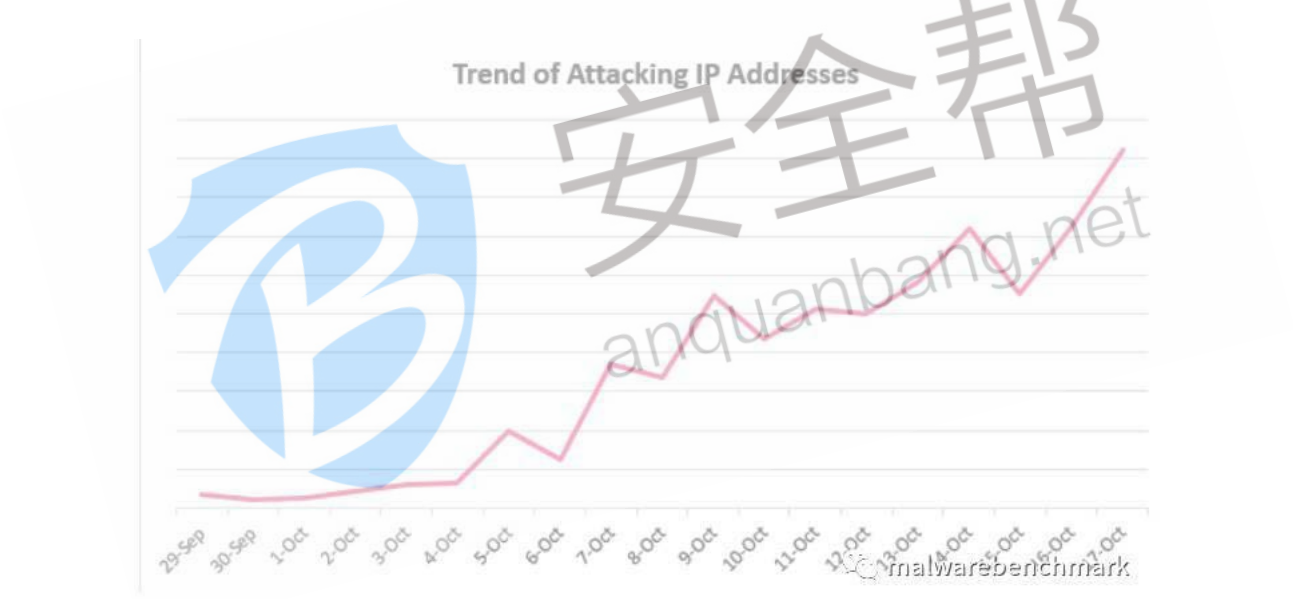


图 5-8　IoTroop 控制的 IP 增长趋势

事件总结：自 9 月侦测到 IoTroop 的存在后，研究人员发现它的扩散速度非常地快，主要是因 IoT 本身就能散布恶意程式，且所开采的漏洞也愈来愈多，众多品牌的无线监视器皆已遭到感染，涵盖 GoAhead、D-Link、TP-Link、AVTECH、NETGEAR、MikroTik、Linksys 及 Synology 等。虽然 IoTroop 是个新的僵尸蠕虫，然而它与 2016 年酿灾的 Mirai 使用许多同样的代码，但 IoTroop 更先进、功能更复杂，它开采的不只是 IoT 装置的预设凭证，还能开采漏洞，它更加复杂，除了弱凭证，还使用了十几个或更多的漏洞来获取这些设备。预期其僵尸网络规模将更甚于 Mirai，可能带来更大的灾难。

第三部分
物联网安全防护体系

第六章

物联网安全防护体系

从物联网的威胁和挑战来看，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。

由于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。

即使分别保证了感知层、网络层、平台层和应用层的安全，也不能保证物联网的安全。这是因为物联网是融合几个层次于一体的大系统，许多安全问题来源于系统整合；物联网的数据共享对安全性提出了更高的要求；物联网的应用对安全提出了新要求，比如隐私保护不是单一层次的安全需求，但却是物联网应用系统不可或缺的安全需求。

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，其安全防护措施能够不断完善。

6.1　物联网安全体系架构

6.1.1　设计原则

（1）由于物联网终端和网端节点可能处于无人值守的环境中，所以物联网终端的本地安全相较于现有通信网络终端的安全问题更加巨大，因此需要更加重视物联网终端和网端节点的安全性。

（2）物联网具有节点数量巨大、网端节点组群化、低移动性等特点，而且，一般的物联网终端携带能量有限，因此需要针对物联网的这些特点定制更加符合物联网特性的、低能耗的安全要求。

（3）物联网中轻量级的，特定的安全要求将会使得物联网安全机制与现有网络安全机制略有不同。但是，由于物联网尽可能地复用了现有网络，因此物联网安全保护强度不能低于

现有网络安全强度，避免在现有网络中制造安全薄弱环节 [3]。

6.1.2 安全体系架构整体设计

物联网的安全架构包括感知层安全、网络层安全、平台层安全、应用层安全、统一安全管理平台，如图 6-1 所示。

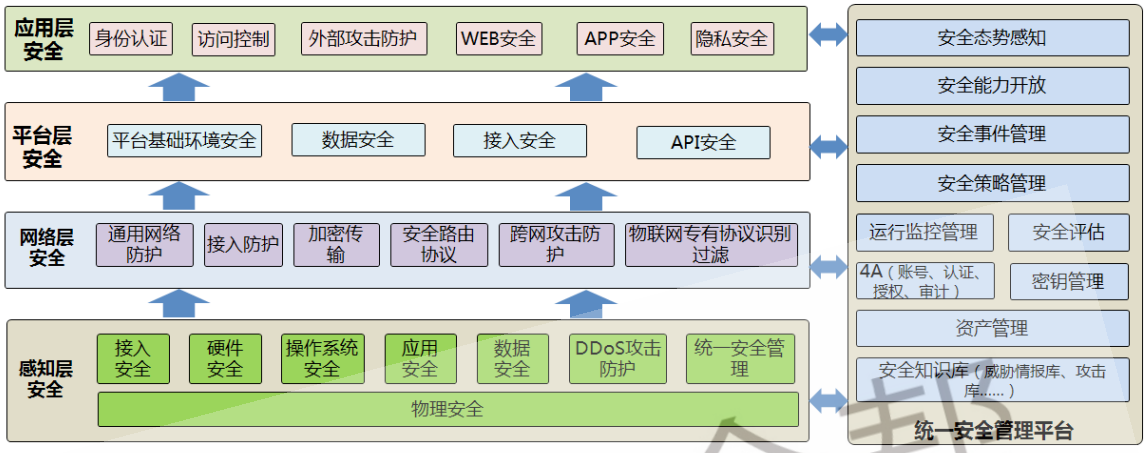


图 6-1 物联网的安全架构

下面将对物联网安全体系结构中的感知层安全、网络层安全、平台层安全、应用层安全和统一安全管理平台进行详细的阐述。

6.2 感知层安全

感知层安全的设计中需要考虑物联网设备的计算能力、通信能力、存储能力等受限，不能直接在物理设备上应用复杂的安全技术。可采取的防护技术和措施如下。

物理安全：采取防水、防尘、防震、防电磁干扰、防盗窃、防破坏的措施。

接入安全：通过轻量级易集成的安全应用插件进行终端异常分析和加密通信等，实现终端入侵防护，从而防止终端成为跳板，攻击关键网络节点。同时需要轻量化的强制认证机制。

硬件安全：确保芯片内系统程序、终端参数、安全数据和用户数据不被篡改或非法获取。在硬件安全方面将主要解决物联网终端芯片的安全访问、可信赖的计算环境、加入安全模块的安全芯片以及加密单元的安全等。将身份识别、认证过程“固化”到硬件中，以硬件来生成、存储和管理密钥，并把加密算法、密钥及其他敏感数据，存放于安全存储器中可增强物联网终端的硬件安全防护。

操作系统安全：使用轻量级安全操作系统，实现操作系统对系统资源调用的监控、保护、提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情情况下执行某种行为，或者用户执行不可控的行为。另外，操作系统还要保证自身的升级是受控的。在操作系统安全方面，主要通过安全调用控制和操作系统的更新来确保操作系统的能力，通过对

系统资源调用的监控、保护、提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情情况下执行某种行为，或者用户执行不可控行为。

应用安全：保证终端对要安装在其上的应用软件进行来源识别，对已经安装在其上的应用软件进行敏感行为的控制，还要确保预置在终端中的应用软件无恶意吸费行为，无未经授权的修改、删除、窃取用户数据的行为。在应用软件安全方面，主要关注应用软件认证签名机制和敏感 API 管控技术。

DDoS 攻击防护：主要分为两种，一种是对设备进行攻击，如频繁向电子标签发送恶意请求信息，使标签无法响应合法请求；另一种是控制很多物联网设备对其他系统进行攻击。针对第一种攻击，物联网远端设备需要嵌入式系统抵抗拒绝服务攻击。针对第二种攻击，一方面加强对节点的保护，防止节点被劫持；另一方面也需要提供有效地识别被劫持节点的方法。

数据安全：主要提供包括移动智能终端的密码保护、文件类用户数据的授权访问、用户数据的加密存储、用户数据的彻底删除、用户数据的远程保护。

统一安全管理：可信的身份认证、安全的固件更新、Internet 服务访问权限管控和加解密及密钥管理等功能。

综上，物联网终端的安全需要从硬件到软件综合考虑，包括硬件芯片级的安全、操作系统的安全和操作系统层以上的终端安全加固。在具体防护时，要依据数据的敏感程度、终端的智能程度和不同的网络架构特点，平衡引入安全机制所带来的资源消耗和成本，甄选各种终端安全技术来适配复杂的海量物联网终端。

终端安全在物联网安全防护中，是重中之重，除了做好上述的安全措施外，还应加强终端的全生命周期管控，在上线前，做好终端设备的严格入网，保障终端具备防护能力要求。上线后，做好终端设备激活、身份认证、安全存储、软件升级，同时对终端设备的进行安全监控，及时发现安全威胁，做好应急响应。退网后，做好终端数据的安全擦除，做好生命周期全程防护。

6.3　网络层安全

物联网的网络层安全，传统网络层安全机制大部分依然适用于物联网，此外还要基于物联网网络层特征，采取特殊防护机制。主要防护技术和措施如下。

通用网络防护：包括网络结构安全，合理划分网络安全域，加强安全边界隔离，避免安全问题的扩散。访问控制，网络边界部署防火墙，制定访问规则，访问控制策略，实现系统内外网边界的访问控制。

网络入侵防护：部署入侵监测设备，对网络攻击进行监控和报警，具备端口扫描、暴力破解、缓冲区溢出攻击、IP 碎片攻击、网络蠕虫、病毒、木马、IP 重用防护、DDoS 等攻击

的监控检测能力。

网络安全审计：通过统一日志管理系统或安全管理平台，对网络设备运行状况、网络流量、用户行为等进行日志审计。

接入防护：防火墙 / 网关要求能处理百万并发连接，支持海量接入的加密能力；实现白名单过滤技术，包括自定义协议能力；需要对终端资源消耗攻击和基于多行业应用流量攻击特征的自动防护；网络安全产品还需要提供基于物联网特征的病毒和高级威胁的防护功能。

加密传输：固网和无线网络加密传输。物联网需要充分利用无线移动通信的物理层传输特性，通过认证、加密和安全传输等技术的应用，在保证用户通信传输质量的同时，防止未知位置的窃听和增加中间人攻击的难度。空口层面，终端和网络基于无线标准进行双向认证，确保经过验证的合法的终端接入合法的网络。同时终端和网络之间建立安全通道，对终端数据提供加密和完整性保护，防止信息泄露、通信内容被篡改和窃听。

安全路由协议：物联网的路由要跨越多类网络，有基于 IP 地址的互联网路由协议，有基于标识的移动通信网和传感网的路由算法，因此我们要至少解决两个问题，一是多网融合的路由问题，二是传感网的路由问题。前者可以考虑将身份标识映射成类似的 IP 地址，实现基于地址的统一路由体系；后者是由于传感网的计算资源的局限性和易受到攻击的特点，要设计抗攻击的安全路由算法。

跨网攻击：由于物联网在感知层所采集的数据格式多样，来自各种各样感知节点的数据是海量的、并且是多源异构数据，带来的网络安全问题将更加复杂。在物联网网络层，重要的关注点之一是建立完善异构网络统一、兼容、一致的跨网认证机制，完善网络安全协议，加强密钥管理，完善机密性算法，加强数据传输过程的机密性、完整性、可用性的保护。

识别并过滤物联网专有协议和应用：物联网终端采用了大量的专有接口，如 KNX、ModBus、CANBus 等，被接入到工控网络中，这些终端和网络大多都是设计在孤立环境中运行的，安全机制相对薄弱。随着物联网的逐步发展，这些终端和网络将被逐步接入到互联网中，这会引入新的安全问题。为解决这些问题，需要物联网防火墙或安全网关等设备支持对工业协议和各行业应用的深度识别和自动过滤；处理百万并发连接，支持海量接入的加密能力；实现白名单过滤技术，包括自定义协议能力；需要对终端资源消耗攻击和基于多行业应用流量攻击特征的自动防护；网络安全产品还需要提供基于物联网特征的病毒和高级威胁的防护功能。

6.4 平台层安全

平台层安全主要保障信息和数据在计算和存储的安全，云平台必须采取适当的安全策略来保证物联网中数据的完整性、保密性和不可抵赖性，此外还要保障接入安全及 API 安全。

（1）平台基础环境安全

主要是保证平台数据计算与运行环境的安全，特别是基于虚拟化技术的云计算安全，重点应考虑虚拟化管理程序安全和虚拟服务器安全，

虚拟机管理程序（VMM）安全：VMM 安全是保证客户虚拟机在多租户环境下相互隔离的重要层次，必须严格限制任何未经授权的用户访问虚拟化软件层，限制对于 Hypervisor 和其他形式的虚拟化层次的物理和逻辑访问控制。对于 VMM 的安全防护手段主要是 VMM 的安全部署和安全配置，在 VMM 部署时采用强口令字进行鉴权，做好物理访问控制和网络访问控制，防止非授权人员访问 VMM，启用 VMM 中的安全选项等。目前针对 VMM 的安全漏洞发掘是安全研究的热点方向之一，主流的虚拟化平台都出现过虚拟机逃逸的案例，但目前针对 VMM 的安全漏洞扫描工具还很少，对于安全漏洞的发现和修补目前主要通过官方公布的安全补丁通告和升级版本的方式。

虚拟服务器安全：虚拟服务器位于虚拟化软件之上，对于物理服务器的安全原理与实践也可以被运用到虚拟服务器上，同时需要兼顾虚拟服务器的特点，包括选择具有 TPM 安全模块的物理服务器、使用支持虚拟技术的 CPU、安装虚拟服务器时分配独立的硬盘分区、使用 VLAN 和不同的 IP 网段、在防火墙中为虚拟服务器做相应的安全设置等，以对它们进行保护和隔离，并与其他安全防范措施一起构成多层次防范体系。

（2）数据安全

数据安全隔离可以根据应用的需求，采用物理隔离、虚拟化等方案实现不同租户之间数据和配置信息的安全隔离，以保护每个租户数据的安全与隐私。

数据访问控制可以采用基于身份认证的权限控制方式，进行实时的身份监控、权限认证，防止用户间的非法越权访问。在虚拟应用环境下，可设置虚拟环境下的逻辑边界安全访问控制策略，如通过加载虚拟防火墙等方式实现虚拟机间、虚拟机组内部精细化的数据访问控制策略。

数据处理安全，确保数据在汇聚与存储、融合与处理、挖掘与分析过程的安全性，常采用的安全机制包括数据隔离与交换、数据库安全防护、数据备份、数据检错纠错、文件系统安全性、访问控制和身份鉴别、统一安全管理等。云计算与存储安全通过数据隔离与交换、冗余备份数据，将数据存放在不同的数据中心中，以保证个别存储设备的故障不影响整个存储系统的可用性；通过数据库防护技术满足数据库的数据独立性、数据安全性、数据完整性、并发控制、故障恢复的要求；通过采用检错和纠错技术使系统迅速发现错误并找寻备份数据来完成数据存取访问，保证数据的正确读写；通过文件系统加密实现存储系统安全。

（3）接入安全

对所有接入设备提供设备与平台采用双向验证，进行证书授权认证及权限管理，确保接入的终端设备与传输的信息安全可靠。消息传输使用加密传输，确保链路上传输消息的安全可靠性和数据完整性，保障用户信息安全。接入设备使用了 MQTT 或 CoAP 等不安全协议

的情况下，支持连接保护的能力，如使用 TLS 或 DTLS；接入设备使用 Wi-Fi 连接的情况下，采用安全协议，如 WAP2；接入设备使用 Wi-Fi 连接的情况下，禁用不安全协议，如 WPA 和 TKIP。

（4）API 安全

加强 API 调用的访问控制，防止未授权访问，调用前进行用户鉴别和鉴权，验证用户凭据，对请求做身份认证，并且防止篡改，重放攻击，对敏感的数据做加密，防范数据被篡改。做好 API 过载保护，实现不同服务等级用户间业务的公平性和系统整体处理能力的最大化；并对 API 的调用进行日志记录。

6.5 应用层安全

应用层安全主要是保障各类应用在用户使用过程安全，包括对用户的身份鉴别、访问控制、应用漏洞管理、外部攻击防护、APP 安全、隐私保护等。

（1）身份和访问控制

应用访问时进行强制认证和业务权限控制，应尽可能采用双因素身份验证机制，加强权限管理，端口控制，敏感信息访问等。

（2）应用安全漏洞管理

防范应用本身漏洞而导致的数据被窃取或系统攻击，如 SQL 注入、跨站脚本编制、上传漏洞、命令注入、应用中间件漏洞、业务逻辑漏洞等，应用层安全漏洞检测主要通过应用漏洞扫描系统来实现；另外还包括渗透测试、代码审计等技术手段。应用层的安全漏洞修补主要通过应用中间件安全配置和应用程序安全代码整改实现。

为了极大减少 Web 应用程序的漏洞，应当加强应用系统全生命周期管理，在设计阶段，将安全防护设计与系统设计相融合；在系统开发阶段，进行代码安全评估，测试阶段同期进行安全测试；在建设阶段进行安全管理；在验收阶段同时进行风险评估和测评，在运营和维护阶段，定期对应用系统进行安全评估和加固，及时更新 Web 应用系统的安全补丁，定期对应用系统进行安全评估和加固。在系统废弃阶段做好残余信息的消除等，保障系统保障全生命周期的系统安全。

（3）外部攻击防护

通过部署 Web 防火墙、IPS 等设备，监控并过滤恶意的外部访问，能够对 SQL 注入、XSS 等已知应用漏洞攻击以及应用层 DoS 攻击起到防护作用；并对恶意访问进行统计记录，作为安全工作决策及处置的依据。

（4）APP 安全

APP 代码按照安全要求严格开发，做好代码加密、加壳防止反编译，APP 与应用平台间数据要求加密传输，要在上线前做好评估，上线后定期评测、加固漏洞。

（5）隐私保护

应用层在各行业或应用中必然会收集用户大量隐私数据，例如其健康状况、通信簿、出行线路、消费习惯等，因此必须针对各行业或各应用考虑其特定或通用隐私保护问题，主要是面向用户提供一些安全手段来保证用户数据在传输、交换和使用过程中的安全性，防止用户数据被非法访问和泄露，常采用的安全机制包括存储加密、交换加密、身份认证与访问控制、接口安全、自我销毁技术等技术措施。这其中最关键的安全因素是个人数据保护，大量的个人数据可会从分散的端侧传输到某个物联网应用平台，个人数据需要得到充分的保护，符合相关国家和地区的隐私保护法律的要求。

6.6　统一安全管理平台

除了各层安全防护外，还需要建立一个全面、统一、高效的安全管理平台。

基于资产与身份标识体系将 4 层设备纳入统一管理体系中，实现对不同层次不同种类的全面安全管理，为各种物联网业务应用提供一种公共、开放、普适的信息安全支撑，促进信息孤岛的相互融合，主要包括以下安全功能 ,。

资产管理：实现对物联网设备的统一管理，建立物联网统一资产库。按照资产信息、漏洞、补丁与备件分类导入或登记入库，并为其他安全运行管理模块提供信息接口。

密钥证书：为物联网业务、应用提供统一的密钥与证书的生成、发放和管理。

安全策略配置管理：为全网安全运行提供统一的安全策略，及策略的统一下发、补丁统一更新。

运行状态监控：监控终端、主机、网络设备、安全设备、应用系统的运行状态，流量监控和资源使用情况，为网络安全管理人员提供统一的运行状态信息，并可根据自定义的阈值报警，结合设备的拓扑显示，能够准确定位设备运行状态事件，保证网络和业务系统的稳定、可靠运行。

风险评估：对物联网的终端、主机、网络设备、安全设备、应用系统安全事件的收集和管理，资产的脆弱状态信息收集和管理，结合事件、脆弱状态信息进行综合关联分析和风险管理。

安全事件管理：通过安全代理（Agent）和引擎（Engine）的部署，在物联网各层上的不同安全信息采集点，通过安全通信方式，集中收集安全事件到安全管理服务器进行处理，从而实现了针对全网的安全事件的集中收集和分析处理。

能力开放：部分信息安全能力进行封装形成 API，为物联网业务应用开放，以降低其信息安全的实现成本。

安全态势感知：万物互联时代带来了海量的联接，物联网复杂度日趋提升，终端多、网络多、应用多，针对物联网的未知攻击、APT 也急剧上升，安全威胁也日益严峻。安全威胁无处不在，不但需要每个层面的多重安全防护，还需要有端云协同的智能大数据安全分析能

力，实现整网的智能安全态势感知、可视化和安全防护，防御被动转主动、静态变动态、知彼知己、防患未然，物联网安全态势感知平台必将是物联网安全的发展方向。物联网态势感知系统主要功能包括以下几类。

- 数据采集

通过采集业务日志、设备日志以及网络流量，用分布式任务调度引擎，自动采集相关安全数据，通过基于缓存的分布式消息队列进行实时处理，根据规则引擎以及决策引擎，针对安全数据进行识别、转换、处理和传输。

- 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，既能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。

- 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。

- 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。

- 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。

物联网态势感知系统通过对各类物联网数据进行采集和主动探测，利用安全大数据分析和建模技术，从多个维度进行安全分析，全面感知物联网各类安全风险，事前准确预警、事中快速处置、事后全面溯源，形成智能化主动防御体系，匹配物联网云管端协同，保障物联网业务可持续健康发展。

第四部分
物联网安全发展展望

第七章

物联网安全产业发展趋势

万物互联的物联网时代正在“扑面而来”，全球最具权威的 IT 研究与顾问咨询公司 Gartner 称，2017 年全球物联网设备数量将达到 84 亿——比 2016 年的 64 亿增长 31%，首次超过全球人口数量（75 亿）。预测到 2020 年，全球物联网设备将达到 204 亿。IHS 预测全球物联网设备的安装基数在 2025 年，这一数字更将达到 754 亿，如图 7-1 所示。

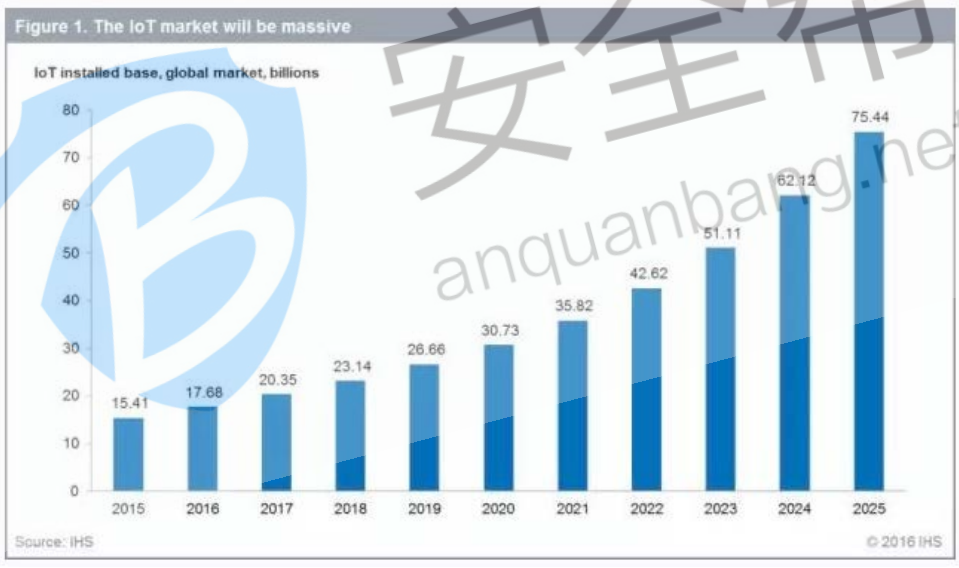


图 7-1　物联网设备安全基数发展分布图（数据来源：IHS）

福布斯（Forrester）预测，交通运输、政府部门的安保与监控零售和库存管理以及初级制造业的工业资产管理将是未来物联网增长的热门领域。相比小公司，大企业更有可能使用物联网。调查中 23% 的大型受访企业在使用物联网，中小企业中，这个比例只有 14%。麦肯锡估计，物联网市场总规模在 2020 年将达 37 亿美元，达到 32.6% 的年复合增长率。2025 年之前，物联网的潜在经济影响力为 2.7 万亿～ 6.2 万亿美元。据贝恩咨询公司预测，到 2020 年，出售硬件、软件和综合解决方案的物联网服务供应商年收入可达 4700 亿美元，可用利润达 600 亿美元。同时贝恩预测云服务提供商、分析和基础设施软件供应商将对物联网交易产生重要影响。

IDC 预测全球物联网收入将从 2015 年的 27.12 亿美元增加到 2020 年的 70.65 亿美元，

复合年增长率（CAGR）达到 21.11%。同时，IDC 还预测物联网设备的安装基数将以 17.5% 年复合增长率在 2020 年增加到 281 亿，如图 7-2 所示。

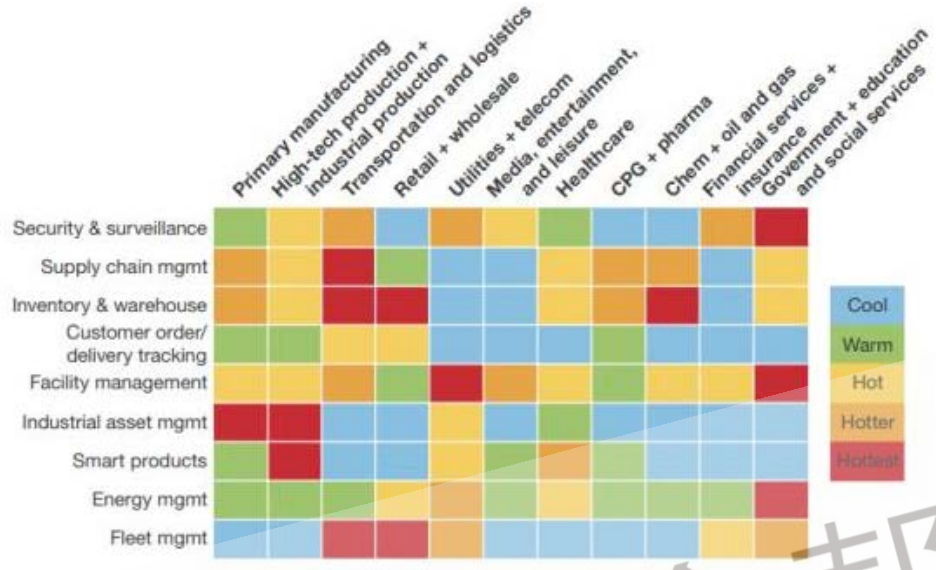


图 7-2　工业应用物联网发展分布图（数据来源：Forrester）

物联网设备从 2015 年到 2021 年以 23% 的复合年增长率（CAGR）增长，到 2018 年将超过手机成为最大的互联设备类别。Ericcson 预计，到 2021 年，全球联网设备将达 280 亿，其中 160 亿与物联网相关。IndustryARC 预测工业物联网到 2021 年，市场将达 1238.9 亿美元。通用电气预测在未来 15 年中，工业物联网（IIoT）领域的投资最高可达 60 万亿美元。埃森哲预计工业互联网到 2030 年能够为全球经济带来 14.2 万亿美元的经济增长。

在物联网迅猛发展的同时，物联网安全成了产业痛点。Gartner 就此预测：到 2020 年，针对企业经确认的安全性攻击中，有 25% 以上将涉及物联网。物联网安全事件频发，既是挑战也同时蕴藏着巨大的商业机会。调查研究公司 MarketsandMarkets 预计，2020 年全球物联网的安全市场将从 2015 年的 68.9 亿美元增长至 289 亿美元，即 2015 年至 2020 年的复合年增长率（CAGR）为 33.2%。

物联网安全将成为万亿规模市场下的蓝海“潜力股”。面对如此规模的“市场蛋糕”，吸引了产业链上下游大批市场玩家的“驻足”。既有传统的 IT 基础设施厂商（防火墙、VPN 等供应商）、互联网安全公司（更多从软件上提供安全防护、病毒查杀等），也有专门瞄准物联网安全的新兴的创业公司。另外还有一类是产业链上下游厂商在基于原有产品服务基础上，提供安全保护增值服务，如在芯片上增加高级安全设计。

但是，物联网安全是一个贯穿全产业链环节的系统工程，仅从硬件或者软件又或者网络传输单一层面进行检测、管理与安全防护，都很难从根本上杜绝安全隐患，尤其是涉及到国计民生等重大物联网项目，闭环安全生态的需求变得更为迫切，执行从底层芯片、软件系统、数据采集、数据存储、数据分析、网络传输到上层应用的全生态链安全变得非常关键。

第八章

物联网安全新技术的探索

在物联网安全产业繁荣发展的同时，加快新技术新应用的研发，以满足不断发展的安全需求，可行的研究方向主要包括去中心化认证、边缘计算、终端安全轻量化防护技术和软件定义边界。

8.1　去中心化认证

区块链（Block Chain，BC）是指通过去中心化和去信任的方式集体维护一个可靠数据库的技术方案。该技术方案主要让参与系统中的任意多个节点，通过一串使用密码学方法相关联产生的数据块（Block），每个数据块中包含了一定时间内的系统全部信息交流数据，并且生成数据指纹用于验证其信息的有效性和链接下一个数据库块。区块链解决的核心问题是在信息不对称、不确定的环境下，如何建立满足经济活动赖以发生、发展的“信任”生态体系。这在物联网上是一个道理，所有日常家居物件都能自发、自动地与其他物件或外界世界进行互动，但是必须解决物联网设备之间的信任问题。如果把区块链的特性优势与物联网相结合，就可以保证设备网络的真实性，提高系统速度，节省一些繁杂的环节。

未来物联网设备的运行环境应该是去中心化的，它们彼此相连，形成分布式云网络。而要打造这样一种分布式云网络，就要解决节点信任问题。在传统的中心化系统中，信任机制比较容易建立，存在一个可信的第三方来管理所有的设备的身份信息。但是物联网环境中设备众多，可能会达到百亿级别，这会对可信第三方造成很大的压力。区块链分布式的网络结构可以提供一种机制，使得设备之间保持共识，无需与中心进行验证，这样即使一个或多个节点被攻破，整体网络体系的数据依然可以运行，是可靠安全的。未来的物联网的降借助区块链技术实现应用多元，各种有助落实相关应用的技术将陆续被提出，为整个物联网行业提供了一个具可行性发展的方向。

8.2　边缘计算

边缘计算是在靠近物或数据源头的网络边缘侧，融合网络、计算、存储、应用核心能力

的开放平台。边缘计算与云计算互相协同，共同助力各行各业的数字化转型。它就近提供智能互联服务，满足行业在数字化变革过程中对业务实时、业务智能、数据聚合与互操作、安全与隐私保护等方面的关键需求。

IDC 预测，到 2018 年，50% 的物联网网络将面临网络带宽的限制，40% 的数据需要在网络边缘侧分析、处理与储存，到 2025 年，这一数字将超过 50%。物联网领域拥有海量的终端设备，如果这些设备产生的数据聚在一起，会是个天文数字。海量数据的分析与储存对网络带宽提出了巨大的挑战，而边缘计算的诞生，就是为了解决这一问题。

（1）分布式和低延迟计算

云计算往往并不是最佳策略，计算需要在更加靠近数据源的地方执行。许多数据流由边缘设备生成，但是通过“远处”的云计算处理和分析，不可能做出实时决策。例如使用可穿戴式摄像头的视觉服务，响应时间需要在 25~50ms，使用云计算会造成严重的延迟；再比如工业系统检测、控制、执行的实时性高，部分场景实时性要求在 10ms 以内，如果数据分析和控制逻辑全部在云端实现，则难以满足业务要求；还有那些会生成庞大数据流的多媒体应用，如视频或是基于云平台的如视频或是基于云平台的网络游戏，依赖云计算也会为玩家造成类似于等待时间过长的问题，无法满足用户的需求。作为云计算的有益补充，可以利用边缘节点（例如，路由器或离边缘设备最近的基站），用以减少网络等待时间。

（2）超越终端设备的资源限制

与数据中心的服务器相比，用户终端（例如智能手机）的硬件条件相对受限。这些终端设备以文本、音频、视频、手势或运动的形式获得数据输入，但由于中间件和硬件的限制，终端设备无法执行复杂的分析，而且执行过程也极为耗电。因此，通常需要将数据发送到云端，进行处理和运算，然后再把有意义的信息通过中继返回终端。

然而，并非来自终端设备的所有数据都需要由云计算执行，数据可以利用适合数据管理任务的空闲计算资源，在边缘节点处过滤或者分析。

（3）可持续的能源消耗

大量研究显示，云计算会消耗庞大的能源，未来 10 年数据中心所消耗的能源量可能是如今消耗量的 3 倍。随着越来越多的应用转移到云，能量需求会日益增长，甚至无法满足。因此，采用能量效率最大化的计算策略显得尤为迫切。

一些嵌入式小型设备的基础信息采集处理完全可以在端完成，即手机传感器把数据传送到网关后，就通过边缘计算进行数据过滤和处理，没必要每条原始数据都传送到云，这省去了大量的能源成本。

（4）应对数据爆炸和网络流量压力

通过在边缘设备上执行数据分析，可有效应对数据爆炸，减轻网络的流量压力。边缘计算能够缩短设备的响应时间，减少从设备到云数据中心的数据流量，以便在网络中更有效的分配资源。

（5）智能计算

不仅是消费级的物联网终端，边缘计算还将在工业应用中发挥重要作用。计算可以分层执行，利用网络远端的资源完成。例如，典型的生产流水线可以过滤设备上生成的数据，在传输数据的边缘节点上执行部分分析工作，之后再通过云端执行更加复杂的计算任务。边缘节点可以通过分担云计算的部分任务，增强数据中心的计算能力。

边缘计算仍处于起步阶段，当前的云计算服务可以支持数据密集型的应用程序，但在网络边缘进行实时的数据处理仍是一个有待开拓的领域。

8.3　轻量化防护技术

未来将有海量的终端接入物联网，这些终端呈现多源异构性，通常情况下功能简单、携带能量少，使得它们无法拥有复杂的安全保护能力，不安全的终端很容易被非法利用，成为攻击的发起点和跳板，造成对物联网核心平台的威胁。终端安全是未来物联网安全中非常重要的一环，所以如何提升计算能力、通信能力、存储能力等受限的海量物联网终端的防护能力，是未来的研究重点。

（1）轻量级加密认证技术

物联网安全技术的挑战重点在于对感知层资源受限设备的轻量级安全保护，包括轻量级安全算法和轻量级安全协议。轻量级安全算法具有通用性，而轻量级安全协议只能做到在小范围内具有一定的通用性。

随着便携式电子设备的普及和 RFID、无线传感器网络等技术的发展，越来越多的应用需要解决相应的安全问题。然而，相比于传统的台式机和高性能计算机，这些设备的资源环境通常有限，比如，计算能力较弱、计算可使用的存储较少、能耗有限等，导致传统密码算法无法很好地适用于这种环境，这就使得受限环境中密码算法的研究成为一个迫切需要解决的热点问题，适宜资源受限环境使用的密码算法被称为轻量级密码算法。

轻量级密码算法与经典密码算法相互影响，互相促进。经典密码算法为轻量级密码算法的设计与安全性分析提供理论支撑和技术指导；另一方面，轻量级密码之“轻量级”的特点将使得一些安全性分析能够更加深入、全面地展开，在这个过程中，可能会衍生出新的问题，从而进一步带动和促进密码算法安全性分析的进展。

除了密码算法需要轻量化外，身份认证技术更需要轻量化，因为后者关系到通信过程，其消耗的资源（主要是功耗）远超过计算过程所消耗的资源。在 RFID、无线传感器网络等应用环境中，节点资源（包括存储容量、计算能力、通信带宽和传输距离等）受到比传统网络更加严格的限制，资源的严重受限使得传统的计算、存储和通信开销较大的身份认证技术无法应用，因此轻量级身份认证技术成为该领域研究的热点。除此之外，轻量级密钥管理方案也是保证物联网系统安全不可或缺的关键技术。应该说，轻量级安全保护体系才是解决物

联网感知层安全问题的整体方案。

（2）芯片

为保证设备的安全，安全芯片作为最基础的设备组成单元，具备安全的智能加密是物联网设备抵御攻击的关键。也是抵御黑客攻击旨在窃取关键数据的唯一靠谱的方法，是各类高安全物联网设备的首选。未来物联网需要低成本、低能耗且标准统一的芯片级安全技术，实现硬件级的高强度加密和隔离，提供可信环境和安全存储，将重要密钥在可信芯片中存储，防止数据泄密；同时支持设备安全启动，对软件和固件的启动、升级进行签名，保护数据完整性。

（3）操作系统

作为完整解决方案，低成本、低能耗、高可靠性操作系统也是未来的研究重点。由于现有操作系统很难完全匹配物联网应用需求，目前物联网操作系统领域涌现出 3 条技术路径。一条是基于 Android、iOS 等操作系统进行裁剪和定制，来适应物联网接入设备的需求；另一条技术路线是以传统嵌入式操作系统和实时操作系统为基础，通过增加设备联网等功能，满足物联网接入设备互联需求，形成新的嵌入式操作系统；第三条技术路线是面向物联网产生的新型操作系统。

面向物联网新型终端大量组网的需求，操作系统需进行新一轮发展创新。架构上，为实现通用化，架构逐渐趋于一致，并具备物联网独有特点；技术上，面向新型终端安全性、低功耗、互联性的需求，一是面向不同厂商的设备，为实现互联互通和互操作，操作系统必须实现互通性要求；二是物联网设备资源受限，低功耗成为物联网操作系统的必备特性；三是联网设备不断增加，网络安全性亟待提升，从操作系统层面保障软硬件安全成为必须；四是物联网设备形态功能各异，需增加软硬件的支撑能力；五是针对大量异构终端，物联网操作系统需实现模块化要求，实现可裁剪和迅速定制。针对新的需求，操作系统需要不断创新提升自身性能以适应未来物联网发展的安全需求。

8.4 软件定义边界

软件定义边界可能成为下一代物联网的访问控制技术。Gartner 预测，到 2017 年年底，至少 10% 的企业组织（目前低于 1%）将利用软件定义边界 SDP 技术隔离敏感的环境，这项技术在安全保障用户访问的同时，也可以改善便利性，而使用一个固定的边界来保护企业内部网站正在逐渐过时。

传统企业网络架构通过建立一个固定的边界使内部网络与外部世界分离，这个边界包含一系列的防火墙策略阻止外部用户的进入，但是允许内部用户对外访问。由于封锁了外部对于内部应用和设施的可见性和可访问性，传统的固定边界确保了内部服务对于外部威胁的安全。但是现在，BYOD 和钓鱼攻击提供了对于内部网络的不可信访问，以及 SaaS 和 IaaS 正

在改变边界的位置，企业网络架构中的固定的边界模型正在变得过时。因此，需要一个新的安全模型，这个模型可以理解上下文信息，如用户位置，用户使用什么设备来建立连接，何时建立连接以及用户的角色。这些信息可以集成到特定上下文的访问规则中，基于上下文参数的认证检查和对于资源的访问，能够提供对于边界内部和外部威胁的更好防护。

软件定义边界（Software Defined Perimeter，SDP）由云安全联盟（CSA）于 2013 年提出，用应用所有者可控的逻辑组件取代了物理设备，只有在设备证实和身份认证之后，SDP 才提供对于应用基础设施的访问。SDP 使得应用所有者部署的边界可以保持传统模型中对于外部用户的不可见性和不可访问性，该边界可以部署在任意的位置，如网络上、云中、托管中心中、私有企业网络上，或者同时部署在这些位置中。

SDP 包含两部分：SDP 主机和 SDP 控制器。SDP 主机可以创建连接或者接受连接。SDP 控制器主要进行主机认证和策略下发，SDP 主机和 SDP 控制器之间通过一个安全的控制信道进行交互。

SDP 改变了传统的网站连接方式。首先，客户端进行多因素认证，认证设备的可靠性等，这一步对用户而言是透明的。认证通过之后，才进入用户登录阶段。这两步均是客户端与 Controller 进行交互，不涉及对于具体服务的访问。当认证通过后，客户端才能够与可访问的服务建立连接。因此，SDP 通过三种方式对抗基于网络的攻击：透明多因素认证可以抵抗用户凭据丢失、服务器隔离可以抵抗服务器利用、TLS 双向认证可以抵抗连接劫持。

SDP 可以提供对于网络系统、服务和应用的以人为中心、可管理的、普遍存在的、安全的和敏捷的访问，它解决了 TCP/IP 中的一个设计漏洞（在认证之前即对报文进行处理）。由于 SDP 的部署代价更低，因此，SDP 可能颠覆网络防火墙和 VPN 技术。SDP 同样有可能颠覆传统的网络安全技术部署，如 NAC、Switch-to-Switch 加密、内部的 VPN 能力，这是因为 SDP 的软件 Agent 技术可以部署在任何其支持的操作系统上，从而创建一个及时的和动态的网络边界。

第九章

物联网安全建设发展建议

（1）加强政府对物联网的合规性要求

物联网正在驱动着一轮新的行业变革。但是在很多行业中，安全需求不同，各行业安全方案既不全面也不成熟，在安全监管及应对方面并没有明确的思路。单靠某个或某些行业的力量来保障物联网安全是不够的，需要有更高层级的协调方使各个相关行业能够协同作战。因此物联网安全相关的政策、法规需要政府作为国家战略之一是重视和加大投入。政府的合规性要求，是自上而下的强制立法，是物联网安全健康发展的首要条件。

有了政府的合规性要求，市场的基本面才能形成，设备厂商、服务提供商与安全企业才会有动力去推进。对于这种缺失，主要有两点原因：一方面，我国的物联网应用落地较晚，目前还处于起步和发展阶段，且尚未出现过大规模的被攻击事件，社会和国家对物联网安全的重视程度还不够；另一方面，我国的物联网产业监管部门较多，有业务交叉，众口难调，很难在短时间内形成一个统一的合规性要求。

合规性管理，可以参考美国的相关做法。2016 年美国东海岸断网事件之后，美国国土安全部便于次月发布了《保护物联网策略准则（1.0 版）》，呼吁物联网生态体系在设计、生产及使用物联网设备与系统时，皆应负起保障物联网安全的责任。2017 年 5 月，美国总统特朗普签署 13800 号总统行政令——《加强联邦网络和关键基础设施的网络安全》，其中内容之一就是要增强美国应对僵尸网络及其他自动化和分布式威胁的能力。6 月 13 日，美国商务部下属的国家电信和信息管理局发布征求评议文件《促进利益相关者对僵尸网络和其他自动威胁的行动》，要求各私营企业、研究机构、社会团体围绕减少僵尸网络威胁和维护物联网终端设备安全问题，提出法律、政策、标准、技术等方面的建议。8 月 1 日，美国 4 名国会议员联名提交了一项关于物联网安全的法案《2017 物联网网络安全改进法》，希望通过设定联邦政府采购物联网设备安全标准，改善美政府所面临的物联网安全问题。

从以上分析看，加强政府的监管和立法，不仅有助于提高社会和国家对物联网安全的重视程度，而且也能进一步推进物联网产业向着健康、安全的方向良性发展。

（2）加强物联网安全标准建设

在技术的发展和演进过程中，标准起到了至关重要的作用，产品和解决方案均须依赖或

遵从其适用的标准。在物联网中，标准扮演着越发重要的作用，因为物联网是多类技术的结合，覆盖从底层接入技术到上层跨垂直行业应用。相应地，物联网安全正在逐渐成为各大标准组织的关注热点。目前很多标准和联盟组织都在针对物联网安全的各种挑战，积极建议和设计安全技术标准，以满足更智能、全联接的生态系统需求。从当前标准和联盟组织的进展来看，物联网安全尚处于起步阶段，以指南和框架为主，能够用于指导产业落地的具体技术标准非常缺乏。急需标准和联盟组织加大相关安全标准的投入，以加快安全标准的输出，促使物联网产业的快速发展。

（3）做好物联网建设的全生命周期安全防护

将安全嵌入物联网建设的整个生命周期。在系统规划、分析、设计、开发、建设、验收、运营和维护、废弃的每一个阶段进行信息安全管理，在设计和分析阶段就进行安全目标、安全体系、防护蓝图等顶层设计，并将安全防护设计与设计相融合；在开发阶段，进行安全评估，测试阶段同期进行安全测试；在建设阶段进行安全管理；在验收阶段同时进行风险评估和测评，保障安全防护的有效性和合规性，在运营和维护阶段同时进行安全运营，并周期进行风险评估，跟踪威胁情报，持续改进安全管理和安全防范措施，在系统废弃阶段做好残余信息的消除等，保障系统保障全生命周期的系统安全。

（4）普及物联网安全防护观念

长期来看，安全问题的根源之一是未“防患于未然”的观念问题。因此，物联网时代必需将万物互联、安全先行的理念根植于产业链各游，使得从产品本身就具备高度安全性，

在物联网实践中，网络传输、云服务与应用产业链各层也从一开始就运行在一个高度安全防护的生态环境中。由于物联网已经渗透到人类生活的方方面面，除了在物联网产业链普及安全观念外，还应该对广大的用户进行广泛普及，引导用户增强对隐私的保护意识，增加安全诉求，抬高安全门槛。只有用户的需求提高了，形成规模了，安全需求才能真正涌现出来，倒逼设备制造商和服务提供商提高物联网设备、网络、平台、应用的安全性，形成全员参与的良好的闭环，有效降低安全事件的发生。

（5）加强物联网安全生态建设

物联网产业快速发展、高度融合、需求多样、威胁激增，物联网安全问题更是从底层传感器、芯片、模组、硬件到通信技术、网络连接再到渗透到各行业的应用层，企业单凭一己之力很难满足物联网的要求，构建开放、合作、共赢的安全生态圈是产业发展的必然。需要

元器件供应商、设备制造商、网络服务运营商、软件服务提供商、系统集成商、渠道伙伴在安全领域开放、合作、共赢，构建良好的物联网安全生态体系，通过与合作伙伴的紧密合作，以更接地气的方式贴近市场实际需求、及时获取行业动向，快速集成技术成果，推进物联网安全生态的良性发展，为物联网产业的繁荣提供可靠的安全保障。

附录 A
发布单位介绍

A.1 中国电信股份有限公司北京研究院

中国电信股份有限公司北京研究院（原中国电信集团北京研究院）是中国电信集团公司为适应集团公司发展和电信市场竞争需要，于 2001 年 4 月 18 日挂牌成立的科研机构，旨在成为集团公司以及各省级公司的企业决策智库、技术创新引擎和产品创新孵化器。

其主要研发领域包括通信信息技术发展趋势与战略研究；通信信息技术发展政策研究；企业决策科学研究；企业战略发展研究；通信网络、技术与业务发展规划研究；通信技术体制和标准研究；通信信息新技术、新设备和新产品的入网测试评估；网络管理和业务管理等支撑系统的开发；应用软件研究与系统集成；通信信息新产品和增值业务的开发和推广；信息情报研究等。

北京研究院现拥有员工 400 多人，硕士研究生及以上学历人员占比达到了 78%，其中博士研究生 52 人，累计获得国家科技进步二等奖 3 项、省部级科技进步奖 36 项、通信行业创新奖 3 项、集团科技进步奖 56 项等。

（1）安全技术与应用产品线

中国电信北京研究院安全技术与应用产品线（以下简称“产品线”），重点聚焦于网络与信息安全保障能力提升和安全服务产品研发领域，进行安全能力输出，致力于成为中国电信安全领域技术与产品的研发及创新基地。

依托“网络安全应急技术国家工程实验室”，在安全态势分析、应急演练与实验验证、云计算安全、物联网安全、SDN 安全、下一代安全等前沿领域展开技术研究，并与 CNCERT、北京邮电大学等机构和院校展开广泛合作。

立足“中国电信基础网络安全防护支撑和测评中心”的定位，研究网络 / 系统 / 业务安全等评估测评技术，开展标准化研究工作，切实解决大网实际安全问题。

自主研发云安全能力开放平台，实现专业安全能力对外开放，并探索安全能力产品化，形成“安全帮”品牌，实现安全服务产业链整合与价值链延伸。

近年来，产品线在安全防护、评估评测、安全管理等方面主导和参与 40 余个国家标准、

行业标准的制定，多人在国家标准组织、北京安全专家委理事任职；核心技术已申请发明专利 10 项，取得软件著作权 3 项；核心期刊发表论文 18 篇，出版安全专著 1 部；获工业和信息化部信息安全技术手段测试机构资质；荣获“2014 年通信网络和高层论坛安全管理与服务创新奖”。

产品线主要安全产品有：手机安全中心 APP，叠加了运营商差异化安全能力，全面保障用户安全；安全帮，包括 SaaS 安全服务电商 (www.anquanbang.net) 、SDS 软件定义安全平台、安全能力开放平台、安全大数据平台、安全态势感知平台，全面服务企业用户。

（2）中国电信安全帮

安全帮，是中国电信北京研究院安全产品线安全团队，自主研发安全产品，产品体系包括：安全帮 SaaS 安全服务电商 (www.anquanbang.net) 、SDS 软件定义安全平台、安全能力开放平台、安全大数据平台、安全态势感知平台。

安全帮 SaaS 安全服务电商 (www.anquanbang.net)，采用“SDS+SaaS+ 电商”的创新模式，主要服务于中小微企业，为企业用户提供专业的中国电信自有品牌的、第三方品牌的云化安全服务和安全能力 API，主要安全服务产品有网站安全监测服务、云 WAF 网站安全防护服务、上网行为管理服务、钓鱼网站监测服务等。用户通过在线注册购买，即可享受及时、在线、智能、便捷的安全服务。安全帮 SaaS 云安全服务电商的创立，旨在解决企业面临的安全厂商多、安全产品繁、安全投资大、安全人才缺 4 大问题，为企业省时省力省钱。

安全帮 SDS 软件定义安全平台、安全能力开放平台、安全大数据平台、安全态势感知平台 4 个系统，服务于中大型企业，提供系统级产品及服务。

A.2　北京神州绿盟信息安全科技股份有限公司

北京神州绿盟信息安全科技股份有限公司（以下简称绿盟科技），成立于 2000 年 4 月，总部位于北京。在国内外设有 40 多个分支机构，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。

基于多年的安全攻防研究，绿盟科技在检测防御类、安全评估类、安全平台类、远程安全运维服务、安全 SaaS 服务等领域，为客户提供入侵检测 / 防护、抗拒绝服务攻击、远程安全评估以及 Web 安全防护等产品以及安全运营等专业安全服务。

在物联网安全方面，绿盟科技已发布多份白皮书，如《工业控制系统及其安全性研究报告》、《绿盟科技物联网安全白皮书》等；对安全事件第一时间发布研究报告，如 2016 年 10 月，发布 Mirai 源码分析报告；漏洞挖掘能力出众，已发现多个工控产品漏洞，并在全球顶级安全技术大会 DEFCON 2017 上做报告；已推出多款工控安全产品，如工控漏洞扫描系统、工控入侵检测系统、工控安全审计系统、工业安全网关、工业安全隔离装置等。

北京神州绿盟信息安全科技股份有限公司于 2014 年 1 月 29 日起在深圳证券交易所创业板上市交易，股票简称：绿盟科技，股票代码：300369。

创新中心：创新中心是绿盟科技的前沿技术研究部门，包括云安全实验室、安全大数据分析实验室和物联网安全实验室。其作为“中关村科技园区海淀园博士后工作站分站”的重要培养单位之一，与清华大学进行博士后联合培养，科研成果已涵盖各类国家课题项目、国家专利、国家标准、高水平学术论文、出版专业书籍等。

创新中心持续探索信息安全领域的前沿学术方向，从实践出发，结合公司资源和先进技术，实现概念级的原型系统，进而交付产品线孵化产品并创造巨大的经济价值。

附录 B

参考文献

[1] 桂小林 , 张学军 , 赵建强 , 等 . 物联网信息安全 [M]. 北京 : 机械工业出版社 , 2014

[2] INCIBE, Red.es, 华为 . 华为物联网白皮书 [R].2017

[3] 中国通信标准化协会 . 物联网安全需求技术报告 [R].2015

[4] 车联网与大数据时代将产生无数应用前景 [EB/OL].http://www.cnii.com.cn/thingsnet/2014-09/10/content_1441643.htm

[5] 中国移动 . 中国智能家居发展情况分析报告 [R].2016

[6] 智能家居 . 智能家居行业应用前景广阔 , 未来产业呈现高速增长 [EB/OL].http://www.chinabgao.com/info/91502.html

[7] 诺威尔 . 智能监控在现实的应用 [EB/OL].https://wenku.baidu.com/view/9b1c5dd3d4d8d15abe234e74.html

[8] 李少伟 , 曹成涛 , 李锋 . 物联网技术在智慧物流中的应用 [J]. 数字技术与应用 , 2015(5)

[9] 时伟伟 . 智能穿戴设备的发展现状和趋势探析 [J]. 电脑知识与技术 ,2016(15)

[10] 范宇萌 . 能源 + 互联网的未来是怎样的？ [EB/OL].http://news.cnfol.com/it/20160406/22522983.shtml

[11] 瞄准智慧光伏电站 , 阳光电源分布式光伏全面发力 [EB/OL].http://www.ne21.com/news/show-59292.html

[12] 谢大平 , 李延 , 王于波 . 智能路灯控制系统安全性研究 [J]. 交通信息与安全 , 2013（5）

[13] 智能照明系统不安全？ ZLL 协议被曝存缺陷 [EB/OL].http://lights.ofweek.com/2016-11/ART-220001-8140-30062193_2.html

[14] NTI. 绿盟威胁情报中心 [EB/OL].https://nti.nsfocus.com/

[15] Shodan[EB/OL].https://www.shodan.io/

[16] ZoomEye[EB/OL].https://www.zoomeye.org/

[17] TR069 协议详解 [EB/OL].http://blog.csdn.net/ericfantastic/article/details/51542812

[18] 打印机智能化大势所趋 [EB/OL].http://column.iresearch.cn/b/201607/774585.shtml

[19] 黑客入侵打印机台湾逾 46 所学校遭勒索比特币 [EB/OL].https://www.icar2go.com/5392.html
[20] 中国打印机市场值得期待 [EB/OL].http://www.qianzhan.com/analyst/detail/220/150807-0da16321.html
[21] 全球 57 万台打印机端口暴露在物联网，打印机厂商怎么看 [EB/OL].https：//www.leiphone.com/news/201705/q7lM9ZICXOObUfFg.html
[22] 一文读懂汽车网络安全丨厚势 [EB/OL].https://www.sohu.com/a/162037721_465591
[23] TGU[EB/OL].http://jcarlosnorte.com/security/2016/03/06/hacking-tachographs-from-the-internets.html?winzoom=1
[24] IP 恒温器参考文档 [EB/OL].http://www.proliphix.com/Collateral/Documents/English-US/Basic%20Series%20Configuration%20Guide.pdf
[25] 智能设备漏洞泛滥 [EB/OL].http://www.cctime.com/html/2016-10-25/1232231.htm
[26] 威胁报告 [EB/OL]. http：//www.freebuf.com/articles/terminal/133668.html
[27] 中国信通院 . 物联网白皮书（2016）[EB/OL].http://www.caict.ac.cn/kxyj/qwfb/bps/201612/t20161228_2185496.htm
[28] 北京匡恩网络科技有限责任公司 .2016 年度物联网安全研究报告 [R].2016
[29] 梆梆安全研究院 .2016 物联网安全白皮书 [R]. 信息安全与通信保密杂志社 ,2016
[30] 物联网安全风险等 . 物联网安全及时 [M]. 北京：人民邮电出版社 , 2016
[31] 2017 年物联网安全问题报告 [EB/OL].http：//baijiahao.baidu.com/s?id=1567812857616118&wfr=spider&for=pc
[32] 桂小林 , 张学军 , 赵建强 , 等 . 物联网信息安全 [M]. 北京：机械工业出版社 , 2012
[33] 王浩，郑武，谢昊飞，智能制造发展规划（2016-2020）[EB/OL]. http://www.miit.gov.cn/n1146295/n1652858/n1652930/n3757018/c5406111/content.html
[34] 新型 IoT 机顶盒恶意软件 Rowdy 网络分析报告 ,http://blog.nsfocus.net/iot-set-top-box-malware-rowdy-network-analysis-report/
[35] 桂小林 , 安健 , 张文东 , 等 . 物联网技术导论 [M]. 北京：清华大学出版社 , 2012
[36] 雷吉成 . 物联网安全技术 [M]. 北京：电子工业出版社 , 2012
[37] YDB187-2017. 面向物联网应用的无线局域网空中接口技术要求 [S]
[38] YD186-2017. 面向物联网应用的无线局域网总体技术要求 [S]
[39] YD188-2017. 面向物联网应用的无线局域网组网技术要求 [S]
[40] YDB165-2017. 面向物联网的蜂窝窄带接入（NB-IoT）无线网总体技术要求 [S]
[41] 2016-1930T-YD. 面向物联网的蜂窝窄带接入（NB-IoT）安全技术要求和测试方法 [S]
[42] 2016-1854T-YD. 面向物联网的蜂窝窄带接入（NB-IoT）核心网总体技术要求 [S]
[43] TC8-WG1#47-009. 物联网感知层协议安全技术要求 [S]

[44] YD/T 2437-2012. 物联网总体框架与技术要求 [S]
[45] YDB101-2012. 物联网安全需求技术报告 [S]
[46] YDB172-2017. 物联网感知通信系统安全等级保护基本要求 [S]
[47] YDB173-2017. 物联网终端嵌入式操作系统安全技术要求 [S]
[48] 物联网安全风险威胁报告 [EB/OL]. http：//www.freebuf.com/articles/terminal/133668.html
[49] 2017 年物联网安全问题报告 [EB/OL]. http：//baijiahao.baidu.com/s?id=1567812857616118&wfr=spider&for=pc
[50] CVE[EB/OL].http：//cve.mitre.org/
[51] CNNVD[EB/OL].http：//www.cnnvd.org.cn/
[52] CNVD[EB/OL].http：//www.cnvd.org.cn/
[53] NVD[EB/OL].https：//nvd.nist.gov/
[54] FreeBuf[EB/OL]. http：//www.freebuf.com/
[55] DBSEC[EB/OL].http：//www.dbsec.cn/
[56] 法制日报 [EB/OL].http://www.legaldaily.com.cn/legaldailyintroduction/legaldailyintro.htm
[57] Hackernews[EB/OL].http：//hackernews.cc
[58] E 安全 [EB/OL].https：//www.easyaq.com
[59] 安全加 [EB/OL].http：//toutiao.secjia.com/
[60] CnBeta[EB/OL].http：//www.cnbeta.com
[61] 安全牛 [EB/OL].http：//www.aqniu.com
[62] 搜狐 [EB/OL].http：//www.sohu.com
[63] 千家网 [EB/OL].http：//www.qianjia.com
[64] COXBLUE[EB/OL].http：//www.coxblue.com
[65] 中商情报网 [EB/OL].http：//www.askci.com
[66] 网易财经 [EB/OL].http：//money.163.com
[67] 智能家居网 [EB/OL].http：//smarthome.ofweek.com

中国电信安全帮
www.anquanbang.net

中国电信北京研究院安全产品线
邮编：102209
电话：010-50902246
邮箱：service@anquanbang.net
地址：北京市昌平区未来科技城南区中国电信北京信息科技创新园