物联网安全白皮书

绿盟科技创新中心

《物联网安全白皮书》

由绿盟科技创新中心撰写

绿盟科技持续关注物联网安全的相关信息，如需了解更多，请联系：



特别声明

为避免客户数据泄露，所有数据在进行分析前都已经匿名化处理，不会在中间环节出现泄露，任何与客户有关的具体信息，均不会出现在本报告中。

版权声明

目录

一 . 物联网安全概述

1.1 引言

早在 1999 年，MIT AutoID 研究室的 Kevin Ashton 在研究将射频识别信息与互联网相连接的时候首先提到了物联网的概念；同年，在美国召开的移动计算和网络国际会议就提出，“传感网是下一个世纪人类面临的又一个发展机遇”；2005 年 11 月 17 日，信息社会世界峰会（WSIS）上，国际电信联盟（ITU）发布了《ITU 互联网报告 2005：物联网》，正式提出了“物联网”的概念；2009 年 8 月，温家宝总理到无锡物联网产业研究院考察时，明确指示在物联网的发展中，要早一点谋划未来，早一点攻破核心技术，并且明确要求尽快建立中国的传感信息中心，或者叫“感知中国”中心。物联网已经被视为继计算机和互联网之后的第三次信息技术革命。

那么什么是物联网呢？维基百科对于物联网（Internet of Things）的定义为物联网是将物理设备、车辆、建筑物和一些其它嵌入电子设备、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的网络。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基于计算机系统，从而提高效率、准确性和经济利益。经过二十多年的发展，物联网已经逐步融入到我们的生活中来。从应用于家庭的智能恒温器，智能电灯等设备，到与身体健康相关的智能穿戴设备。每一种智能设备的出现，都大大便利了人们的生活。

但是物联网在给人们的生活带来便利的同时，也会给人们带来种种隐忧。2014 年，研究人员演示了如何在 15 秒的时间内入侵家里的恒温控制器，通过对恒温控制器数据的收集，入侵者就可以了解到家中什么时候有人，他们的日程安排是什么等信息。许多智能电视带有摄像头，即便电视没有打开，入侵智能电视的攻击者可以使用摄像头来监视你和你的家人。攻击者在获取对于智能家庭中的灯光系统的访问后，除了可以控制家庭中的灯光外，还可以访问家庭的电力，从而可以增加家庭的电力消耗，导致极大的电费账单。种种安全问题提示人们，在享受物联网带来的方便快捷的同时，也要关注物联网的安全问题。

CSA 发布的白皮书《Security Guidance for Early Adopters of the Internet of Things （IoT）》[1] 中提到 IoT 带来如下新的挑战：

1 https://cloudsecurityalliance.org/download/new-security-guidance-for-early-adopters-of-the-iot/

（1）增加的隐私问题经常让人感到困惑。

（2）平台安全的局限性使得基本的安全控制面临挑战。

（3）普遍存在的移动性使得追踪和资产管理面临挑战。

（4）设备的数量巨大使得常规的更新和维护操作面临挑战。

（5）基于云的操作使得边界安全不太有效。

物联网是互联网的延伸，因此物联网的安全也是互联网安全的延伸，物联网和互联网的关系是密不可分、相辅相成的。但是物联网和互联网在网络的组织形态、网络功能以及性能上的要求都是不同的，物联网对实时性、安全可信性、资源保证等方面有很高的要求，物联网与互联网的区别在表 1.1 中得到体现。物联网的安全既构建在互联网的安全上，也有因为其业务环境而具有自身的特点。总的来说，物联网安全和互联网安全的关系体现在：物联网安全不是全新的概念，物联网安全比互联网安全多了感知层，传统互联网的安全机制可以应用到物联网，物联网安全比互联网**安全更复杂**。

表 1.1 物联网和互联网对比

	物联网	互联网
体系结构	分为感知层、网络层和应用层	比物联网少了感知层
操作系统	广泛使用嵌入式操作系统，如：VxWorks 等	通用操作系统（Window、UNIX、Linux 等），功能相对强大
系统实时性	一些领域如：工业控制对系统数据传输、信息处理的实时性要求较高 一些领域如：智能家居对系统的实时性要求不高	大部分系统的实时性要求不高，信息传输允许延迟，可以停机和重启恢复
通信协议	Zigbee，蓝牙，WiFi 也会用到互联网的协议（HTTP、HTTPS、XMPP 等）	TCP/IP、 HTTP、FTP、SMTP 等
系统升级	一些专有系统兼容性差、软硬件升级较困难，一般很少进行系统升级，如需升级可能需要整个系统升级换代	采用通用系统、兼容性较好，软硬件升级较容易，且软件系统升级较频繁
运维管理	不仅关注互联网所关注的问题，还关注对物联网设备远程控制和管理	互联网运维通常关注系统响应、性能
漏洞分析	针对行业特定协议的漏洞和嵌入式操作系统	通用操作系统 TCP/IP 协议
开发流程	不像传统 IT 信息系统软件在开发时拥有严格的安全软件开发规范及安全测试流程	开发时拥有严格的安全软件开发规范及安全测试流程
隐私问题	物联网的很多应用都与人们的日常生活相关，其应用过程中需要收集人们的日常生活信息，利用该信息可以直接或者间接地通过连接查询追溯到某个人	用户网络行为、偏好方面的信息
网络的组织形态	无线传感网传感器节点大规模分布在未保护或敌对环境中；无线多跳通信；设备资源受限	网络节点大多分布在受保护的环境中；设备资源充足。
物理安全	节点物理安全较薄弱	主机大多分布在受保护的环境中

1.2 物联网安全的体系结构

对于物联网安全的体系结构的理解有助于快速找到安全的切入点，本节将首先介绍物联网的体系结构，然后引出物联网安全的体系结构。

物联网的体系结构通常认为有 3 个层次：底层是用来感知（识别、定位）的感知层，中间是数据传输的网络层，上面是应用层。

感知层包括以传感器为代表的感知设备、以 RFID 为代表的识别设备、GPS 等定位追踪设备以及可能融合部分或全部上述功能的智能终端等。感知层是物联网信息和数据的来源，从而达到对数据全面感知的目的。

网络层包括接入网和核心网。接入网可以是无线近距离接入，如无线局域网、ZigBee、蓝牙、红外，也可以是无线远距离接入，如移动通信网络、WiMAX 等，还可能是其他形式的接入，如有线网络接入、现场总线、卫星通信等。网络层的承载是核心网，通常是 IPv4 网络。网络层是物联网信息和数据的传输层，将感知层采集到的数据传输到应用层进行进一步的处理。

应用层对通过网络层传输过来的数据进行分析处理，最终为用户提供丰富的特定服务，如智能电网、智能物流、远程医疗、智能交通、智能家居、智慧城市等。依靠感知层提供的数据和网络层的传输，进行相应的处理后，可能再次通过网络层反馈给感知层。应用层对物联网信息和数据进行融合处理和利用，达到信息最终为人所使用的目的。

物联网的安全架构可以根据物联网的架构分为感知层安全、网络层安全和应用层安全。如图 1.1，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，网络层安全用于保障通信安全，应用层则关注于各类业务及业务的支撑平台的安全。

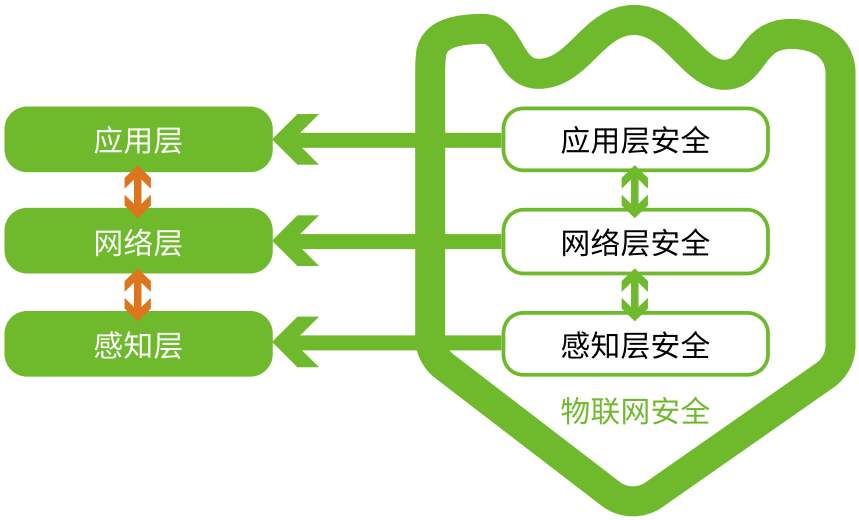


图 1.1 物联网安全体系结构

1.3 研究项目和标准化组织

1.3.1 物联网安全项目

物联网安全项目（Secure Internet of Things Project ）是一个跨学科的研究项目，包括斯坦福大学、UC 伯克利大学和密歇根大学的计算机系和电子工程系。

项目为期 5 年，目标是：

（1）研究和定义新的密码学计算模型和安全机制以确保物联网设备在未来数十年的安全。

（2）研究和实现安全、开源的软硬件框架来对物联网应用进行原型和构建，使其可以正确使用这些新的机制。

研究涉及三个方面：

（1）分析

如何将物理世界的巨大的数据流与现有数据集成？

（2）安全

泛在的传感和分析系统如何保护用户安全？

（3）软硬件系统

什么样的软硬件系统可以使得对于物联网安全应用的开发和现在的 Web 应用一样容易？

2015 年 6 月确定了第一年的研究计划：

（1）20 年的安全

物联网设备周边的计算机基础设施发展迅速（我们会更换手机，服务器也会去更新），但是设备本身依然处于部署状态，因此必须能够准备好以适应和经受安全局面的改变。20 年的安全方面的工作主要有三个方面：

第一，设计未来嵌入式 SoC 所需要的密码学原语。密码学趋于计算密集，因此如果运行在软件中会消耗大量的嵌入式设备的功耗，硬件的支持使得密码学更有效率，但是能够在未来 20 年使用的加密算法会与今天正在使用的有很大的不同。在未来，量子计算机会成为现实，因此物联网设备需要可以抵抗量子攻击的签名算法。由于嵌入式 SoC 的成本降低，可以在其中加入可编程密码部件的支持。

第二，关于随机数生成。随机数是密码学和计算机安全的基础，然而，物联网设备使用的低功耗微控制器中很少具备现代处理器中用于生成随机数的硬件部件（如 x86 的 RDRAND 和 RDSEED 指令）。此外，正确和安全的生成随机数需要精心设计。物联网安全的一个关键是快速而价格低廉的随机数生成方法，这使得任何人可以轻易并入设备中。我们将探索软硬件结合的方法来在嵌入式设备的整个生命周期提供足够的随机性。

第三，设计和实现新的、安全的嵌入式操作性系统。当下的嵌入式系统主要使用低层次的 C 语言编写。在 20 世纪末，这导致了缓冲区溢出和许多其他的安全漏洞。桌面和服务器上的操作系统使用多种技术和硬件机制来抵抗这些攻击，但是嵌入式处理器并不具备这样的能力。我们的假设是使用一个类型安全的系统语言可以提供一个可证明安全的操作系统内核，从而允许多个不可信的应用（如智能手表上加载的多个应用）同时运行。

（2）应用开发框架

大部分的物联网应用遵从 MGC 架构，由三部分组成，嵌入式设备（eMbedded devices）、网关设备（Gateway device）如手机和云中（Cloud）或网络中的服务器。这些设备使用自己的语言、操作系统和应用框架，在这些系统之间验证和建立安全特性很困难。我们将研究新的操作系统、网络协议和工具来使得一个通过所有这些设备的应用依旧可以维持其安全特性。如果安全很难使用，开发人员则会选择不使用。因此，我们的目标是使得安全物联网应用的开发和现代的网站开发一样容易。我们将研究如何支持软件定义的硬件（software-defined hardware），使得软件工程师可以根据代码中所需的库和特性来指定物联网设备。现在的做法是使用数据合成技术来自动读取数以千计的数据手册，从而形成一个丰富的数据库。

（3）物联网网关

网关是几乎所有物联网应用的关键部分。它提供了低功耗的无线网络和互联网之间的桥梁。我们正在探索网关需要提供给用户和应用怎样的特点和抽象。当前关注于两个问题：通信可见性（communication visibility）和应用沙盒化（application sandboxing）。

假设在未来你的家庭中有 100 到 1000 的物联网设备，它们在做什么？当前这些设备都是黑盒，例如，你并不能看到你的 Nest 恒温器正在发送什么，由于它与 Nest 服务器是通过加密的端到端连接的。与笔记本和电话不同的是，用户并不能在恒温器上安装新的安全证书以使得用户可以看到它的数据。我们假设这是物联网系统的一个基本需求：用户可以看到他们的设备是如何通信的以及通信内容。从技术角度来看，物联网网关应该提供物联网设备正在与什么样的服务和系统进行通信的信息。这些收集的数据可以提供有价值的关于什么是正常行为、它们正在做什么的洞见。这种检测流量的能力并不仅仅是查看发送的数据包有多少字节，当用户授权网关对于设备的权限时，网关具有窥探流量内容的能力。这种窥探的能力不能违反完整性，同时网关在看到流量的同时也不能伪造数据。达到这两个目标需要新的密码学和协议机制。

研究人员期望物联网网关可以发展成富应用平台（rich application platforms），就像当下的手机一样。有两个理由支持这种观点：一是对于用户体验和交互性来说拥有本地接口和数据存储是非常有用的，二是即使与互联网的连接中断，这些应用也需要持续工作。物理网关对于嵌入式设备可以提供有用的安全保护。低功耗操作和受限的软件支持意味着频繁的固件更新代价太高甚至不可能实现。反而，网关可以主动更新软件（高级防火墙）以保护嵌入式设备免受攻击。实现这些特性需要重新思考运行在网关上的操作系统和其机制。研究人员正在探索类似 Intel SGX 和 ARM TrustZone 这样的技术如何

对网关和其上的应用提供新的安全保护。

1.3.2 TRUST

TRUST[2] 是斯坦福大学的计算机安全实验室[3] 的一个项目，针对的是物理基础设施的安全研究。该项目定位于下一代的 SCADA 和网络嵌入式系统，它们控制关键的物理基础设施（如电网、天然气、水利、交通等）以及未来的基础设施（如智能建筑）和结构（如 active-bridges，它的结构完整性依赖于动态控制或 actuators）。

该研究具有前瞻性，随着工业化与信息化的融合，原有的工业控制环境发生了变化，为了更好地抵抗来自互联网的攻击，有必要设计下一代的 SCADA 和网络嵌入式系统。

1.3.3 OWASP Internet of Things Project

开放式 Web 应用程序安全项目（OWASP，Open Web Application Security Project）[4] 是一个组织，它提供有关计算机和互联网应用程序的公正、实际、有成本效益的信息。其目的是协助个人、企业和机构来发现和使用可信赖软件。OWASP 物联网项目的目标是帮助制造商、开发人员、消费者更好地理解与物联网相关的安全问题，使得用户在构建、部署或者评估物联网技术时可以更好地制定安全决策。该项目包括物联网攻击面、脆弱性、固件分析、工控安全等子项目。

1.3.4 CSA

云安全联盟（Cloud Security Alliance，CSA）[5]，成立于 2009 年 3 月 31 日，其成立的目的是为了在云计算环境下提供最佳的安全方案。CSA 包含很多个工作组，其中的物联网工作组（https://cloudsecurityalliance.org/group/internet-of-things/）关注于理解物联网部署的相关用例以及定义可操作的安全实施指南。主要关注于如下方面：

（1）分析不同行业物联网实现的用例；

（2）物联网安全实现的最佳实践；

（3）实现物联网安全控制和云控制矩阵的映射；

（4）确定物联网设备和实现的威胁；

（5）确定安全标准和物联网安全实践之间的差距；

（6）确定技术解决方案和物联网安全实践之间的差距；

（7）研究物联网安全新方法；

（8）与其他 CSA 组织合作共同化解物联网安全控制的冲突；

2 https://www.truststc.org/index.html
3 http://seclab.stanford.edu/
4 https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
5 https://cloudsecurityalliance.org/

（9）保证支持物联网的云基础设施和服务的安全；

（10）保护边界设备安全，防止通过边界设备进入企业内部；

（11）物联网的审计、验证、访问控制、授权、库存管理、隐私和风险管理的解决方案。

1.3.5 NIST

美国国家标准与技术研究院（National Institute of Standards and Technology，NIST）直属美国商务部，从事物理、生物和工程方面的基础和应用研究，以及测量技术和测试方法方面的研究，提供标准、标准参考数据及有关服务，在国际上享有很高的声誉

国家安全和经济安全依赖于可靠的关键基础设施的运作。网络空间安全对关键基础设施系统会造成很大的影响，为了能够处理这个威胁，NIST[6] 提出了网络安全架构。这个架构是由一系列的工业标准和工业最佳实践组成的，目的是帮助企业管理网络空间安全威胁。

这个架构是业务驱动的，来指导网络空间安全活动，并使企业将考虑网络空间安全威胁作为企业威胁管理的一部分，架构主要包括三个部分：架构核心、架构轮廓和架构实现层。这个架构使企业 -- 不管规模是多少、面临的网络安全威胁有多严重或者网络空间安全问题的复杂性—都可以应用这些规则和最佳实践来进行风险管理以提高关键基础设施的安全性和恢复力。

1.3.6 IoT Security Foundation

IoTS[7] 的成员包括 ARM、华为等公司。他们的目标是帮助物联网实现安全性，使得物联网能够被广泛使用，同时他的优点能够被最大化的利用。为了实现这个目标，他们要提升技术理论水平和了解业界的最佳实践，为那些生产或者使用物联网设备的人提供支持。

包含五个工作组：

（1）自认证方案

这个工作组的目标是为创建低成本的、易于实现的并且与目标相匹配的自认证系统进行需求分析，以提高物联网产品的安全标准。

（2）面向用户产品

这个工作组的目标是为不同层次的用户设备提供与之相对应的最佳安全实践指南。

（3）修补现有的设备

低成本的 IoT 系统主要的挑战是如何保证系统在他的生命周期中的可维护性和可更新性，这个工作组的目标是为系统部署受限的资源要素提供最佳实践指南。

（4）负责任的披露

6 http://www.nist.gov/cps/

7 https://iotsecurityfoundation.org/working-groups/

当一个研究人员在你的产品中发现了一个脆弱点以后将会发生什么？这个工作组的目标是建立一个交流通道，并且建立一个最佳实践框架给研究人员和企业来遵从。

（5）物联网蓝图

这个工作组寻求在更高的层次，在系统范围或者端到端的角度建立物联网映射，找到系统脆弱性在哪里，并指导 IoTSF 未来的工作方向。

二 . 物联网安全需求及对策

2.1 引言

物联网技术的出现，使我们的生活更加方便、快捷的同时，也不可避免地带来了一些安全问题。物联网中的很多应用都与我们的生活息息相关，如摄像头，智能恒温器等设备，通过对它们的信息的采集，可直接或间接地暴露用户的隐私信息。由于生产商缺乏安全意识，很多设备缺乏加密、认证、访问控制管理的安全措施，使得物联网中的数据很容易被窃取或非法访问，造成数据泄露。物联网这种新型的信息网络往往会遭受有组织的 APT 攻击。由此可见，物联网安全问题需要引起我们的高度重视。

物联网涵盖范围广泛，本章关注于物联网安全中较为通用的安全需求，并给出了相应的对策，让读者对物联网安全需求和研究方向有更加深刻的了解。通过图 2.1，也可以发现，物联网的不同层次可能面临相同的安全需求。

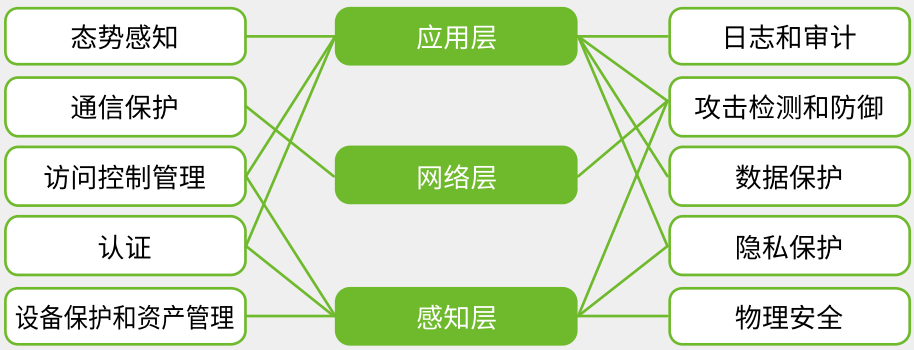


图 2.1 物联网各层的安全需求

2.2 隐私保护

物联网中的很多应用都与我们的生活息息相关，如摄像头，智能恒温器等设备，通过对它们的信息的采集，会直接或间接地暴露用户的隐私信息。所以隐私保护是物联网安全问题中应当注意的问题之一。

（1）威胁

基于数据的隐私威胁：物联网中数据采集、传输和处理等过程中的隐私信息泄露。

基于位置的隐私威胁：物联网中各节点的位置隐私以及物联网在提供

各种位置服务时的位置隐私泄露问题。

（2）对策

通信加密。

最小化数据采集。

匿名化数据采集和处理。

由相关用户决定是否授权数据采集。

路由协议隐私保护法保护节点准确位置信息。

2.3 认证

（1）威胁

物联网环境中的部分访问无认证或认证采用默认密码、弱密码。

（2）对策

一方面开发人员应考虑在设计时确保用户在首次使用系统时修改默认密码，尽可能使用双因素认证，对于敏感功能，需要再次进行认证等；

另一方面作为用户，应该提高安全意识，采用强密码并定期修改密码。

2.4 访问控制管理

（1）威胁

未授权访问

安全配置长期不更新、不核查

（2）对策

身份和访问管理、边界安全（安全访问网关）。

持续的脆弱性和错误配置检测清除。

网关是很多公司的关注点。Vidder 公司的产品基于 CSA 定义的软件定义边界，只有认证后才能对服务进行访问。CUJO 公司的智能防火墙，采用了网关 + 云 + 手机 APP 的模式，手机 APP 可以看到对于内部网络的访问情况，并进行访问控制，云端对网关采集的流量数据进行分析并提供预警。

未来的智能家庭安全将会是一个关注点，随着家庭中智能设备的增多，设备本身的访问控制并不足以抵抗日益复杂的网络攻击，如果设备本身存在漏洞，攻击者将可能绕过设备的认证环节。一个自然的思路是在网络的入口做统一的访问控制，只有认证的流量才能够访问内部的智能设备。

2.5 数据保护

（1）威胁

数据的泄露和篡改问题。如基于修改的医疗数据，医疗服务提供者有可能错误地对患者进行诊断和治疗。

（2）对策

很多公司都提供了 DLP 产品。

对于物联网环境下的数据安全问题，信息安全公司一般采用将已有的 DLP 产品作为解决方案的一部分进行推出。

2.6 物理安全

（1）威胁

部署在远端的缺乏物理安全控制的物联网资产有可能被盗窃或破坏。

（2）对策

尽可能加入已有的物理安全防护措施。

并非技术层面的问题，更应作为标准的一部分进行规范。

2.7 设备保护和资产管理

（1）威胁

设备的配置文件被修改。

设备的数量巨大使得常规的更新和维护操作面临挑战。

未认证代码执行。

断电引发的异常。

设备逆向工程。

（2）对策

定期审查配置。

固件自动升级（over-the air （OTA））。

定义对于物联网设备的全生命周期控制。

对代码签名以确保所有运行的代码都是经过认证的，以及在运行时防护。

断电保护。

用白盒密码来应对逆向工程。

物联网环境下有两点尤其要注意，一是众多设备如何升级，二是对于设备的逆向工程。对于第一点，应定义对于物联网设备的全生命周期控制，并提供设备固件自动升级的方式；对于第二点，目前已知的技术是采用白盒密码。

2.8 攻击检测和防御

2.8.1 拒绝服务攻击

（1）威胁

在物联网中拒绝服务攻击主要分为两种，一种是对设备进行攻击，如：一直给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它系统进行攻击。

（2）对策

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的节点的方法。

Zilog 和 Icon Labs 联合推出了使用 8 位 MCU 的设备的安全解决方案。防火墙控制嵌入式系统处理的数据包，锁定非法登录尝试、拒绝服务攻击、packet floods、端口扫描和其他常见的网络威胁。

2.8.2 病毒攻击

（1）威胁

病毒攻击指在计算机程序中插入的破坏计算机功能或者数据的代码。

（2）措施

物联网设备需要代码签名，以确保所有运行的代码都是经过授权和认证的。

赛门铁克的白皮书中指出设备保护需要对代码签名以确保所有运行的代码都是经过认证的；天威诚信 VeriSign 代码签名证书；Instant SSL、微软、Digicert 等都在做代码签名相关的工作。

2.8.3 APT 攻击

（1）威胁

APT（Advanced Persistent Threat）指的是高级持续性威胁。 利用先进的攻击手段有组织地对特定目标进行长期持续性网络攻击。APT 入侵途径主要包括以下几个方面。

1）以智能手机、平板电脑和 USB 等移动设备为攻击对象，进而入侵企业信息系统。

2）恶意邮件，钓鱼网站，恶意链接等。

3）利用防火墙、服务器等系统漏洞继而入侵企业网络。

（2）对策

1）使用威胁情报。

及时获取最新的威胁情报信息，如：APT 操作者的最新信息；不良域名；恶意邮件地址，附件，主题；恶意链接和网站等信息，及时进行防护。

2）建立防火墙和网关，进行访问控制。定期检查配置信息，及时更新升级。

3）收集日志进行分析和溯源。

4）全网流量行为的模型建立和分析。

5）对用户的访问习惯进行监测。

在检测到 APT 攻击的同时，也可以对 APT 攻击进行监测和溯源分析，并将威胁情报共享。

2.8.4 蜜罐

蜜罐是设置好故意让人攻击的目标，引诱黑客前来攻击。所以攻击者入侵后，你就可以知道他是如何得逞的，可以让人随时了解针对系统所发动的最新的攻击和漏洞。

2.9 态势感知

态势感知是在大规模系统环境中，对能够引起系统状态发生变化的安全要素进行获取、理解、显示以及预测未来的发展趋势。

这里我们将对一个态势感知系统中比较重要的几部分进行介绍。

2.9.1 异常行为检测

异常行为检测的方法一般是运用大数据分析技术，在特定的环境中，如工控领域等可以进行全流量分析和深度包检测。

一个异常行为检测系统应能自动进行异常行为检测，对客户的网络进行分析，知道什么是正常的行为，并建立一个基线，然后如果发现不正常的或者可疑的行为就会报警。除监视应用程序的行为外，它还应监视文件，设置，事件和日志，并报告异常行为。

总结来说有两种方法，一个是建立正常行为的基线，从而发现异常行为，另一种是对日志文件进行总结分析，发现异常行为。

2.9.2 脆弱性评估

客户如何知道他们是否采用了足够的安全措施，或者是否采用了正确的步骤来保护他们的资产和业务。客户需要从众多的公布的标准和最佳实践中获取信息来指导他们的工作，但是有时候阅读和理

解一些相关的标准有些困难。所以需要为用户提供一套解决方案来被动或者主动地评估系统、网络和应用，发现不良行为，并不断提供脆弱性评估报告。

脆弱性评估应具备从多传感器中收集到的网络通信和事件信息数据来分析环境的脆弱性和威胁的能力，对 IT 安全进行持久的监控。

2.9.3 威胁情报交换

物联网设备的经销商、制造商甚至政府机构能够合作起来，及时发现各类木马病毒和 0day 漏洞威胁，防范并拦截 APT 攻击、未知威胁等新型恶意攻击，实现共赢局面。

Intel 白皮书中指出汽车的经销商、制造商甚至政府机构能够合作起来，进行威胁情报交换，能够快速将零日漏洞和恶意软件通知相应的车辆。CUJO 通过将流量信息与商业威胁情报源进行对比，以确保未授权的 IP 没有连接到用户的网络中。

通过利用威胁情报，及时对最新的攻击进行防御。当遭受到未知攻击的时候，及时将威胁情报发布出去，实现威胁情报的共享。

2.9.4 可视化展示

可视化展示能够直观的呈现数据特点，同时容易被读者接受和理解，所以大数据分析（深度包检测、全流量分析）结果需要可视化展示。

大多数分析系统都有可视化的功能，如：NexDefense 支持网络流量 3D 可视化等。

可以通过与手机 APP 结合实现移动可视化。

2.9.5 物联网事件响应措施

当系统遭到攻击时，需要快速的识别攻击来源，攻击路径，对攻击做出快速的响应，在攻击造成更大的破坏之前，实施有效的措施，减少损失。在攻击之后，需要快速地防止此类攻击的再次发生。

采用的策略一般是态势感知中的常用方法、异常行为检测和及时打补丁。

2.10 通信保护

物联网设备与设备之间，设备与远程系统之间需要进行通信，如果通信缺少传输加密和完整性验证，那么通信很可能会被窃听或篡改。通信保护需要对于设备和远程系统之间的通信进行加密和认证。

很多公司的产品或者解决方案中都有数据的传输加密、以及授权和认证功能模块，如 Mocana 公司的安全服务平台；Arrayent 的 Arrayent Connect Platform；Device Authority 的 Data Centric Security Platform；SecureRF 开发了快速，超低功耗的加密工具，Bastille 指出的无线鼠标和键盘劫持问题也与通信保护有关。

在工控场景中，可通过单向网闸，实现数据只能从低安全等级的系统流向高安全等级的系统。

2.11 日志和审计

（1）威胁

对于威胁的检测。

行业安全标准的合规。

（2）对策

日志分析。

合规性检查。

从行业角度来说，特定行业的合规性必不可少。对于日志的分析有可能发现潜在的威胁，但关键点在大数据的分析能力。

三 . 物联网安全相关技术

3.1 引言

物联网安全产品的核心在于技术，由于物联网的安全是互联网安全的延伸，那么我们可以利用互联网已有的安全技术，结合物联网安全问题的实际需要，改进已有技术，将改进后的技术应用到物联网中，从而解决物联网的安全问题。如：互联网环境中的防火墙技术，主要是对 TCP/IP 协议数据包进行解析，而在物联网环境中，防火墙还需要对物联网中的特定协议进行解析，如工控环境中的 Modbus、PROFIBUS 等协议。此外物联网还有其独特性，如终端设备众多，设备之间缺乏信任的问题，互联网中现有的技术难以解决此类问题，所以我们还需要探索一些新的技术来解决物联网中特有的新问题。此外，由于物联网将许多原本与网络隔离的设备连接到网络中，大大增加了设备遭受攻击的风险。同时物联网中的设备资源受限，很多设备在设计时较少考虑安全问题。还有物联网中协议众多，没有统一标准等等这些安全隐患都可能被黑客利用，造成极大的安全问题，所以我们需要利用一些漏洞挖掘技术对物联网中的服务平台，协议、嵌入式操作系统进行漏洞挖掘，先于攻击者发现并及时修补漏洞，有效减少来自黑客的威胁，提升系统的安全性。因此主动发掘并分析系统安全漏洞，对物联网安全具有重要的意义。

通过对物联网安全需求和对策的分析，我们总结出以下需要重点关注的技术。本章将分别从已有技术在物联网环境中的应用、新技术的探索和物联网相关设备、平台、系统的漏洞挖掘和安全设计三个方面介绍物联网安全技术研究的一些思路。

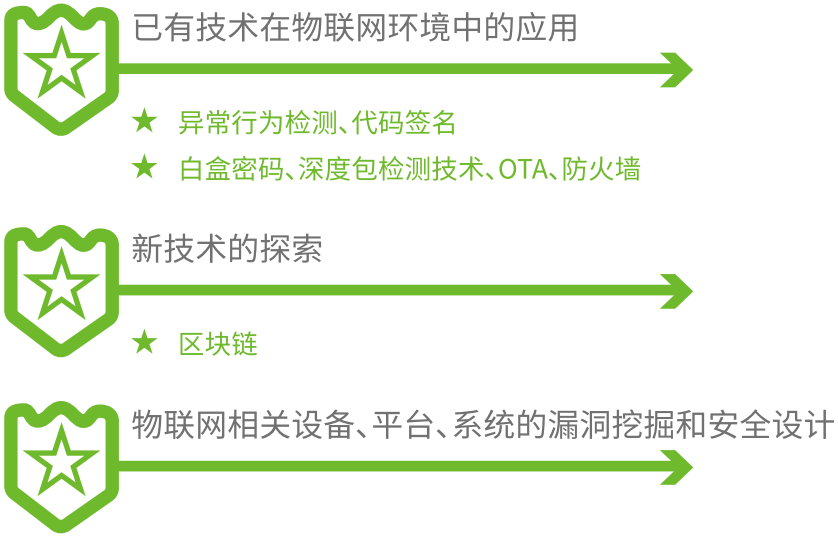


图 3.1 物联网安全相关技术

3.2 已有技术在物联网环境中的应用

3.2.1 异常行为检测

异常行为检测对应的物联网安全需求为攻击检测和防御、日志和审计。

文章前面已经提到过，异常行为检测的方法通常有两个：一个是建立正常行为的基线，从而发现异常行为，另一种是对日志文件进行总结分析，发现异常行为。

物联网与互联网的异常行为检测技术也有一些区别，如利用大数据分析技术，对全流量进行分析，进行异常行为检测，在互联网环境中，这种方法主要是对 TCP/IP 协议的流量进行检测和分析，而在物联网环境中，还需要对其它的协议流量进行分析，如工控环境中的 Modbus、PROFIBUS 等协议流量。此外，物联网的异常行为检测也会应用到新的应用领域中，如在车联网环境中对汽车进行异常行为检测。360 研究员李均 [8] 利用机器学习的方法，为汽车的不同数据之间的相关性建立了一个模型，这个模型包含了诸多规则。依靠对行为模式、数据相关性和数据的协调性的分析对黑客入侵进行检测。

3.2.2 代码签名

对应的物联网安全需求：设备保护和资产管理、攻击检测和防御。

通过代码签名可以保护设备不受攻击，保证所有运行的代码都是被授权的，保证恶意代码在一个正常代码被加载之后不会覆盖正常代码，保证代码在签名之后不会被篡改。相较于互联网，物联网中的代码签名技术不仅可以应用在应用级别，还可以应用在固件级别，所有的重要设备，包括传感器、交换机等都要保证所有在上面运行的代码都经过签名，没有被签名的代码不能运行。

由于物联网中的一些嵌入式设备资源受限，其处理器能力，通信能力，存储空间有限，所以需要

8 http://www.leiphone.com/news/201605/yi85tcbQlReaA0cy.html

建立一套适合物联网自身特点的、综合考虑安全性、效率和性能的代码签名机制。

3.2.3 白盒密码

对应的物联网安全需求：设备保护和资产管理。

物联网感知设备的系统安全、数据访问和信息通信通常都需要加密保护。但由于感知设备常常散布在无人区域或者不安全的物理环境中，这些节点很可能会遭到物理上的破坏或者俘获。如果攻击者俘获了一个节点设备，就可以对设备进行白盒攻击。传统的密码算法在白盒攻击环境中不能安全使用，甚至显得极度脆弱，密钥成为任何使用密码技术实施保护系统的单一故障点。在当前的攻击手段中，很容易通过对二进制文件的反汇编、静态分析，对运行环境的控制结合使用控制 CPU 断点、观测寄存器、内存分析等来获取密码。在已有的案例中我们看到，在未受保护的软件中，密钥提取攻击通常可以在几个小时内成功提取以文字数据阵列方式存放的密钥代码。

白盒密码算法[9]是一种新的密码算法，它与传统密码算法的不同点是能够抵抗白盒攻击环境下的攻击。白盒密码使得密钥信息可充分隐藏、防止窥探，因此确保了在感知设备中安全地应用原有密码系统，极大提升了安全性。

白盒密码作为一个新兴的安全应用技术，能普遍应用在各个行业领域、应用在各个技术实现层面。例如，HCE 云支付、车联网，在端点（手机终端、车载终端）层面实现密钥与敏感数据的安全保护；在云计算上，可对云上的软件使用白盒密码，保证在云这个共享资源池上，进行加解密运算时用户需要保密的信息不会被泄露。

3.2.4 over-the air（OTA）

对应的物联网安全需求：设备保护和资产管理。

空中下载技术（over-the air，OTA），最初是运营商通过移动通信网络（GSM 或者 CDMA）的空中接口对 SIM 卡数据以及应用进行远程管理的技术，后来逐渐扩展到固件升级，软件安全等方面。

随着技术的发展，物联网设备中总会出现脆弱性，所以设备在销售之后，需要持续的打补丁。而物联网的设备往往数量巨大，如果花费人力去人工更新每个设备是不现实的，所以 OTA 技术在设备销售之前应该被植入到物联网设备之中。

3.2.5 深度包检测（DPI ）技术

对应的物联网安全需求：攻击检测和防御。

互联网环境中通常使用防火墙来监视网络上的安全风险，但是这样的防火墙针对的是 TCP/IP 协议，而物联网环境中的网络协议通常不同于传统的 TCP/IP 协议，如工控中的 Modbus 协议等，这使得控制整个网络风险的能力大打折扣。因此，需要开发能够识别特定网络协议的防火墙，与之相对应的技术则为深度包检测技术。

9 http://china.safenet-inc.com/webback/UploadFile/DownloadDoc/46825c79-0829-46d1-acdd-03cf7de742 8d.pdf

深度包检测技术（deep packet inspection，DPI）是一种基于应用层的流量检测和控制技术，当 IP 数据包、TCP 或 UDP 数据流通过基于 DPI 技术的带宽管理系统时，该系统通过深入读取 IP 包载荷的内容来对 OSI 七层协议中的应用层信息进行重组，从而得到整个应用程序的内容，然后按照系统定义的管理策略对流量进行整形操作。

思科和罗克韦尔[10]自动化联手开发了一项符合工业安全应用规范的深度数据包检测 （DPI ）技术。采用 DPI 技术的工业防火墙有效扩展了车间网络情况的可见性。它支持通信模式的记录，可在一系列安全策略的保护之下提供决策制定所需的重要信息。用户可以记录任意网络连接或协议（比如 EtherNet/IP）中的数据，包括通信数据的来源、目标以及相关应用程序。

在全厂融合以太网 （CPwE ）架构中的工业区域和单元区域之间，采用 DPI 技术的车间应用程序能够指示防火墙拒绝某个控制器的固件下载。这样可防止滥用固件，有助于保护运营的完整性。只有授权用户才能执行下载操作。

3.2.6 防火墙

对应的物联网安全需求：攻击检测和防御。

物联网环境中，存在很小并且通常很关键的设备接入网络，这些设备由 8 位的 MCU 控制。由于资源受限，对于这些设备的安全实现非常有挑战。这些设备通常会实现 TCP/IP 协议栈，使用 Internet 来进行报告、配置和控制功能。由于资源和成本方面的考虑，除密码认证外，许多使用 8 位 MCU 的设备并不支持其他的安全功能。

Zilog[11] 和 Icon Labs[12] 联合推出了使用 8 位 MCU 的设备的安全解决方案。Zilog 提供 MCU，Icon Labs 将 Floodgate 防火墙 [13] 集成到 MCU 中，提供基于规则的过滤，SPI（Stateful Packet Inspection）和基于门限的过滤（threshold-based filtering）。防火墙控制嵌入式系统处理的数据包，锁定非法登录尝试、拒绝服务攻击、packet floods、端口扫描和其他常见的网络威胁。

10 http://www.automation.com/automation-news/industry/rockwell-and-cisco-developing-dpi-technology-for- enhanced-security
11 http://www.zilog.com/
12 http://www.iconlabs.com/
13 http://www.iconlabs.com/prod/products/device-protection/floodgate-firewall

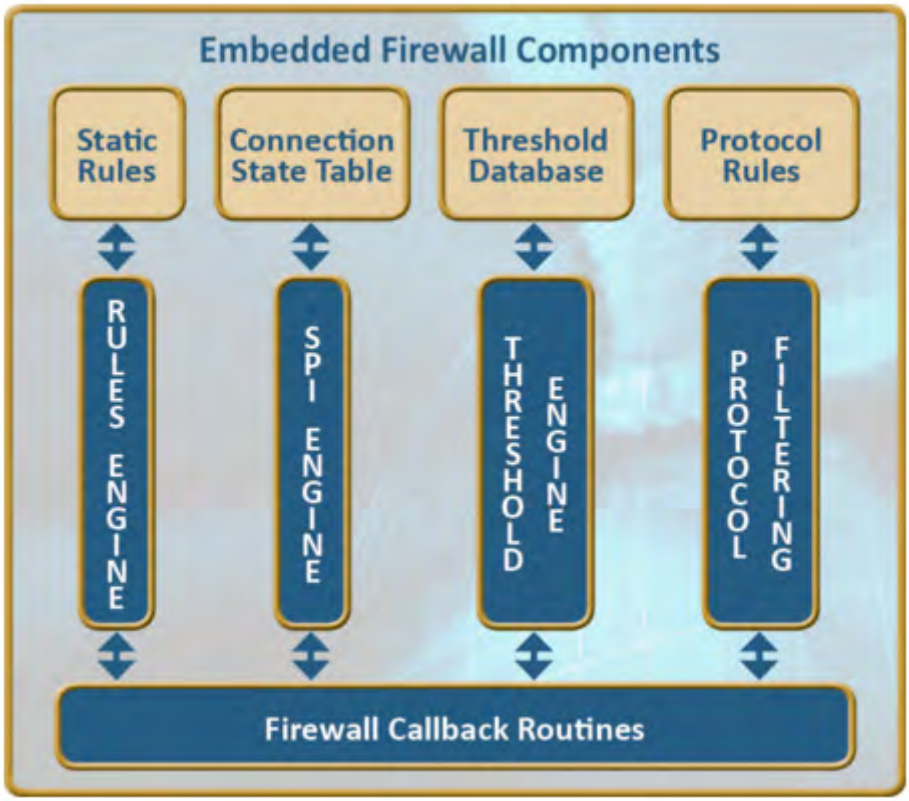


图 3.2 嵌入式防火墙

3.2.7 访问控制

对应的物联网安全需求：认证、访问控制管理

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来阻止外部用户的进入，但是允许内部用户对外的访问。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。企业网络架构中的固定的边界模型正在变得过时，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。

软件定义边界（Software Defined Perimeter，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、私营企业网络上，或者穿过这些位置的一些全部。

SDP 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。

大量设备连接到 Internet 中，管理这些设备、从这些设备中提取信息的后端应用通常很关键，扮演了隐私或敏感数据的监护人的角色。SDP 可以被用来隐藏服务器和服务器与设备的交互，从而最大

化地保障安全和运行时间

3.3 新技术的探索

3.3.1 区块链

对应的物联网安全需求：认证

区块链（Blockchain，BC）[14] 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（chain）下一个数据库块。结合区块链的定义，需要有这几个特征：去中心化（Decentralized）、去信任（Trustless）、集体维护（Collectively maintain）、可靠数据库（Reliable Database）、开源性、匿名性。区块链解决的核心问题不是“数字货币”，而是在信息不对称、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、自动地与其它物件、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。

越来越多的侵犯用户隐私的报告说明第三方收集和控制大量的个人数据的模式需要被改变。IBM[15] 认为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。IBM 认为中本聪的比特币区块链技术可以完满地解决这个问题。

Guy Zyskind 等人 [16] 提出一种分散式的个人数据管理系统，来实现用户数据的保护，确保用户可以拥有并管理自己的数据。实现了将区块链应用于自动访问控制管理而不需要可信第三方。与比特币不同，系统交易（transaction）不是严格的金融交易——他们被用于携带指令，比如存储、查询和共享数据的指令。

3.4 物联网相关设备、平台、系统的漏洞挖掘和安全设计

物联网相关设备、平台、系统的漏洞挖掘技术，有助于发现 0day 漏洞和未知威胁，从而提升 IDS、防火墙等安全产品的检测和防护能力。

将安全产品嵌入到设备之中，或者产品设计时采用物联网设备安全框架，在物联网设备生产之时就考虑安全问题，可以极大提升物联网设备的安全性。

3.4.1 物联网平台漏洞挖掘

14 https://www.zhihu.com/question/27687960
15 http://36kr.com/p/215152.html
16 http://web.media.mit.edu/~guyzys/data/ZNP15.pdf

随着物联网的发展，将会出现越来越多的物联网平台。BAT 三家均已推出了智能硬件开放平台[17]。国外免费的物联网云平台有 Temboo、Carriots、NearBus 和 Ubidots。不过，目前对于物联网平台的安全性的分析还不多，相信以后物联网平台的安全性将会越来越多地吸引到人们的关注。

Samsung SmartThings 是一个智能家庭编程平台，密歇根大学和微软研究院的研究人员[18]对其上的 499 个应用和 132 个设备管理器（device handlers）进行了静态代码分析（static code analysis），论文[19]发表在 S&P 2016 上。主要有两点发现，一是，虽然 SmartThings 实现了一个特权分离模型（privilege separation model），但是，有两个固有的设计缺陷（intrinsic design flaws），可导致 APP 越权；二是关于 SmartThings 的事件子系统，设备与 APP 之间通过其进行异步通信，该子系统并未对包含敏感信息（如 lock codes）的事件提供足够的保护。研究人员利用框架设计漏洞实现了四个攻击的概念证明：修改门锁密码，窃取已有的门锁密码，禁用家庭的假期模式，触发一次虚假的火灾告警。

3.4.2 物联网协议的 0Day 漏洞主动挖掘技术

在现代的汽车、工控等物联网行业，各种网络协议被广泛使用，这些网络协议带来了大量的安全问题。很多研究者开始针对工控等系统，特别是具有控制功能的网络协议的安全性展开研究。研究人员在 QCon2016[20] 的议题中提到用网络协议 fuzzing 技术对 0Day 漏洞进行挖掘。

3.4.3 物联网操作系统漏洞挖掘

物联网设备大多使用嵌入式操作系统，嵌入式系统通常内核较小，专用性强，系统精简，高实时性，安全在嵌入式系统中处于较低的位置，随着设备逐渐接入互联网，操作系统的安全性需要重点关注。

2015 年，44CON 伦敦峰会中，研究人员采用了 Fuzzing 框架 Sulley 对 VxWorks 系统的多个协议进行了 Fuzzing，挖掘到一些漏洞，并结合 VxWorks 的 WDB RPC 实现了一个远程调试器，进行了相关调试分析

3.4.4 嵌入式设备安全框架

嵌入式设备众多，而且大多在安全设计方面考虑不足。联网的设备往往存在极大的潜在威胁。作为设备制造商，应在嵌入式设备的设计过程中就将安全框架考虑进入，对嵌入式设备进行安全设计。

Icon Labs[21] 是嵌入式设备安全厂商，提出 Floodgate 安全框架，用于构建安全的嵌入式设备。Floodgate 安全框架模块既可以作为单独的产品使用，也可以集成到已有的嵌入式 Linux 和任何 RTOS 中。

17 http://iot.open.qq.com/、https://open.alink.aliyun.com/、http://iot.baidu.com/
18 https://iotsecurity.eecs.umich.edu/
19 https://iotsecurity.eecs.umich.edu/img/Paper27_CameraReady_SmartThings_Revised_IEEEGen.pdf
20 http://2016.qconbeijing.com/presentation/2954
21 http://www.iconlabs.com/

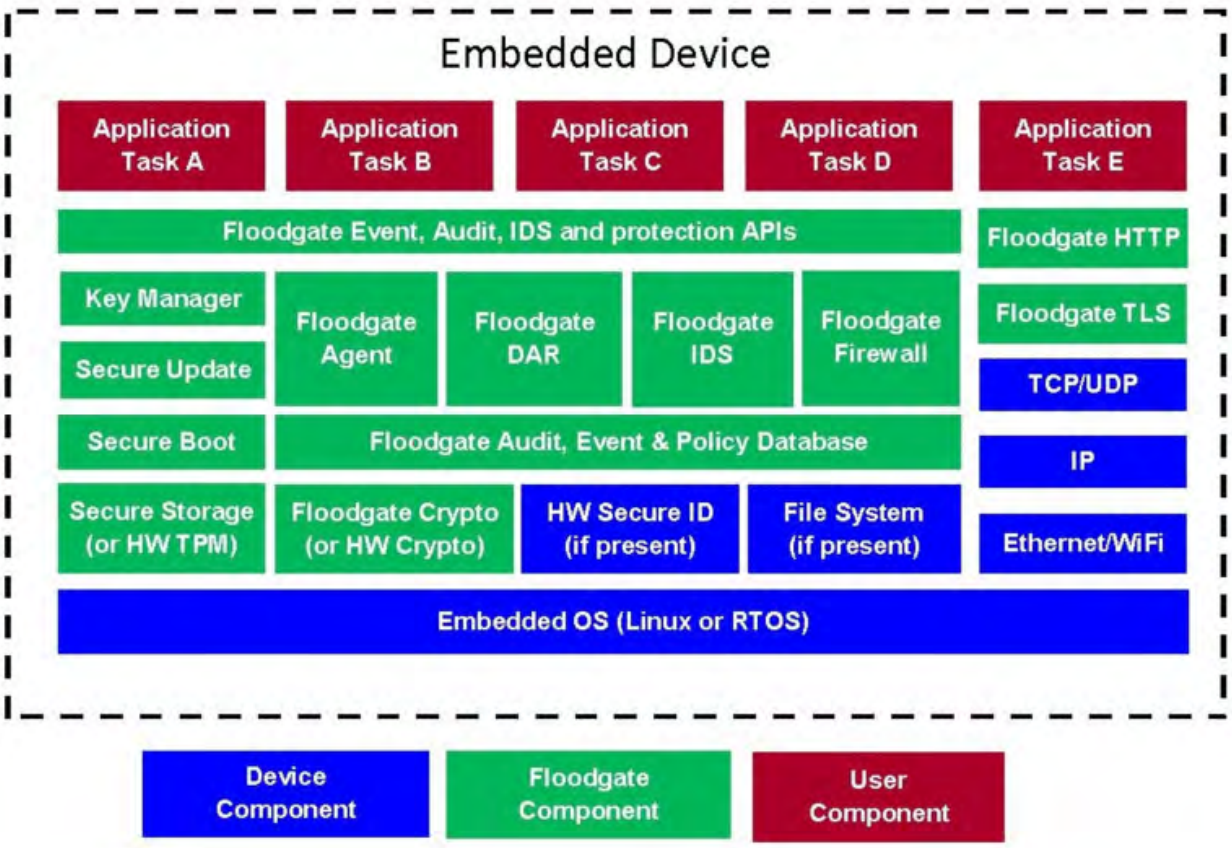


图 3.3 Floodgate 架构

Floodgate Firewall，是一个嵌入式防火墙，提供状态包检测（Stateful Packet Inspection，SPI）、基于规则的过滤和基于门限的过滤来保护嵌入式设备免受来自互联网的威胁。

Floodgate IDS 对嵌入式 Linux 和 RTOS 设备提供保护，其能检测出固件、配置信息和静态数据的改变。

Floodgate Secure Boot 确保只有从 OEM 认证的固件才允许在这台设备上运行。

Floodgate Agent 提供对于嵌入式和物联网设备的态势感知、安全事件报告、命令审计日志和安全策略管理，同时也提供与企业安全管理系统的集成。

四 . 物联网安全公司及产品介绍

4.1 引言

消费行业的市场处于物联网普及的开端，可穿戴设备、智能家庭产品、照明设备和其他的智能设备正在成为主流。商业和公共部门对于物联网的采用在消费市场之后，Verizon 在 2015 年的物联网报告中预测 2011 年到 2020 年之间的企业对企业（Business-to-Business，B2B）的物联网连接每年将以 28% 的速度增长。工业，如制造型、能源、交通和零售已经采用了物联网 initiatives。埃森哲在其 2015 年的工业物联网市场定位报告中预测，到 2030 年，单纯美国的工业物联网将价值 7.1 万亿美元，将支持效率、安全、生产力和 service provisioning 的增强。

全球的多个城市也正在采用物联网，依赖于从数以千计的按地理位置分布的不同类型的传感器捕获的数据，它们正在往智慧城市的道路上发展。在医疗行业，我们可以看到制造商已经开始在设备中加入网络连接性和智能以探索物联网的应用，例如患者床边设备。我们同样可以看到个人和商业之间的物联网能力的互联性正在开始，智能穿戴设备很快就可以搜集数据，然后将其传输给云中的医疗服务提供商。交通行业是另一个令人振奋的行业，车联网已经萌芽，随着无人驾驶汽车的实验，基于物联网的路边设备对于传感数据的收集和分析的能力将变得越来越重要。在能源行业，集成和互联的系统（如现代变电站综合系统、智能电网系统）趋于增加系统的自动化和远程访问能力，以在近乎实时的情况下向大范围的用户传输信息以及控制相关的多个任务，以求精简运作和性能。

本章选取了五家公司，在介绍公司产品的同时，也会对其所关注的行业的需求进行一个介绍。赛门铁克提出了一个通用的物联网安全架构。CUJO 是一家智能家庭领域的安全公司，其主打产品为智能防火墙，在智能设备在家庭中日益普及的今天，以智能防火墙作为切入点非常值得关注。Vidder 的技术基础是软件定义边界（Software Defined Perimeter，SDP），其借助于软件定义网络的思想来做访问控制，实现了认证与实际数据访问的分离。NexDefense 是一家工控安全领域的公司，其主打产品 Sophia 是一个工业网络异常检测系统。Intel 发布了关于解决下一代汽车安全和隐私问题的汽车安全最佳实践的白皮书，提出了一种三层纵深汽车安

全防御体系。

4.2 赛门铁克

由于物联网设备的资源受限，因此并不完全支持传统的安全解决方案。赛门铁克[22]将物联网安全分为四个部分：通信保护、设备保护、设备管理和理解当前的系统。这几个部分可以结合起来组成一个功能强大的、易于部署的安全架构来移除物联网中的大部分的安全威胁，如 APT 和复杂的威胁。白皮书“An Internet of Things Reference Architecture”中对这四部分进行了介绍。

通信保护需要对于设备和远程系统之间的通信进行加密和认证，作为认证机构（CA）的领导者，赛门铁克已经在十亿以上的物联网设备中嵌入了设备证书密钥。

设备保护需要对代码签名以确保所有运行的代码都是经过认证的，以及在运行时防护。运行时防护可以通过基于主机的保护（Host based protections）方法。

设备管理需要提供设备固件安全升级的方法，通常可将 over-the air（OTA）内置在设备中。

理解当前的系统需要对系统进行安全分析以检测出系统中的异常行为。很多已经运行的系统不能轻易被取代，对系统的检测和分析可以作为临时的解决方案进行部署。

下图是赛门铁克对于 PC 时代和物联网时代的安全做法的对比。

图 4.1 赛门铁克对于 PC 时代和物联网时代的安全做法对比

赛门铁克[23]在工控系统安全方面主要有两类解决方案，一是针对操作者如何保护工厂和基础设施的安全，二是针对设备供应商如何在其产品中增加安全性。

赛门铁克利用分析技术和机器学习对 ICS 网络建模以使用户理解自己的网络，从而检测高级威胁。

22 https://www.symantec.com/solutions/internet-of-things
23 https://www.symantec.com/solutions/industrial-control

Symantec Embedded Security: Critical System Protection (SES CSP) 是一个轻量级的安全客户端，通过保护终端和嵌入式设备来保护物联网安全。它在不影响设备性能的情况下向制造商和资产所有者提 供 embedded systems robust signatureless, host-based protection in managed and unmanaged scenarios。由于是基于策略的防护，SES CSP 不需要像杀毒软件那样进行安全内容更新。

赛门铁克对汽车安全领域的分析沿用了上文提出的安全框架，同样分为四部分：

(1) 保护所有通信

(2) 保护各传感器，执行器，微控制器（MCU），以及微处理器

(3) 安全和有效地管理整个车辆通过空中下载（OTA）

(4) 减轻高级威胁

图 4.2 汽车安全需要注意的四个点

赛门铁克 [24] 嵌入式安全：保护关键系统，保护关键单元和大多数汽车的 IVI 系统。保护 OBD-II 接口设备，包括经销商的诊断设备和 UBI 加密狗。设备认证嵌入式安全证书可以用来认证数据。赛门铁克代码签名证书目前支持全系列代码签名的，包括安全启动签名代码。

嵌入式汽车安全分析用来监测 CAN 总线或 FlexRay 总线。这个软件可轻松部署到单板计算机中，包括用于 IVI 的 SBS。为汽车安全启动设计的代码签名，由赛门铁克全球领先的备份证书机构（CA）和代码签名基础设施支持。嵌入式软件保护同样建立在我们的代码签名证书和 CA 服务的基础上，但是做的并不只是代码签名。在签名之前，嵌入式模糊处理和其他形式保护直接进入代码，使汽车制造商代码可以自己保护自己，甚至在有限的 MCU，例如几十年的老 8 位和 16 位器件。全球物联网安全性分析，从数以百万计的汽车中收集数据进行分析，以抵抗高级威胁。总之，不管你们如何保护每个模块，无论做的多么好，你总是需要一个监测和分析框架，以检测最先进的威胁。

赛门铁克嵌入式安全：关键系统防护，可配置在许多这些模块中，加强良好代码的白名单，确保

24 https://www.symantec.com/solutions/automotive

它们只能执行提前批准的代码，并控制这些代码的行为。使用白名单和沙盒作为最小特权保护战略的一部分，只允许已知的代码执行已知的功能。赛门铁克公司嵌入式安全：关键系统保护不仅直接监视应用程序的行为，而且也监视文件，设置，事件和日志，并报告异常行为。特点包括复杂的基于策略的审核和监控；日志整合，便于搜索；先进的事件分析和反应能力。

4.3 CUJO

智能家居（smart home, home automation）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。但是“便利”向来是把双刃剑，在物联网中传输的数据越多，信息暴露的可能性就越大，存在的安全隐患也因此而剧增。

在智能家庭中，一个很流行的应用是 Nest 公司的智能恒温器，该设备可以控制家庭的温度。但是，由于设备搜集家庭中的人的信息，因此，智能恒温器知道家中什么时候有人，他们的日程安排是什么，他们什么时候起床、什么时候睡觉，他们偏好于多少温度。

许多智能电视带有摄像头，即便电视没有打开，入侵智能电视的攻击者可以使用摄像头来监视你和你的家人。由于缺乏安全标准，攻击者甚至会锁定电视从而达到勒索的目的。

许多智能家庭的用户将车库开门器、门锁、摄像头等安防系统连接到网络上，通过手机 APP 可对其进行控制。攻击者一旦攻破这样的系统很明显会带来问题。比如攻击者在你去度假的时候打开房门，或者在午夜打开车库门等等。

攻击者在获取对于智能家庭中的灯光系统的访问后，除了控制家庭中的灯光外，还可以访问家庭的电力，从而可以增加家庭的电力消耗，导致极大的电费账单。

CUJO[25] 是一个智能防火墙，可以使连接到家庭网络的设备远离网络威胁。CUJO 在本地采样网络流量数据，然后发送元数据到云端用于分析。出于保护用户隐私，并没有发送全部的文件和内容到云端。如果检测到威胁或者受怀疑的活动，CUJO 会下发锁定命令（issue a block），在移动 APP 上也会收到相应的通知。

CUJO 扮演用户设备和与它们相连的网络之间的网关的角色，将数据包头发送到云中用于设备行为分析，通过将流量信息与商业威胁情报源进行对比，以确保未授权的 IP 并没有连接到用户的网络中。

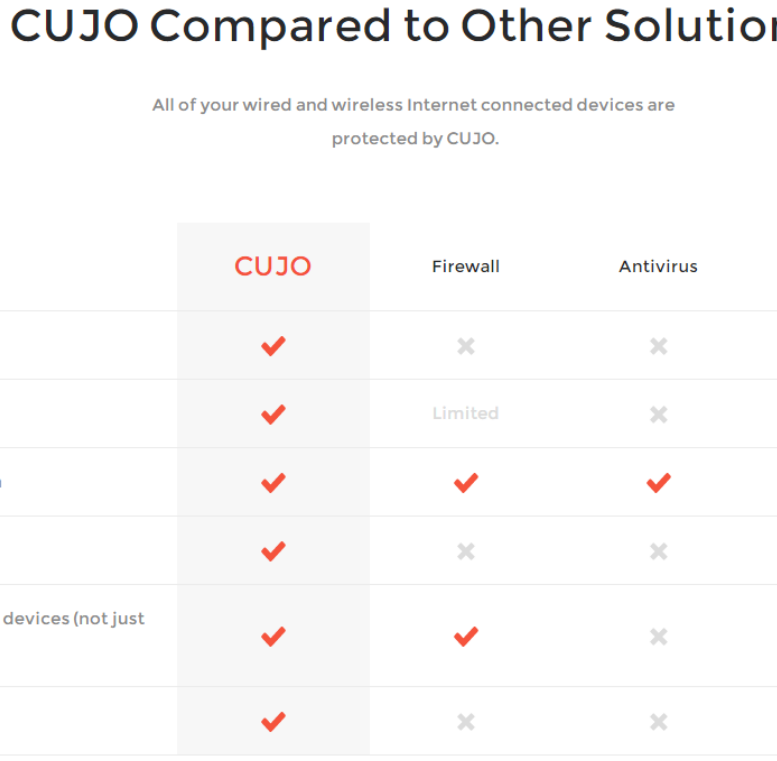
移动 APP 的功能有：

（1）控制和监测用户网络中的所有设备

（2）实时接收威胁通知

（3）控制选定设备的网络访问

25 https://www.getcujo.com/



CUJO Compared to Other Solutions

All of your wired and wireless Internet connected devices are protected by CUJO.

Protection	CUJO	Firewall	Antivirus	Standard Wireless Routers
Hacks	✔	✖	✖	✖
Malware	✔	Limited	✖	✖
Rule Based Protection	✔	✔	✔	✖
Behavior Learning	✔	✖	✖	✖
Secures all connected devices (not just PCs)	✔	✔	✖	✖
Automatic Updates	✔	✖	✖	✖

图 4.3 CUJO 与其它产品功能对比

4.4 Vidder

Cryptzone 通过问卷调研，对于企业网络访问安全有三个发现：

（1）很多企业使用的是过时的方法，在旧的网络安全模型下，缺乏对于限制授权用户和第三方的访问的解决方案。

（2）大部分的信息安全方面的破坏来自于内部威胁（insider threats）。

（3）一些公司并没有经常回顾访问策略，有的甚至已经几年没有这么做了。当策略制定好后，它们不会或者不去自动实施这些安全策略。

因此，我们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的，何时建立连接的，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的威胁的更好的防护。

对于用户的访问控制并不仅仅是在用户访问网络之前对于用户的认证，安全的一个基本方法就是要意识到任何人都可以声称他 / 她是某个人。

Vidder[26] 公司的产品为 PrecisionAccess。PrecisionAccess 使得用户和不同公司、组织、控制区域

26 https://www.vidder.com/

的应用进行安全连接。PrecisionAccess 基于 SDP。PrecisionAccess 基于预认证（pre-authentication）建立连通性。预认证的意思是在提供应用的可见性和连通性之前首先验证用户的可信和权限。它通过三种方式对抗基于网络的攻击：透明 MFA 可以抵抗证书丢失，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。

PrecisionAccess 的架构如下图所示，由三个组件组成，PA 控制器、PA 网关和 PA 客户端。PA 控制器决定了哪些 PA 客户端可以互相连接。控制器有可能将信息转发到外部的认证服务，比如证实、地理定位、身份服务器等。PA 客户端与 PA 控制器进行通信来请求可连接的主机列表。控制器可以在提供信息之前向 PA 网关之内的主机请求信息，如软硬件清单。初始时，PA 网关之内的主机只与 PA 控制器进行通信，只在控制器的请求下与 PA 客户端建立连接。

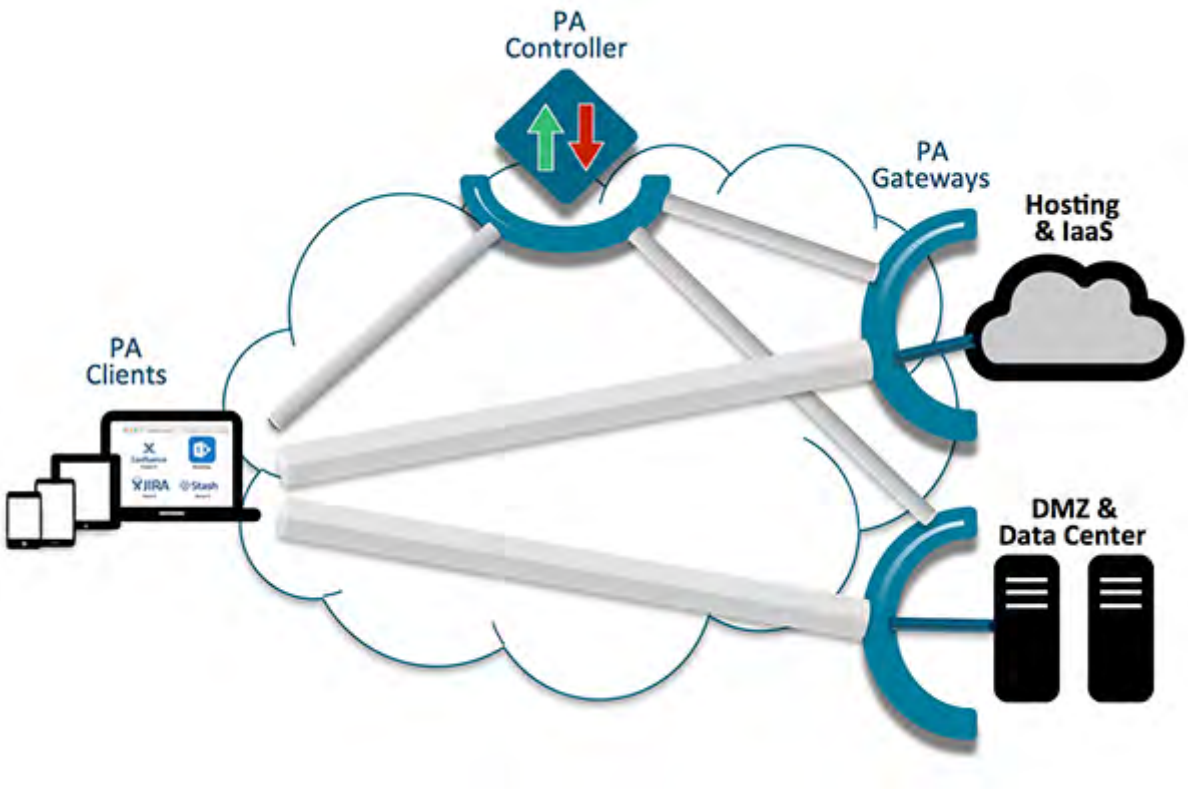


图 4.4 Vidder 架构图

4.5 NexDefense

针对工业控制系统的攻击将导致严重的后果。2010 年 6 月，伊朗布什尔核电站遭到“震网”病毒攻击，1/5 的离心机报废。2014 年，德国的一个钢铁厂，遭受到高级持续性威胁（APT）攻击，攻击者的行为导致工控系统的控制组件和整个生产线被迫停止运转，由于不是正常的关闭炼钢炉，从而给钢厂带来了重大破坏。2014 年，仅仅在美国就发生了 245 起攻击事件。2015 年 12 月，乌克兰电网系统遭受黑客攻击，数百户家庭供电被迫中断。

工业 4.0 驱动制造业、过程控制、基础设施、其他工业控制系统的连通性，对于这些系统的威胁不断上升。

NexDefense[27] 建于 2012 年，致力于实时保护关键基础设施中的系统的完整性，打击复杂的安全威胁。Sophia 是该公司提供的商用安全软件，保持对于威胁的持续洞察和控制，使安全专业人员在不牺牲效率、性能的情况下增加合规性，它能够增加关键基础设施中的工业控制系统的安全性和可靠性。

面向领域：电力、油气、国防。

Sophia 是一个工业网络异常检测系统，由美国能源部、Battelle Energy Alliance 和 Idaho National Laboratory （INL）的网络安全专家协作完成。最初应用于能源和国防组织，用于评估实时威胁和应急协议。它致力于寻找可以降低风险、减少责任（reduce liabilities）和确保自动化和控制系统的完整性的最佳方法和工具。

它可以检测到正常的自动化操作和系统控制操作中的偏差，然后提供预警。Sophia 跟踪网络中的所有设备，知道什么状态是正常的，什么状态是不正常的，对不正常的通信进行报警。

通过对 packet level 数据包级别的监测，来检测网络通信的改变，并对这些改变进行报警。可以提供相应的数据来帮助用户做决定，从而增加 ICS/SCADA 的安全性和可靠性。

它的特点有：

（1）被动（没有对于 ICS/SCADA 的扫描和数据发送）、在线、综合实时通信分析。

（2）在生产环境中可安全使用。

（3）用户在一两天内即可精通。

（4）网络流量 3D 可视化。

（5）对于不在白名单中的非正常 ICS/SCADA 操作进行检测和报警。

（6）支持线下分析。

（7）适用于新的或遗留系统。

（8）支持第三方的离线分析。

4.6 Intel

随着车联网的普及，汽车上的无线技术使用也越来越多， 在给人们的生活带来便利的同时，也带来了很多的安全问题。2015 年爆出黑客可以利用美国通用公司 OnStar 系统的漏洞来远程操纵汽车。可见智能汽车安全问题应该得到我们的高度重视。

现代汽车通信与以往有很大不同，目前出现了三种汽车通信方式：

27 http://www.nexdefense.com/

（1）Car-to-Car Communication （V2C）汽车与汽车之间。汽车之间交互信息，相互提醒路上的障碍物或者其它危害。

（2）Car-to-Infrastructure Communication （V2I），汽车和基础设施之间通过无线进行通信，例如交通信号，各种网络节点。

（3）Car-to-X Communication （V2X），汽车和任意物体之间。泛指任意的信息交换，例如汽车与移动电话，或者互联网应用和云服务。

如此广泛的交流方法意味着黑客可利用的方面非常多，因为任何暴漏在网络中的节点都可能遭受到攻击，或者通过被攻击的节点去连接其他的节点。

另一个问题就是汽车平均十几年的时间才换一次，这导致了行驶在道路上的车辆可能有不同的系统和不同的安全等级，相互通信的组件之间也可能会有不同的安全等级，并且对车辆系统和组件之间宽的兼容性的要求可能会增加新的可以利用的点。一个旧的不安全的智能手机连接到一个新的汽车中可能会导致汽车受到攻击。

同时攻击者也可以通过无线的方式利用汽车中的娱乐信息系统，可以侵入“CAN 总线”，向其他设备发送指令。

总结来说，攻击者攻击一辆汽车，要迈过两道重要的“关卡”[28]：

（1）攻破 Wi-Fi 或蜂窝网络进入汽车系统内部；

（2）绕过系统内部的验证机制，对重要设备的发送指令。

Intel 发布了关于解决下一代汽车安全和隐私问题的汽车安全最佳实践的白皮书[29]，文章中提出了一种三层纵深汽车安全防御体系，将在本小节中作重点介绍。

Intel 白皮书中指出：下一代车辆会使用的系统有：

（1）Advanced driver assistant systems（ADAS）。智能照明控制、自适应巡航控制、车道偏离警示系统和提车辅助。

（2）Advanced fleet management （车队管理）。实时远程信息处理（车联网），司机疲劳驾驶检测和包裹跟踪

（3）Smart transportation。（Vehicle-to-infrastructure）车辆和基础设施通信。例如交通灯控制，避免碰撞等。

（4）Autonomous driving 自动驾驶。实现无人驾驶车辆的零事故死亡率或者撞车率。

指出了下一代车辆最可能被攻击的几个点：

28 http://bluereader.org/article/172957754

29 http://www.mcafee.com/us/resources/white-papers/wp-automotive-security.pdf

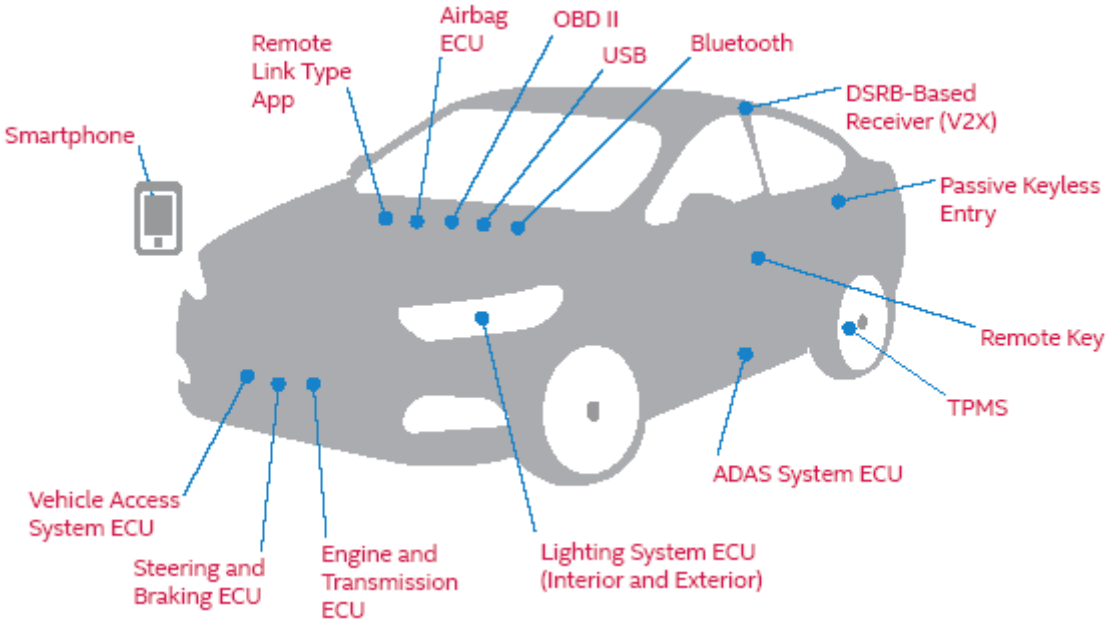


图 4.5 汽车可能被攻击的几个点

Intel 提出的安全纵深防御由三层组成：硬件安全模块、 硬件安全服务和软件安全服务，如图 4.5 所示。

硬件安全保护：它的主要职责是安全启动，将环境带到可信赖的初始环境状态，安全存储和一个受信任的执行环境。

硬件安全服务：基于硬件安全建造，并提供快速加密性能、 永恒不变的设备标识、 消息验证和执行隔离。

软件安全服务：在硬件的基础上通过入侵检测和保护服务（IDPS）、防火墙、黑名单 / 白名单。恶意软件检测、加密服务、生物特征识别，over-the-air 更新和其他功能加强安全性。

下面会简要介绍各个层次的主要技术。

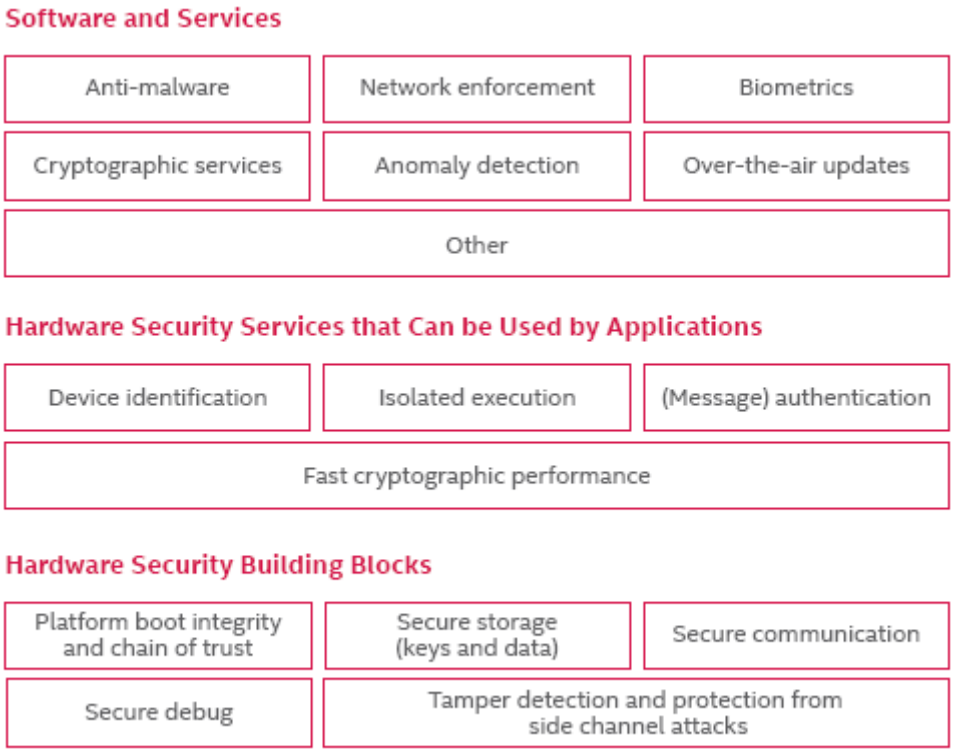


Figure 3. Defense-in-depth building blocks.

图 4.6 汽车安全纵深防御架构

（1）硬件安全

硬件安全系统就像汽车的物理保护系统一样，它可以保护汽车的操作组件免受意外或者故意损害。在计算机安全产业有很多硬件安全技术可以用来保护 ECUs 和总线的安全，这些措施包括：

安全启动和软件证明功能：通过检查数字签名和产品秘钥来检测引导加载程序和关键操作系统是否被篡改。不合法的文件将不能运行。

可信执行技术：如可信任的处理器模块：使用密码技术来为每个被批准组件产生唯一标识符，将启动环境中的成分与一个已知的好的代码进行比较，如果代码不匹配则不允许执行。

篡改保护：加密的加密密钥，知识产权，帐户凭证，在编译时其他有价值的信息，并在一个小的执行窗口中解密，防止逆向工程并对消息进行监测，防止消息篡改。

加密加速：优化硬件减少加密工作负载，提高加密性能，并使对称或公钥加密更容易地广泛地应用到应用程序和通信中

主动内存保护：通过在硬件中嵌入 pointerchecking 减少代码漏洞，来防止缓冲区溢出等情况。

设备标识直接在设备上：使制造商能够知道唯一确定每个设备的身份，确保安全识别和防止未经

批准的设备访问该制造商的网络或系统。这种技术，集成到芯片，也可以加密身份标识保持匿名。

（2）软件安全

汽车网络和控制单元在硬件架构上被隔离保护，使它们很难受到攻击，但攻击者只要花费足够的时间和金钱依然可以闯入这些系统中。此外更多的 ECUs 通过常规协议连接起来增加了汽车可攻击的点。而且在 ECUs 中增加硬件安全能力是很困难的，所以我们需要基于软件的安全保护措施，保护汽车软件技术包括：

安全启动：与硬件协作，以确保加载的软件组件是有效的，以为其他系统提供信任根。

虚拟化：常用的软件和硬件的结合，使得它可以为单一的 ECU 创建一个防御屏障，分隔面向外部的功能和那些驱动车辆的功能，减少了巩固多个系统到一个单一的 ECU 的复杂性。

软件容器：用于单独系统和应用程序隔离，使之更新或替换单独的功能时，不会影响整体操作或镜像功能，从而实现快速故障转移。

认证：通过一个物理钥匙解锁车门并发动汽车不再是足够的，并正在通过软件增强认证能力，因为汽车提供跨越多种功能和配置文件的个性化服务。汽车需要电子密钥，密码和生物识别来管理和授权访问的个人信息，

允许正确的行为：黑客从一个系统跳到另一个系统或者从一个被俘获的组件发送信息给一个正常的组件是很常见的。防止这种网络活动是检测和纠正意外或者恶意威胁的关键。

（3）网络安全

车联网中传输了很多操作和个人信息，包括：位置，导航历史记录，麦克风录音等，为了保护操作安全和用户隐私，保护通信过程中的信息和数据安全十分重要。保护通信的措施主要有：

消息验证：验证消息从被批准的发送源中发送过来，以防欺骗或者重放攻击。

所有系统行为的可预测性：根据预先定义好的征程行为限制网络通信，限制不正常的行为。

防火墙：明确只允许预先批准的系统和传感器之间通信和传递消息，未经批准的和不恰当的信息会被限制，并将这次不合法的尝试发送给安全系统。

（4）云安全服务

车辆安全性是必不可少的，有些额外的安全服务要求实时更新，因此系统需要能够连接到基于云的安全服务，以便于能够及时检测和预防威胁。

与云的安全认证通道：在远程控制，软件更新和其通信过程中，利用硬件辅助的加密实现数数据保护。

车辆活动的远程监控：包括适当的隐私约束以帮助检测异常行为，发现行为异常的车辆，过滤和

删除恶意软件。

威胁情报交换：汽车的经销商、制造商甚至政府机构能够合作起来，能够快速将零日漏洞（zero-day exploit）和恶意软件通知相应的车辆。

OTA：当发现漏洞的时候，可以更新系统，大幅度降低召回成本。

证书管理：联网的车辆组件、车主和司机认证，为用户的配置文件和账户提供安全管理，身份证明以及相关联的加密密钥和服务。证书的安全性是数据隐私的关键。

（5）供应链风险管理

为了保持安全架构的可信和完整性，检测和避免零部件被渗透和污染十分重要，必须要防止攻击者物理地访问车内的硬件。已知的保护供应链的最佳实践包括：

授权分销渠道：用于采购的用来建造和维护车辆的所有硬件和软件。

追踪记录：检测在安全系统中的所有重要部件。

持续的备件和维修部件的供应计划：包括一个长期的部件可用性策略。

（6）数据隐私和匿名。

数据隐私有两个方面 ：个人数据的机密性和不在用户控制范围内的数据泄露。为了保证数据的机密性，数据在车内或者车外存储和传输的时候都需要进行加密处理。对于数据泄露，需要方法防止非法访问。

其它公司所做的工作，大多在这三层体系中得以体现，如：

（1）Argus

该公司提供了一个独特的入侵检测和预防系统（IDPS），利用正在申请专利的深度包检测算法识别恶意攻击，扫描所有车载网中的流量，识别不正常的传输，并且实时对威胁做出回应。同时为管理员们提供一个综合性的网络攻击和不合法的行为的概览，使原始设备制造商识别非授权的对 ECU（电子控制单元）调整和改变行为。

因为威胁是动态的，Argus 研究团队持续更新系统，利用 Argus 安全云服务实时通过 Over-The-Air 更新系统。

这种防御方式属于三层中的软件安全服务层，通过入侵检测和保护服务（IDPS）来增强系统安全性。

（2）Karamba

该公司指出完成一个成功的攻击，黑客首先需要找到一种方式进入汽车的控制器局域网（CAN 总线）。虽然有连接到 CAN 总线有过百的 ECU，只有少数有外部通信接口。这些的 ECU 是进入车内入口。检测、并在这些入口处阻止攻击者，那么攻击者渗透到汽车的网络，并破坏汽车的安全操作的风险会

显著减少。

Karamba 与系统供应商合作，为每个 ECU 定义出厂设置，生成所有 ECU 允许的程序二进制、程序、脚本、网络行为等的白名单，这一政策被嵌入外部连接的 ECU 内，以确保只有明确允许的策略代码和行为会在其上运行。

该防御方法属于硬件安全服务层，将产品集成在硬件中，提供安全服务，增强系统的安全性。

五 . 总结及思考

通过前几章的介绍，我们可以了解到：物联网覆盖的范围较为广泛，物联网安全问题所需要关注的方面也非常多，不仅包含传统网络安全问题，还存在着一些物联网特有的安全问题。

本章中我们总结出了物联网安全研究可以切入的三个领域：工业控制、智能汽车和智能家居，然后又列出了六点需要重点关注的方面，公司可以从这些点作为物联网安全研究的切入点。

5.1 物联网安全可以作为切入点的领域

（1）工控安全

针对工业控制系统的攻击将导致严重的后果。工业 4.0 驱动制造业、过程控制、基础设施、其他工业控制系统的连通性，对于这些系统的威胁不断上升。

（2）智能汽车安全

随着特斯拉汽车的推出，以及苹果、谷歌等互联网巨头新的智能汽车系统的成熟，车联网正在从概念变为现实，但是智能汽车一旦遭受黑客攻击，发生安全问题，可能会造成严重的交通事故，威胁人们的生命安全。

（3）智能家居安全

随着物联网技术的迅速发展，智能家居概念颇为火热，但是如果黑客能轻松的利用网络攻破一些智能家用产品的安全防线， 如：黑客侵占智能设备（恒温控制器、智能 TV、摄像头），可以获取用户隐私信息，带来安全隐患。

5.2 物联网安全研究点

基于调研，我们总结了物联网安全的六个关注点：

（1）物联网安全网关

物联网设备缺乏认证和授权标准，有些甚至没有相关设计，对于连接到公网的设备，这将导致可通过公网直接对其进行访问。另外，也很难保证设备的认证和授权实现没有问题，所有设备都进行完备的认证未必现实（设备的功耗等），可考虑额外加一层认证环节，只有认证通过，才能够对其进行访问。结合大数据分析提供自适应访问控制。

对于智能家居内部设备（如摄像头）的访问，可将访问视为申请，由网关记录并通知网关 APP，由用户在网关 APP 端进行访问授权。

未来物联网网关可以发展成富应用平台，就像当下的手机一样。一是对于用户体验和交互性来说拥有本地接口和数据存储是非常有用的，二是即使与互联网的连接中断，这些应用也需要持续工作。物理网关对于嵌入式设备可以提供有用的安全保护。低功耗操作和受限的软件支持意味着频繁的固件更新代价太高甚至不可能实现。反而，网关可以主动更新软件（高级防火墙）以保护嵌入式设备免受攻击。实现这些特性需要重新思考运行在网关上的操作系统和其机制。

软件定义边界可以被用来隐藏服务器和服务器与设备的交互，从而最大化地保障安全和运行时间。

细粒度访问控制：研究基于属性的访问控制模型，使设备根据其属性按需细粒度访问内部网络的资源；

自适应访问控制：研究安全设备按需编排模型，对于设备的异常行为进行安全防护，限制恶意用户对于物联网设备的访问。

同时，安全网关还可与云端通信，实现对于设备的 OTA 升级，可以定期对内网设备状态进行检测，并将检测结果上传到云端进行分析等等。

但是，也应意识到安全网关的局限性，安全网关更适用于对于固定场所中外部与内部连接之间的防护，如家庭、企业等，对于一些需要移动的设备的安全，如智能手环等，或者内部使用无线通信的环境，则可能需要使用其他的方式来解决。

（2）应用层的物联网安全服务

应用层的物联网安全服务主要包含两个方面，一是大数据分析驱动的安全，二是对于已有的安全能力的集成。

由于感知层的设备性能所限，并不具备分析海量数据的能力，也不具备关联多种数据发现异常的能力，一种自然的思路是在感知层与网络层的连接处提供一个安全网关，安全网关负责采集数据，如流量数据、设备状态等等，这些数据上传到应用层，利用应用层的数据分析能力进行分析，根据分析结果，下发相应指令。

传统的 Web 安全中的安全能力，如 URL 信誉服务、IP 信誉服务等等，同样可以集成到物联网环境中，可作为安全服务模块，由用户自行选择。

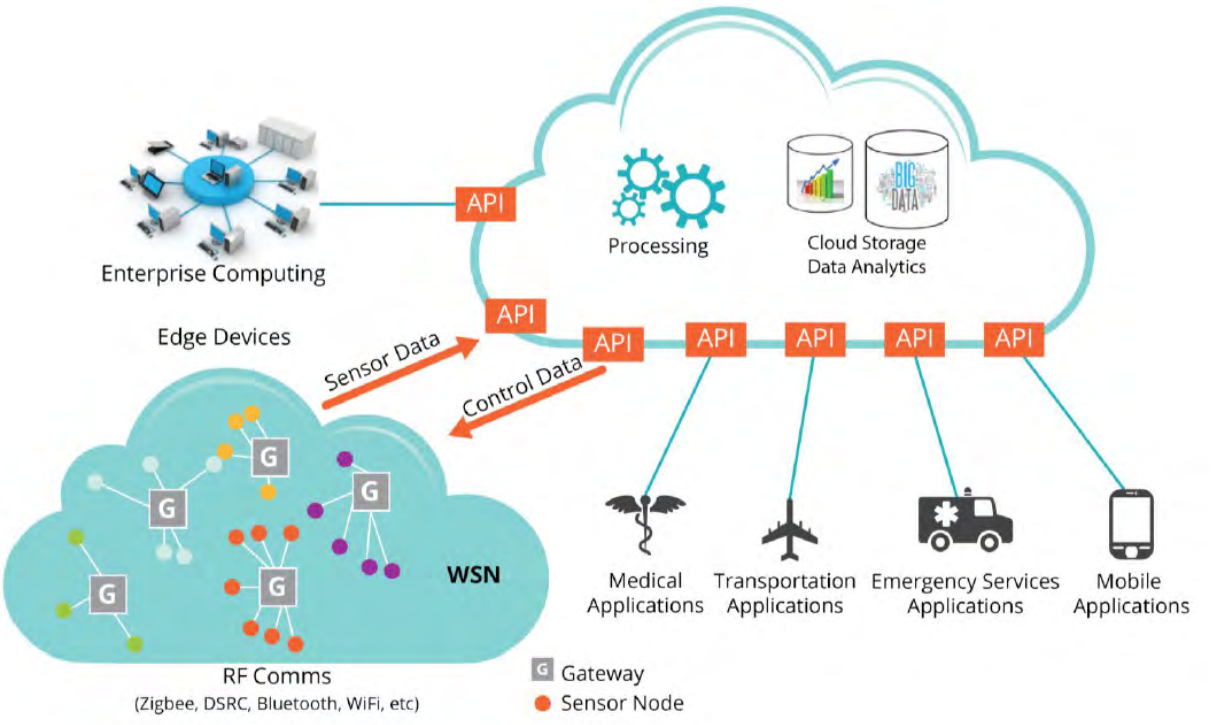


图 5.1 利用云端进行大数据分析

（3）漏洞挖掘研究

物联网漏洞挖掘主要关注两个方面，一个是网络协议的漏洞挖掘，一个是嵌入式操作系统的漏洞挖掘。分别对应网络层和感知层，应用层大多采用云平台，属于云安全的范畴，可应用已有的云安全防护措施。

在现代的汽车、工控等物联网行业，各种网络协议被广泛使用，这些网络协议带来了大量的安全问题。需要利用一些漏洞挖掘技术对物联网中的协议进行漏洞挖掘，先于攻击者发现并及时修补漏洞，有效减少来自黑客的威胁，提升系统的安全性。

物联网设备多使用嵌入式操作系统，如果这些嵌入式操作系统遭受了攻击，将会对整个设备造成很大的影响。对嵌入式操作系统的漏洞挖掘也是一个重要的物联网安全研究方向。

（4）物联网僵尸网络研究

今年最为有名的物联网僵尸网络便是 Mirai 了，它通过感染网络摄像头等物联网设备进行传播，可发动大规模的 DDoS 攻击，它对 Brian Krebs 个人网站和法国网络服务商 OVH 发动 DDoS 攻击，对于美国 Dyn 公司的攻击 Mirai 也贡献了部分流量。

对于物联网僵尸网络的研究包括传播机理、检测、防护和清除方法。

（5）区块链技术

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。

在物联网环境中，所有日常家居物件都能自发、自动地与其它物件、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。

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，未来可能会达到百亿级别，这会对可信第三方造成很大的压力。

区块链系统网络是典型的 P2P 网络，具有分布式异构特征，而物联网天然具备分布式特征，网中的每一个设备都能管理自己在交互作用中的角色、行为和规则，对建立区块链系统的共识机制具有重要的支持作用。[30]

（6）物联网设备安全设计

物联网设备制造商并没有很强的安全背景，也缺乏标准来说明一个产品是否是安全的。很多安全问题来自于不安全的设计。信息安全厂商可以做三点：一是提供安全的开发规范，进行安全开发培训，指导物联网领域的开发人员进行安全开发，提高产品的安全性；二是将安全模块内置于物联网产品中，比如工控领域对于实时性的要求很高，而且一旦部署可能很多年都不会对其进行替换，这是的安全可能更偏重于安全评估和检测，如果将安全模块融入设备的制造过程，将能显著降低安全模块的开销，对设备提供更好的安全防护；三是对出厂设备进行安全检测，及时发现设备中的漏洞并协助厂商进行修复。

30 摘自《中国区块链技术和应用发展白皮书（2016）》

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。

www.nsfocus.com