物联网安全设计指南

意见征集稿

中国云安全与新兴技术安全创新联盟

目录

1 物联网概念和体系架构

1.1 物联网概念

物联网是使用互联网连接的物理世界中使用的非传统计算设备的总称。它包括了从互联网支持的运营技术(如电力和水)到健身追踪器、联网灯泡、医疗设备等等。这些技术越来越多地部署在个人和企业环境中，例如:

a) 企业视频监控和智能安防;

b) 实体物流的数字跟踪;

c) 家庭电表、气表、水表读数自动上报;

d) 为个人提供相关的健康生活的应用。

欧洲网络与信息安全署 （ENISA）将物联网系统定义为“互联传感器和执行器的赛博物理生态系统，可实现智能决策”。

1.2 物联网的体系架构

物联网的体系主要分为感知层、网络层、应用层。平台层为可选，一般与应用层在一起，位于应用层的下面。

感知层包含传感器以及相关的传感网络，完成物理世界的数据采集及数据短距离的传输;

网络层为感知层向应用层的通信管道，如 Wifi、LTE、5G 等;

应用层负责为用户提供具体服务，可视化呈现从感知层获取的数据信息，以及对数据信息的处理，它包含 App 应用、云端服务、计算存储等。除此之外，涉及到物联网的设备如何管理，用户如何管理，数据包如何解析，大数据如何展示等也是物联网模块中非常重要的部分，本文将建构在云端的物联网平台也作为物联网的体系架构中的一层来考虑。

1.3 物联网的标准体系

物联网总体性标准:包括物联网导则、物联网总体架构、物联网业务需求等。

感知层标准体系:主要涉及传感器等各类信息获取设备的电气和数据接口、感知数据模型、描述语言和数据结构的通用技术标准、 RFID 标签和读写器接口和协议标准、特定行业和应用相关的感知层技术标准等。

网络层标准体系:主要涉及物联网网关、短距离无线通信、自组织网络、简化 IPv6 协议、低功耗路由、增强的 M2M (Machine to Machine，机器对机器)无线接入和核心网标准、M2M 模组与平台、网络资源虚拟化标准、异构融合的网络标准等。

应用层标准体系:包括应用层架构、信息智能处理技术、以及行业、公众应用类标准。应用层架构重点是面向对象的服务架构，包括 SOA 体系架构、面向上层业务应用的流程管理、业务流程之间的通信协议、元数据标准以及 SOA 安全架构标准。信息智能处理类技术标准包括云计算、数据存储、数据挖掘、海量智能信息处理和呈现等。

共性关键技术标准体系:包括标识和解析、服务质量(Quality of Service，QoS)、安全、网络管理技术标准。标识和解析标准体系包括编码、解析、认证、加密、隐私保护、管理，以及多标识互通标准。安全标准重点包括安全体系架构、安全协议、支持多种网络融合的认证和加密技术、用户和应用隐私保护、虚拟化和匿名化、面向服务的自适应安全技术标准等。

2 物联网趋势和安全威胁

2.1 物联网发展趋势

5G 网络促使 IoT 持续增长：5G 几乎可以实时收集、传输、管理和分析数据，从而进一步扩展了物联网市场。对于无人机、无人驾驶等对响应时间和传输速度要求很高的领域，5G 更是大有可为，可以发掘物联网的潜能。

物联网与人工智能结合：使用物联网设备与技术收集到的数据增长惊人，很多过去不能感知的数据可以通过物联网技术呈现出来。而传统的计算方式已经无法满足数据处理需求。人工智能可用于自动化地数据分析，并且可以更好地进行图像处理、视频分析，有效地辅助决策。同时，随着人工智能和物联网技术的结合，可以创建出新的应用场景，生产质量管理和优化能源管理就是其中的几个可行的应用。

安全和合规：物联网产品的安全性不容忽视。在医疗健康、安防、金融等处理特别敏感数据的领域，物联网设施的安全将受到更多的关注。各种立法和监管机构纷纷提出更加严格的用户数据保护规定，用户的数据必将受到更严格的监管。这种监管将会给物联网产业带来挑战。如何合法合规地收集、使用、分享和管理用户数据，仍然是一个不断摸索的过程。

边缘计算：主要优势是降低大数据平台需要存储、分析的数据量；本地计算处理可以利用边缘设备算力，提高数据分析时效性的同时减少云端算力需求。同时，边缘计算把大部分数据传输和分析集中在本地，给业务提供了更大的灵活性。制造业往往需要实时决策，物流行业常常不能保证网络连通，无人驾驶则两种情况都存在，对于这些行业边缘计算就特别有帮助。

2.2 物联网所面对的安全威胁和挑战

2.2.1 感知层安全威胁

感知层的资源有限，并且大多部署在无人区，运行在恶劣的环境中，因此很容易受到恶意攻击。感知层面临的安全威胁主要有以下 5 种类型：

a) 干扰：干扰是使正常的通信信息丢失或不可用。感知层设备大多使用无线通信方式，只要在通信范围内，便可以使用干扰设备对通信信号进行干扰，也可以在感知层设备节点中注入病毒（恶意代码或指令等），这有可能使整个感知层网络瘫痪，所有通信信息都变得无效，或者多个设备频繁的同时发送数据，使整个网络瘫痪。

b) 截取：攻击人员使用专用设备获取感知层节点或者簇中的基站、网关或后台系统的重要信息。

c) 篡改：非授权人员没有获得操作感知层节点的能力，但是可以对感知层设备通信的正常数据进行篡改，或者使用非法设备发送大量垃圾数据包到通信系统中，把正常数据淹没在垃圾数据包中，使本来数据处理能力就不高的感知层设备节点无法正常的提供服务。

d) 假冒：假冒就是使用非法设备假冒正常设备，进入到感知层网络中，参与正常通信，获取信息，或者使用假冒的数据包参与网络通信，使正常通信延迟，或诱导正常数据获得敏感信息。

e) 漏洞：近年来黑客利用感知层设备自身漏洞发动网络攻击的事件越来越多，黑客主要通过利用感知层设备软硬件层面和操作系统层面的 0day 漏洞获取感知层权限，进而由点到面达到控制大量感知层设备的目的。

2.2.2 网络层安全威胁

物联网网络层的安全威胁主要来自以下几个方面：

a）病毒蠕虫威胁：随着物联网业务终端的日益智能化，计算能力的增强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，一旦某一个节点的终端被入侵成功，那么其通过网络传播将变的非常容易，病毒、木马或恶意代码在物联网内具有更大传播性，更高的隐蔽性和更强的破坏性，相比单一的通信网络而言更加难以防范；简而言之，病毒、蠕虫是威胁的实现技术手段，网络层的蠕虫、病毒通常其目的是为了进一步渗透获取漏洞利用，进而实现非法权限获取及数据的非法获取、篡改、仿冒等；或单纯的直接发起攻击，如 DoS 等。 因此，对于网络层的威胁总结包含 DoS、窃听、渗透、篡改等；

b）承载网络信息传输安全：物联网的承载网络是一个多网络叠加的开放性网络，随着网络融合加速及网络结构的日益复杂，物联网基于无线或有线链路进行数据传输将面临更大的威胁，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分析；对系统无线链路中传输的业务与信令、控制信息进行篡改，包括插入、修改、删除等，攻击者通过物理级和协议级干扰，伪装成合法网络实体，诱使特定的协议或者业务流程失效；

c）核心网络安全：未来全 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，大多数物联网业务信息要利用互联网传输，移动通信网络和互联网的核心网络具有相对完整的安全保护能力，但由于物联网中业务节点的数量将大大超过以往任何服务网络，并以分布式集群方式存在，在大量数据传输时可能将使承载网络阻塞，产生拒绝服务攻击。另外由于物联网网络应用

的广泛性，不同架构的承载网络需要互联互通，跨网络的安全认证、访问控制和授权管理方面也会面临更大的安全挑战。

2.2.3 应用层安全威胁

物联网应用层主要威胁如下：

a) 身份冒用：由于物联网设备无人值守的特点，这些设备可能被劫持，然后伪造客户端或应用服务器发送数据并执行相关指令。例如针对智能锁，攻击者可伪造用户或管理员进入后台服务器，实现远程开锁；

b) 应用层窃听/篡改：由于物联网通信需要通过异构、多域网络，其安全机制相互独立，因此应用层数据可能被窃听、注入和篡改；

c) 隐私威胁：根据隐私数据的类型，物联网隐私可分为 3 类：一是身份隐私，它关于个人身份、特征、信用状况等；二是数据隐私，是指关于个人的医疗、购物、休闲等过程形成的数据记录；三是位置隐私，是指个人在活动中所出的地点和周围环境信息，例如 GPS 等，物联网时代下的个人隐私越来越受到关注，物联网大量与个人生活息息相关的摄像头、GPS、各类传感器及 RFID 设备连接到网络上，如果得不到保护，个人隐私数据必然赤裸裸的暴露于互联网上；

d) 由于物联网应用层多数位于云端，必然也会面临其他云安全通常的威胁，例如数据泄露、不安全的接口和 API、系统漏洞、账户劫持、恶意内部人员等威胁；

e) 安全意识薄弱：一些企业错误的认为，由于他们的应用跑在云端，保护其应用的安全依靠云平台提供商就可以了，虽然云平台提供商可提供通用性的安全防护措施，但是云端数据备份恢复以及业务自身安全性是用户的主要责任而非云平台提供商的责任。

2.3 物联网安全事件

亚马逊智能音箱发生重大监听事故：超千条用户录音泄露。2018 年 12 月 20 日，德国媒体《c't》报道称，由于亚马逊的人为错误，导致德国一位 Alexa 智能音箱用户接收到了 1700 份的陌生人录音。今年 8 月，这位用户根据《通用数据保护条例》要求亚马逊提供自己的个人活动语音数据时，没想到对方竟然发来了 1700 份陌生人录音。

《c't》听取了其中部分录音发现，仅凭这些信息可以“拼凑”出一个人的生活细节和个人习惯。有些录音还有沐浴的声音。《c't》根据这些信息找到了不幸被泄露隐私的两位用户，其中一位表示震惊和愤怒。

智能家居设备部署在私密的家庭环境中，如果设备存在的漏洞被远程控制，将导致用户隐私完全暴露在攻击者面前。智能家居设备中摄像头的不当配置(缺省密码)与设备固件层面的安全漏洞可能导致摄像头被入侵，进而引发摄像头采集的视频隐私遭到泄露。2017 年 8 月，浙江某地警方破获一个在网上制作和传播家庭摄像头破解入侵软件的犯罪团伙。查获被破解入侵家庭摄像头 IP 近万个，获取大量个人生活影像、照片，甚至个人私密信息。 2017 年 2 月 28 日安全专家 Troy Hunt 曝光互联网填充智能玩具 CloudPets(泰迪熊)的用户数据存储在一个没有任何密码或防火墙防护的公共数据库中，暴露了 200 多万条儿童与父母的录音，以及超过 80 万个帐户的电子邮件地址和密码。

利用设备漏洞控制物联网设备发起流量攻击，可严重影响基础通信网络的正常运行。物联网设备基数大、分布广，且具备一定网络带宽资源，一旦出现漏洞将导致大量设备被控形成僵尸网络，对网络基础设施发起分布式拒绝服务攻击，造成网络堵塞甚至断网瘫痪。2016 年 10 月 21 日，美国域名服务商 Dyn 遭

受到来自数十万网络摄像头、数字录像机设备组成的僵尸网络高达 620G 流量的 DDoS 攻击，导致美国东海岸大面积断网，Twitter、亚马逊、华尔街日报等数百个重要网站无法访问。同年，德国电信遭遇网络攻击，超 90 万台路由器无法联网，断网事故共持续数个小时，导致德国电信无法为用户提供正常网络服务。

3 物联网安全定级建议

3.1 定级依据和标准

本指南所编写的物联网安全定级依据和标准参考了目前业界的主流方法，将物联网场景中受侵害客体分为公民、法人和其他组织的合法权益以及社会秩序、公共利益，受侵害程度分为一般侵害、严重侵害、特别严重侵害。

安全等级与受侵害客体、受侵害程度关系如下表所示。

受侵害的客体	对客体的侵害程度		
	一般损害	严重损害	特别严重损害
公民、法人和其他组织的合法权益	等级一	等级二	等级三
社会秩序、公共利益	等级二	等级三	第四级

表 3-1

物联网场景 CIA（可用性/机密性/完整性）要求不同，本指南根据不同设置的 CIA 和物联网场景的定级参考要求如下表：

可用性	机密性	完整性	等级
H	H	H	4
H	H	L/N	3

H	**L**	**L/N**	**2**
L	**L**	**L/N**	**1**

表 3-2

3.2 物联网场景安全定级建议

每种场景的物联网产品的安全级别不同，厂商可以根据上一小节的物联网安全定级标准来评估本身应该具备的安全级别。

物联网系统和物联网终端应当有不同的定级标准。物联网终端由于功能和部署位置不同，对定级要求不同，应当采取简化的定级和认证手段。一款设备应该当有入网级别的认证，这个认证是设备基础定级认证。当此设备被用于更高保护等级网络中，应该提高安全级别，通过相应的终端级别认证。

比如智能家居产品一般是等级为 1 或者 2，但如果部署此产品的建筑或者建筑里面的用户本身是高安全价值目标，容易被 APT 攻击盯上。使得智能家居产品安全性无法满足新的安全需求，需要提升物联网安全等级。

如用户使用运动手环进行运动，上传运动数据但包含了 GPS 位置，就会造成风险。在 2018 年 4 月，Strava 发布的热图中暴露了美军多个海外军事基地。充分说明了同一款 IoT 设备随着用途而需要不同的安全等级。反之过分提高设备安全等级又会提高准入门槛，不利于物联网产业健康发展。

4 物联网安全架构

4.1 总体安全架构

物联网的安全架构可以根据物联网的架构可分为感知层安全、网络层安全、平台层安全和应用层安全。如下图所示：

图 4-1

4.2 感知层安全

感知层包括物联网感知终端设备，在物联网中主要负责感知外界信息，包括信息采集、捕获数据和识别物体等。感知层的设备终端数量和种类众多，功能从简单到丰富，状态或联网或断开，呈现多源异构性。由于大部分感知终端设备通常功能简单，存储、计算能力较弱，其上部署的安全措施较少，且感知终端设备多部属于无人值守环境中，面临较为复杂的安全威胁。因此感知层终端的安全架构需统筹考虑其计算、通信、存储等资源，在以下方面实现其安全设计：

a) 物理安全：需要保护终端的部署安全以及从物理上对感知设备的篡改，在遭受物理攻击时，确保终端设备在被突破后其身份、认证以及账户信息相关的重要数据不会被攻击者利用；

b) 接入安全：需要确保感知终端在接入时经过严格的标识和认证，防止伪造和假冒；

c) 硬件安全：感知终端设备需要确保身份、认证以及账户信息等重要数据的存储安全；

d) 通信安全：感知终端需采取安全的通信传输协议，确保身份、认证以及其他重要数据在传输过程中不被恶意攻击和泄露；

e) 操作系统安全：感知终端需采取措施确保设备固件完整真实，满足访问控制、日志审计、接口安全、失效保护等安全要求；

4.3 网络层安全

网络层是连接感知层和平台及应用的传输通道，主要包括 WiFI、ZigBee、蓝牙、红外、移动通信网等传输接入网以及以 IPv4/6 为主的核心网络。由于感知层的传输网络多样化，因此网络层需要将多种传输网络进行融合，因此多采取多网络叠加的开放性网络，其通信传输比传统网络更为复杂，协议破解、中间人攻击等威胁十分突出。因此在网络层安全架构设计上需考虑：

a) 通用网络安全：网络层需考虑与终端的相互认证方式，确保终端接入安全，同时具备访问控制等安全措施；

b) 传输安全：网络层需采取加密措施确保通信网络数据的机密性和完整性，防止通信数据发生劫持、重放、篡改和窃听等中间人攻击；

c) 网络攻击防护：网络层需考虑病毒传播、DDoS 等网络攻击行为，确保接入网及核心网的安全可靠；需要通过协议健壮性测试保障开放的协议和端口能抵御畸形报文攻击；

d) 协议融合安全：作为多网络融合的开放性网络，网络层需要考虑异构网

络间信息交换的安全。

4.4 平台层安全

平台层主要提供为感知层终端提供设备管理，数据管理、分析和反馈等服务，也具备数据挖掘、决策等重要功能。平台层融合云计算、大数据等多种先进技术，在进行大规模、分布式、多业务管理时，设计上需考虑：

a) 平台基础环境安全：需关心承载平台层的云计算平台等基础环境的安全，考虑硬件环境、虚拟化、稳定性、漏洞防护等安全问题；

b) 接入安全：需要具有可靠的密钥管理机制，从而对实现并支持用户、设备接入过程中安全传输的能力，并能够阻断异常的接入；

c) 数据安全：需考虑平台所传输和存储的物联网数据完整性、保密性和不可抵赖性；

d) 接口安全：需考虑平台对外提供 API 服务的安全性，确保 API 不被非法访问和非法数据请求，防止通过 API 过度消耗系统资源。

4.5 应用层安全

应用层主要对平台层提供的数据进行分析处理，面向用户实现具体业务功能，需考虑：

a) 身份认证：需考虑应用用户的身份认证，防止身份伪造，确保用户仅访问其授权的资源；

b) 访问控制：需考虑用户与系统资源的访问策略，严格限制用户访问的系统权限；

c) WEB 应用攻击防护：需考虑 WEB 应用可能面临的 SQL 注入、跨站脚本、信息泄露、恶意代码等攻击行为；

d) APP 安全：需综合考虑 APP 面临的移动安全问题，包括不安全传输、信息泄露、反编译等攻击行为。

5 物联网生命周期安全防护

5.1 云端应用生命周期防护

安全漏洞本质上是软件质量缺陷，安全性是软件质量的重要组成部分。在国际上，有很多软件开发质量方面的最佳实践，SDL security development lifecycle（安全开发生命周期），是微软提出的从安全角度指导软件开发过程的管理模式。SDL 是一个安全保证的过程，其重点是软件开发，它在开发的所有阶段都引入了安全和隐私的原则。

本节针对云端应用系统应当遵循的应用开发安全标准进行了规范性说明，旨在指导应用系统设计人员、代码开发人员和安全检查管理人员进行应用安全开发的安全配置，以提高应用系统的安全防护能力。

只有将安全融入到整个应用开发流程中，执行到位，才能保障产品的安全能力及落地。一个在完整的应用安全开发过程，应该包括如下几个阶段：

a) 安全需求

b) 安全设计

c) 安全开发

d) 安全测试

e) 安全交付和维护

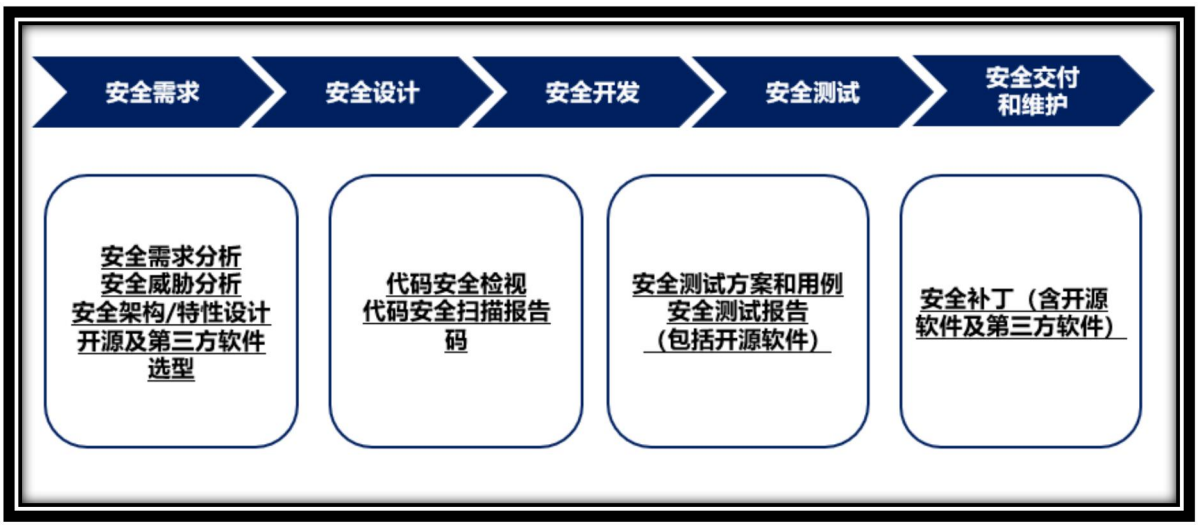

图 5-1

在这几个阶段中，应注重落实安全需求分析、威胁分析、安全设计活动，使产品在设计阶段落实相关安全需求，保障产品的安全能力。

5.2 终端生命周期防护

一个物联网设备的完整生命周期包括了设计、开发、测试、投产、运营几个阶段。物联网设备的研发需求通常来自业务的自动化或业务数据的采集，往往设计生产后会在很长一段时间内处于无人维护的环境，导致物联网设备容易被非使用人员接触甚至破坏，也很难通过巡检的方式来保障安全。所以要保持物联网设备的相对安全，就需要从设计阶段开始尽量针对设备投产后面临的威胁进行针对性的安全机制引入。

5.2.1 开发安全

在设备的设计和开发阶段主要需要解决以下几个安全问题：

a) 硬件安全

硬件安全包括模组选型、防拆卸设计及能量攻击防护。

- 模组选型，从安全上需要避免选择已知具有硬件漏洞的模组，避免选择模组固件具有已知漏洞的模组版本。

- 防拆卸设计，在物理设计上需要尽量增加通过物理方式接触硬件调试接口，包括直接对关键模组、芯片通过飞线等方式进行物理破解的难度。对关键重要的物联网设备，如果条件允许，可以考虑增加物理拆卸感知上报的机制。

b) 代码及供应链安全

- 代码安全，主要指对物联网设备进行业务开发时开发人员的代码规范和通过代码检查工具对编写完成的代码进行静态、动态的检查，尽早发现代码层面的缺陷、漏洞。

- 软件供应链安全，开发人员在进行业务开发过程中为了节省开发时间、提高效率会引入一些开源或成熟的软件包、资源库等。为了避免引入的软件包或资源库存在安全漏洞，需要在开发过程中使用相关的安全检查工具对代码引入的软件包、资源库进行定期检查。

5.2.2 设备安全

a) 安全启动

在设备启动至业务流程执行过程，需要确保执行环境的安全：

- 具备通过难以篡改的信任根对固件进行完整性验证。
- 启动代码自身需要具备完整性校验。
- 业务关键流程和重要数据需要采用加密方式存储在专用安全存储区。
- 设备上需要具备独立安全运行空间，确保关键进程难以被篡改。

b) 设备状态监控

设备投产使用过程中，需要对关键信息进行采集并上报：

- 设备存活状态。物联网设备应当具备定期对管理平台报活的机制。
- 设备启停事件。物联网设备启动停止事件对于非法移动或仿冒的判断属

重要信息，应当上报管理平台。

- 设备网络异常事件。如设备网络地址变更或活跃网络接口数量变更。
- 传感器状态。对于终端连接的传感器，设计时应当考虑传感器状态判断，并在应用或系统层面对传感器状态进行上报。
- 设备拆卸告警。对于设计了防拆告警的终端设备，此类事件信息应当作为重要告警上报。
- 用户登录。在系统层面，用户登录往往意味着此时操作人员已经获取了系统权限，已经超出了应用访问的层面。
- 进程启停。对于高级设备而言，系统中运行了哪些进程，以及各进程的启动、停止的生命周期可以准确的还原系统上某一时间段内的行为，对于威胁分析以及安全事件溯源分析十分有用。条件允许的话应当对进程的调用关系同样进行采集、上报。
- 系统对外提供的服务以及对外开放的端口。
- 系统关键设置被改变。
- 设备网络访问。设备上对网络访问进行采集、上报，可以使得管理平台结合网络流量威胁分析时可以快速发现威胁并且进行准确定位。对于在网络中横向渗透的威胁行为具有很好的追踪溯源效果。

c) 安全防护

设备安全防护主要指针对物理接触或远程入侵等手段的一些防护措施：

- 侧信道攻击防护。对于非接触式能量或电磁攻击，设备的关键芯片或重要电路部分需要具备一定的电磁屏蔽措施。
- 物理调试接口防护。开发完成后两场设备应当屏蔽 JTAG 等硬件调试端

口，或设计特殊访问方式，防止固件被逆向。

- 物理外设接口防护。设备投产后应当确保除业务必须的外设接口外的其他接口处于禁用状态。

- 系统漏洞修补。对于运行通用操作系统（如标准 Linux、标准 Android）的高性能物联网设备，通常因完整固件较大整体分发对于流量占用巨大，故需具备对系统漏洞及运行在设备上的特定程序进行打补丁方式修复的能力。

- 固件更新安全通道。对于固件分发通道，应当至少采用 HTTPS 等加密传输的方式对传输内容进行加密。高性能设备可以通过专用防护软件增强对终端 DNS 劫持、中间人劫持等攻击手段的检测与防御机制。

- 固件更新防护。远程更新固件时需要对固件来源及完整性校验的机制。固件更新失败时应当上报，并且尽可能保持业务可用的同时具备拒绝刷入非法固件的机制（如只允许刷入与固件更新前具有同样完整性校验特征码的特定版本固件）。

- 应用升级防护。需要具备对需升级应用进行来源校验和完整性校验。升级过程需要用户授权且升级失败具备将应用回滚至升级前状态的能力，同时将升级相关日志上报。

- 恶意行为上报。可以对设备应用的异常行为或经过检测确认为恶意行为的事件进行上报。如可以进一步响应处置更佳。

5.2.3 安全运维

物联网网络环境复杂，海量设备离散部署、网络异构、设备碎片化等特点，对设备的集中管理、数据分析和威胁发现都是挑战。为确保设备生命周期内的可安全可控应当针对安全运维做好以下几点：

a) 设备安全信息采集能力。设备端关键状态及行为信息是做好安全大数据分析的重要基础，设备端需要采集上报的相关信息内容请参考设备安全 2、3 两节内容。

b) 海量大数据分层处理集中分析的能力。物联网设备数量巨大，传统的集中式数据处理分析不光对大数据处理平台形成技术压力，同时增大了系统对于安全事件的发现-响应闭环时间导致数据时效性差，威胁处置不及时的问题。利用机器学习、人工智能、区块链和边缘计算等新技术将海量数据的处理分层化，将威胁发现与处置能力边缘化，有助于解决以上问题。

c) 安全能力边缘化的安全架构。安全能力边缘化可以缩短安全响应闭环，提高数据时效性和威胁识别准确率。故此，对于高性能设备，可以通过软、硬件的方式预制安全模块，对于 NB 等低性能设备建议提高接入侧设备安全能力。

d) 动态直观的安全可视化平台。安全运维人员对于海量设备、海量日志的分析已经不可能再像传统安全一样简单的通过人工对全网设备重要日志进行筛选、过滤来发现威胁。结合大数据和威胁情报的自动化、协同化的机制结合物联网设备业务需求建模后通过多种安全维度以直观可视化的方式对物联网安全态势的展示可以极大的满足安全运维人员的需求。

e) 情报驱动的安全协同通道。威胁情报作为大数据时代重要的安全信息交换手段，实现了人、机协同，提高了安全事件响应效率。所以物联网安全运维平台需要具备与安全服务商提供的威胁情报同步的能力。

f) 贯穿始终的专业服务。运维是永远不会 100%被自动化的服务，运维的成果取决于运维人员与相关工具的协同。建立专业的安全运维团队或聘请专业人员提供服务将是物联网时代安全运维的新需求。

6 物联网身份标识和认证

物联网设备的身份标识和认证对物联网安全具有重要意义。在物联网应用系统和网络接入都需要依赖身份标识和身份鉴别，确保正确的设备接入正确的网络，传输正确的数据，执行正确的动作。

各类感知终端和接入设备在接入网络时应具备唯一标识；设备必须能够证明其唯一身份，并运用这一身份与服务器或其他设备之间建立安全通讯。

网络和应用对各类感知终端接入行为具有身份鉴别机制；在终端接入网络时，终端需要对网络进行认证，网络也需要对终端接入认证。终端向应用系统发送数据或接受数据或指令时，需要对应用系统进行认证，应用系统也需要对终端合法性进行验证。

6.1 终端身份标识

身份标识需要在设备生命周期的起始阶段就建立，譬如工厂制造阶段，就与安全厂商进行合作，通过注册将设备的唯一标识和相关密钥灌入到设备中的安全存储区域。

应建立规则以识别使用相同身份凭证进行身份验证的设备，这可能表明存在安全隐患，应进行检测并修复问题。

6.2 身份认证

使用密码认证的，应审计和识别包含默认密码的设备，在部署时立即改变这些密码(最好是在连接到网络之前)。识别与其他设备共享密码的设备并立即改变这些密码。识别共享远程访问密钥的设备并根据设备唯一身份凭据进行密码更新。

使用数字证书进行身份认证的，应建立管理设备证书的安全更新和信任锚的流程并获取相关技术，尽可能选择自动更新方式。限制授权管理员访问来更新设

备信任锚。建立证书管理政策。定义在提供证书前验证设备身份的最低要求(登记)。设备识别验证应该基于(a)现场审查,或(b)在已有的关键材料基础上(例如由制造商)自动提供。建立包括证书更新在内的自动化证书流程。证书的寿命不超过三年。制造商嵌入的设备身份证书没有过期时间，但这些证书只能用于建立短期证书。

身份认证包括终端身份认证、感知层网关身份认证以及通信网接入系统身份认证。

6.2.1 终端身份认证

a) 身份认证鉴别机制

终端应能向接入网络证明其网络身份，至少支持如下身份认证机制之一，建议采用推荐的身份认证机制。

- 基于网络身份标识的认证
- 基于 MAC 地址的认证
- 基于对称密码机制的认证（推荐）
- 基于非对称密码机制的认证（推荐）

b) 认证失败处理机制

终端应具备设置鉴权失败告警产生的频度门限以及相应的处理机制，如当超过设定的认证失败次数后终止访问，并在一定的安全事件间隔后才能恢复。

c) 操作系统用户身份认证

- 具有操作系统的终端，应提供对终端的操作系统用户的身份认证机制。使用用户名和口令认证时，口令应由字母、数字及特殊字符组成，且长度不小于 8 位。

- 具有执行能力的终端应能鉴别下达执行指令者的身份。

d) 访问控制

- 具有操作系统的终端应能控制操作系统用户的访问权限。
- 具有操作系统的终端，操作系统用户应仅被赋予完成任务所需的最小权限。
- 终端应能控制数据的本地或远程访问。
- 终端应提供安全措施控制对其的远程配置。
- 终端系统访问控制范围应覆盖所有主体、客体以及他们之间的操作。
- 禁用闲置的通信接口，包括但不限制：USB 口、UART 串口、SPI、RS-485、以太网口、光纤口、CAN、ModBus 等。
- 必要的时候可以增加其他的限制，例如地理围栏系统和时间限制系统。

e) 物联网设备使用 IEEE 1609.2 证书时，可以将身份验证凭据绑定到授权使用这些凭据的特定应用程序。 如果使用 IEEE 1609.2 证书，请指定应用程序唯一标识符，并在 IEEE 1609.2 SSP / PSID 位中使用。 当进行授权决策时验证 SSP / PSID 字段。

f) 禁用未认证的蓝牙进行配对（例如，直接连接）。

6.2.2 感知层网关身份认证

感知层网关的身份认证，包括感知层网关南向对接终端所需要支持的身份认证机制以及本身的身份认证机制。

（一）南向对接终端所需要支持的身份认证机制

a) 终端接入认证

- 保证对感知终端标识的感知层网关生命周期内的唯一性。

- 提供对终端身份认证的机制。
- 对基于口令的鉴别，提供检测已失效的或复制的口令数据重放的安全机制。
- 提供防暴力破解机制，如当超过设定的认证失败次数后终止终端的访问，并在一定的安全事件间隔后才能恢复。

b) 网络访问控制

- 支持访问控制表（ACL）等访问控制策略，防止资源被非法访问和非法使用。
- 控制相同网络内部的相互访问。
- 控制不同网络之间的跨网访问。
- 访问控制的覆盖范围应扩展到访问相关的主体、客体以及他们之间的操作。
- 支持黑名单、白名单机制。
- 能够控制终端访问数量。

（二）感知层网关本身所需要具备的身份认证机制

a) 感知层网关身份认证

b) 感知层网关用户访问控制

- 控制感知层网关用户的访问权限，并避免权限扩散。
- 仅赋予感知层网关完成任务所需要的最小权限。
- 控制数据的本地或远程访问。
- 提供安全措施对感知层网关进行远程配置。
- 控制范围应覆盖所有主体、客体以及他们之间的操作。

6.2.3 通信网接入系统身份认证

本章节主要关注通信网接入系统的身份认证，包括通信网接入系统本身的身份认证机制以及感知层接入实体的身份认证机制。

（一）通信网接入系统身份认证机制

a) 接入实体接入认证（含终端以及感知层网关，至少两种方式）

- 基于接入实体标识和接入口令的单向认证
- 基于预共享密钥的单向或双向认证
- 基于公钥基础设施的接入认证

b) 认证失败处理机制

- 当认证应答超过规定时限时，接入系统应能终止与待接入的接入实体之间的当前会话。
- 提供防暴力破解机制，在经过一定次数的认证失败以后，接入系统应能终止由该接入实体发起的建立会话的尝试，并在一定的时间间隔后才能允许继续接入。

c) 访问控制

- 通过 ACL 方式控制感知层接入实体对通信网的访问。
- 支持制定和执行访问控制策略的功能，访问控制策略可以是基于 IP 地址及端口、用户/用户组、读/写等操作、有效时间周期、敏感标记等的两种及以上构成的组合。
- 支持白名单，限制接入实体对通信网的访问。

（二）感知层接入实体身份认证机制

a) 接入实体认证支持功能

- 基于接入实体标识和接入口令的单向认证
- 基于预共享密钥的单向或双向认证（预共享密钥，是物联网实体设备之间进行保密通信的初始密钥）
- 基于公钥基础设施的接入认证
- 提供实体标识、接入口令等的存储以及管理功能

b) 接入实体访问控制

- 提供 ACL 列表实现访问控制。
- 支持基于接入实体用户/用户组的访问控制，并部署用户访问控制策略。

6.3 密钥管理

密钥管理是物联网安全非常重要的一环。应建立物联网系统的密钥管理流程，至少包括密钥生成、密钥派生、密钥建立/传输、密钥存储、密钥生命期和密钥归零/销毁。假设设备有足够的熵随机源，只要有可能，密钥应该在设备上生成。如果使用中央密钥生成和分发则需要有安全的传输机制用于传递密钥材料(包括以带外方式传递)。

对于传统网络，如互联网和移动通信网络，终端的差异性不大，并且对计算资源限制不大，因此选择的密钥管理方案较多。但对于物联网网络而言，终端硬件存在巨大的差异性，存在大量低功耗嵌入式的产品类型，这就对物联网密钥管理方案提出了更多的挑战。所以物联网密钥管理主要面临两类问题：一是如何匹配物联网终端系统及其协议的多样性。二是如何解决密钥管理层面的问题。以下是密钥管理建议：

a) 密钥生成：物联网平台应具备算法动态生成密钥的能力，并且算法有非常高的安全性。

b) 动态密钥：无论采用对称加密或者非对称加密算法，保证每台物联网终端都有属于自己的唯一密钥。每次建立会话都可以更新密钥、从而在逻辑上形成通信隔离。

c) 加密方式：根据终端应用场景和对资源的敏感程度，提供不同的对称或者非对称加密算法。

d) 密钥存储：密钥可以存储在物联网设备的 FLASH 中，也可以只存放在内存中。安全级别较高的设备可以把密钥存储在 SE 芯片中。

e) 密钥备份：备份保存可以分为三种方式。密钥托管备份、密钥分割备份、密钥共享方式备份。

f) 密钥生命周期：密钥管理系统中，应该具备对终端密钥生命周期管理的能力。

g) 建立策略确保私钥不会跨多个设备或组共享。在密钥派生时尽可能采用前向保密性(如不使用静态机制)。密钥应该存储在一个安全组件(软件或硬件)中，限制未经授权的角色访问密钥。密钥的生命期在可能的情况下不超过三年，理想情况下只有一年。同时可以依据策略通过云端进行自动密钥更新机制(如轮换或派生)。

h) 为物联网设备和服务建立专门的密钥管理用户组用于密钥管理安全配置。

i) 建立安全地引导物联网设备接入网络的流程。优先使用能够零接触的物联网设备，因为这些设备预置了硬件制造商的凭证。零接触配置需要一个可信的、带外过程加载提供的序列号和设备的公钥配置。如果零接触不可用，在网络上部署设备之前建立一个可信的设施登记设备序列号和预加载的身份识别/密钥/证书。所有帐户的注册和更新命令都需要采用加密机制。

7 物联网安全可信

7.1 物联网安全可信体系总体架构

物联网分为感知层、网络层、平台层和应用层，构建物联网安全可信体系需重点解决边缘侧及应用层安全可信，平台层归属于传统网络范畴故本指南不对相关要求进行说明。

通过对感知层设备构建本地安全可信，结合设备入网身份认证、入网权限的分配、设备入网的管控实现感知层设备的可信接入；通过密钥管理、设备管理对通过安全测评的设备进行全网唯一标识管理，结合通讯技术、密码技术等对数据进行存储、传输的安全可信保障；结合安全测评和固件安全分发实现物联网系统生命周期的安全管理，完成下图所示的物联网系统安全可信的体系架构建设。

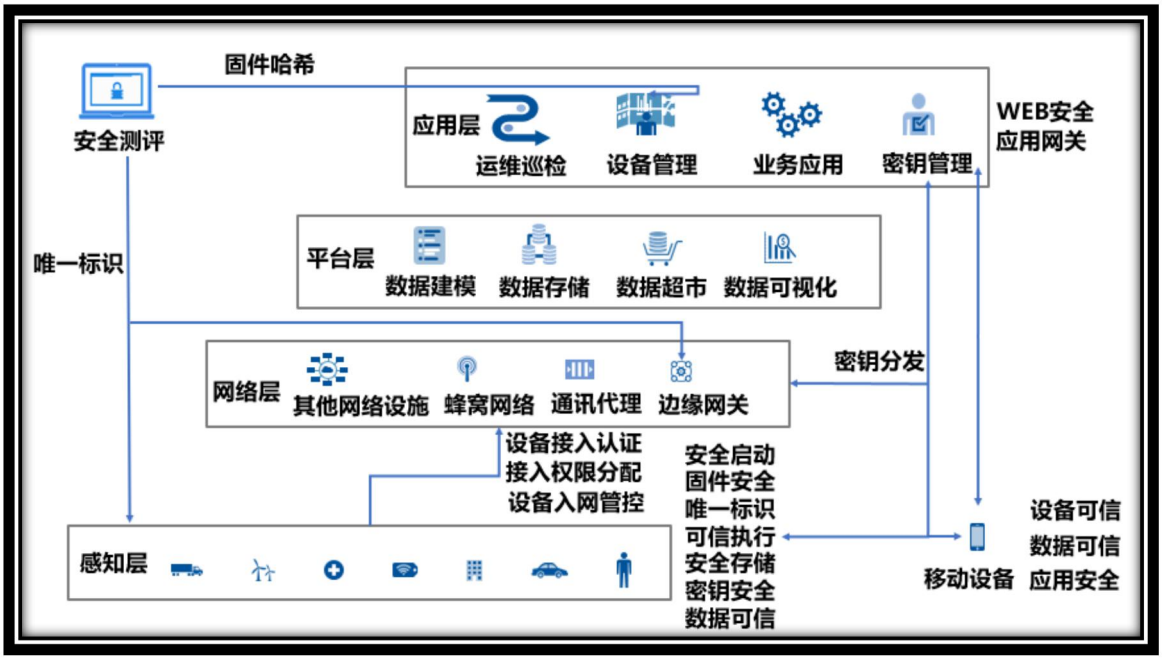

图 7-1 物联网安全可信体系总体架构图

7.2 感知层安全可信

因为物联网的兴起，企业边界正在逐渐瓦解，单纯基于边界的安全防护体系

正在失效。在传统网络安全行业，重点关注南北向的防护策略，通过防火墙、WAF、IPS 等边界安全产品/方案对企业网络进出口进行防护，而忽略感知层东西向的安全。

感知层的安全可信主要解决两方面问题：一、感知层设备面对物联网云平台时双向的身份可信。二、感知层设备自身面对来自边缘侧的安全威胁应做到安全感知。

综合设备身份可信、感知层入侵防护、密钥管理、源码安全、固件安全和敏感信息泄漏几方面因素，将感知层可信划分为设备端可信和数据可信。

7.2.1 设备端可信

设备端的可信主要指设备上的可信环境的构建以及设备入网时自身的接入认证。

物联网设备的端上可信环境的构建包括以下几点：

a) 安全启动：请参考第五章 5.2 节设备安全中相关部分内容。

b) 固件安全：固件安全主要包括运行固件放篡改和固件更新安全。请参考第五章 5.2 节安全防护相关内容。

c) 设备标识：设备应当具备不可篡改的唯一标识，作为入网和与平台交互时的身份识别标志。

d) 可信执行：设备上启动的任何程序都应当经过技术手段验证其合法性，并具有阻断非法进程启动的机制。如，引入 TEE/SE 模块或软件实现的应用白名单等。

7.2.2 数据可信

数据可信应当包括设备本地重要数据的安全存储、对外交互时的传输可信和

感知数据可信。

a）本地数据安全存储。设备上需要本地保存的数据如关键业务数据、设备身份标识、通讯密钥、根密钥等应当保存在加密的安全区域，并默认阻止非可信进程的访问。

b）密钥安全。设备认证、通讯以及其他业务相关需求的密钥应当具备一定的机密性，如随机数熵值不低于 128 位、临时密钥用后销毁、对可靠性要求较高的场景采用一次一密的通讯机制等。

c）感知数据可信。感知数据可信包括感知设备自身对传感器采集到的数据合理范围的预知，例如智能空调感知到零下 273 度的室温，此种属于可确定的感知错误的情况应当触发告警上报机制；对于一些攻击倾向的难以直接发现的感知数据干扰应当从设计角度增加相应的识别能力，如通过超声波对倒车雷达进行同频抵消可以使车辆无法感知障碍物，厂商可以适当的增加不同波段的超声波雷达探头，对攻击进行识别并将异常时的雷达数据上报云端平台进行深入分析；同时业务平台对于感知层上报的数据也应当具备一定的异常检测、告警机制，实现业务应用层的数据准入，避免生产数据受到污染的同时可以快速发现攻击行为。

7.2.3 可信基线与动态鉴权

具备强 M2M 交互的物联网系统内，M2M 的访问应当在设立安全基线（综合 7.2.1、7.2.2 及 7.4.1 中的相关要求和物联网系统业务应用进行安全基线的设计）的前提下实现对不同应用、不同接口、不同子系统访问时的动态鉴权。实现依据设备可信级别对权限的动态赋予，最大程度降低交互风险。

a）设备接入认证。设备入网时应当对设备合法性进行校验，验证设备是否是合法设备、是否被篡改、是否是仿冒设备。

b）设备与其他设备或系统进行交互时应当对设备身份和设备安全基线进行动态判断，依据当时满足安全要求的不同级别对设备入网的权限进行不同授权。

c）设备与控制端之间应当具备双向认证，即控制端通过身份鉴权后接入平台对受管设备进行指令分发等操作后，设备端在收到指令执行前具备对平台指令发送设备的身份及指令时效性进行验证的技术手段。且整个确认过程应当具备防窃听防篡改机制。如，对指令进行加密，且采用一次一密的动态密钥机制。

7.3 网络层安全可信

承载物联网的网络从广义上讲，可以分为蜂窝网络和非蜂窝网络。其中，蜂窝网络包括 2G/3G/4G/5G/NB，非蜂窝网络包括有线网、WiFi、蓝牙、Lora 等。

在蜂窝网络方面，安全可信大部分依赖于运营商。物联网设备通过 SIM 卡接入蜂窝网络，蜂窝核心网网元对设备连接进行可信认证。同时，设备在借助物联网卡进行网络访问时，连接管理平台会对设备和卡的身份可信进行校验，一般通过 IMEI 和卡的 ICCID 做机卡绑定或者 IMEI 白名单。对未通过可信身份认证的应当进行网络隔离（如 VLAN、受限 IP 等）或阻断入网。

非蜂窝网络方面，安全依赖于物联网设备的身份可信认证、边缘网络安全防护、边缘准入管控以及传统网络安全防护。物联网设备入网时边缘接入网关应当依据设备是否通过身份可信认证、设备是否被篡改、设备安全状态是否符合标准等进行入网管控，对于非法设备、被篡改设备及存在严重威胁隐患的设备应当进行网络隔离（如 VLAN、受限 IP 等）或阻断入网。对于具有强 M2M 交互设计的物联网系统，还应当依据 7.2.3 可信基线与动态鉴权中的标准对“阻断设备入网”到“正常访问”的权限区间进行多权限级别的细粒度划分，对设备入网后的

通讯交互进行权限管控。

7.4 应用层安全可信

应用层是物联网和用户的接口，负责向用户提供业务操作入口。应用层处于物联网系统的最顶层，通常包含了业务应用、设备管理、运维巡检等多种应用。随着移动设备的发展和网络技术的进步，为了方便物联网系统的监控管理引入的移动应用和专用移动设备也应并入物联网系统应用层安全考量因素。

移动设备安全可信：参考 7.2 感知层安全可信内容并应用至移动设备。同时由于移动设备存在丢失风险，应当考虑采用开机强密码、生物特征结合的强认证，以及设备丢失后的远程数据擦除等技术的应用。

移动应用安全可信：应当通过对移动应用进行安全加固、可靠分发、双向认证等手段确保移动应用不被篡改，保障应用数据安全可信。

WEB 应用安全可信：对于物联网系统的 WEB 应用，应当具备防跨站攻击、防注入攻击、抗 DDoS 攻击等安全防护。条件允许的还应当考虑应用网关，对应用数据进行可靠校验以及过滤，最大可能的确保数据的安全可信。

此外，为保障设备全生命周期应当对设备投产、换代以及新版本固件先进行安全测评，确保安全达标后对设备分配防篡改的唯一识别码并上线；对新版本固件通过双向加密通道分发固件哈希后再将硬件发布至 OTA 通道。

8 网络传输保护

网络传输过程中，受到的威胁主要有被窃取、被修改、被重放、被拦截等，必须采用相应的措施保障网络传输的安全。

网络传输安全具体是指通过安全技术或方案为物联网传输层提供安全保障以及安全性支持，为防范在传输过程信息被第三方恶意截获、监控、分析、重放、篡改等。

网络传输安全需要采用端到端保护原则，确保在中间人无法恶意插入。数据传输应采用加密，即便数据被接触也可以在生命周期内保障安全，网络应采用隔离等手段，减少被截获、篡改的风险。数据应采用完整性机制，在数据被篡改能及时发现，并采用时间戳和序列号方式，检测拦截，避免重放等。

8.1 端到端安全传输原则

物联网传输安全框架采用端到端原则（end-to-end principle），即通信中的两端主机，其安全性不依赖其通信实际经过的物理路线的安全性，将连接的特性与功能放在网络边缘设备上而非核心网中。物联网边缘设备包括物联网终端设备和物联网应用层的各设备实体，在数据传输中位于数据最开始发送和最终处理的设备。

物联网系统的端到端数据安全传输应遵循以下原则：

- 建立数据传输的双方应采用合适的认证机制，确保端点可信；
- 物联网边缘设备应尽可能进行安全的加密/解密、签名/验证等密码功能；
- 控制数据与业务数据分离；
- 传输安全应尽量不依赖来于原有的通信网络安全框架；
- 在第一条未能满足的情况下，物联网系统中完成安全传输功能的主体应

尽量接近物联网系统的边缘；

- 系统应根据物联网安全等级划分规则选择合适强度的加解密或完整性方案；高等级系统需要采用数字证书认证和加密；
- 数据的端到端安全传输原则保障物联网系统中数据的发送节点到接收节点间实现安全传输，但是此设计应不影响中间节点中对数据进行鉴权、验证和过滤。

8.2 传输协议保护

物联网是互联网的延伸，但在物联网应用层就引入了 MQTT、CoAP 等通信协议，这些协议的安全性关系到物联网的安全性。

a) MQTT 协议安全防护建议：

- 在网络层可以通过物理专线、VPN 等方式提高网络传输的安全性。同时可以采用 TLS 协议进行数据加密，防止中间人劫持、重放攻击等。在低功耗设备上可以考虑轻量级对称加密的方式对数据进行加密，采用数字签名的方式保证数据传输的完整性。
- 终端与云端进行身份验证时，可以采用自有协议的方式加以校验。终端如果也采用证书的方式校验身份，成本过大。
- 在应用层可以使用客户标识以及用户名密码，来验证设备。
- 应注意权限管理问题，订阅发布机制做好用户权限，如禁止通配符的使用。
- 基于 MQTT 做 OTA 升级，应具备检测升级过程中完整性的能力，防止中间被篡改或植入恶意代码。应具备对升级源地址校验的能力，防止固件来源非法。

➢ 云端基于 MQTT 具备检测异常行为的能力，如重复的连接请求、连接的异常终止、发送无法传达的消息。

b) CoAP 协议安全防护建议：

➢ CoAP 网络层基于 UDP 协议，通信过程中会出现丢包现象，应设置丢包重传机制。同时对于用户根据具体的需求判断使用场景，以提高效率。

➢ 在网络层可以采用 DTLS 协议进行数据加密，但需考虑对 DTLS 进行精简。防止中间人劫持、重放攻击等。在低功耗设备上可以考虑轻量级对称加密的方式对数据进行加密，采用数字签名的方式保证数据传输的完整性。

➢ 可以业务数据进行序列化，增加安全性的同时，提高数据处理效率。

➢ OTA 升级，应具备检测升级过程中完整性的能力，防止中间被篡改或植入恶意代码。应具备对升级源地址校验的能力，防止固件来源非法。

8.3 传输加密技术

在杜绝明文传输的基础上，进一步加强数据过滤、认证等加密操作，确保传送数据的正确性。同时， 还可进行设备指纹、时间戳、身份验证、消息完整性等多维度校验， 最大程度保证数据传输的安全性。

物联网系统的传输加密应遵循以下原则：

a) 选择占用系统资源少或轻型的加密算法来控制智能硬件设备的功耗及流量成本，常用的是 AES 加密技术、SSL/TLS 加密技术；

b) 加强数据过滤、认证等加密操作，确保传送数据的正确性；

c) 进行设备指纹、时间戳、身份验证、消息完整性等多维度校验，最大程度保证数据传输的安全性；

d) 应采用经过市场检验公开的合规加密算法，并采用合适的强度，保障生

命周期内安全性。

e) 加密密钥应采用合适的方式进行协商或更换。

8.4 传输数据完整性

物联网系统的传输数据完整性应遵循以下原则：

a) 选择安全的校验机制来实现物联网传输过程中的完整性校验，最大范围内防止传输过程中数据被篡改或者重放，确保传输数据安全。

b) 应采用业界公认的安全算法实现传输过程中的完整性校验机制，确保校验机制的可靠性。

c) 选择占用系统资源少或轻量性的算法来实现网络传输数据完整性校验，常用的是 HMAC-sha256 技术；

d) 考虑在全局和每个客户端上限制到每个终端到服务器的流量，明确消息尺寸，以限制攻击者通过发送大消息使系统过载的能力,保证传输的可用性。

9 近场通信安全

9.1 近场无线射频通信技术概述

近场射频通信主要是通过一套通信协议，使得电子设备间能够在短距离之内（10m）进行通信。这些电子设备在通信过程中主要涉及的近场射频技术有：

a) 射频识别技术（RFID）

b) 近场通信技术（NFC）

c) 无线遥控技术

以上技术在整个近距离的传输过程中经过信号调制、编码、传输、解码的过程。另外，在近场射频技术中，RFID 指通讯频率从低频、高频、甚高频到微波的通讯，包含了 NFC 的范围。NFC 是 RFID 的一种实现。

9.2 RFID 无线射频安全分析

9.2.1 RFID 安全威胁

目前，RFID 空中接口面临的主要威胁分为恶意搜集信息式威胁、伪装式威胁及拒绝服务威胁三大类。其中，恶意搜集信息式威胁主要包括窃听、嗅探、数据篡改、跟踪、物理攻击等，其主要特点是非法用户远距离监听阅读器与标签通信内容，获取其中的有用信息，进而导致标签内部重要数据泄露或被篡改。伪装式威胁主要包括：欺骗、标签伪造与复制、病毒（或恶意代码）攻击、重放等，其主要特点是通过伪造 RFID 标签来欺骗阅读器，进而使得非法用户成为合法用户。拒绝服务威胁主要包含未授权杀死标签、干扰或屏蔽标签等，也包括对标签实施破坏的物理攻击，其主要特点是非法用户通过干扰、屏蔽或杀死标签等手段，阻碍标签与阅读器之间的通信，造成有用信息的丢失。

9.2.2 RFID 安全防御方法

RFID 的安全防御方法主要包括基于访问控制的方法、基于密码技术的方法及二者的结合。

基于访问控制的方法是一种基于物理方法的标签安全机制，这类方法主要有：Kill 命令机制、睡眠机制、法拉第笼、主动干扰、阻塞器标签和可分离的标签等。这些方法主要用于一些低成本的电子标签，因为这类 RFID 标签有严格的成本限制，功能简单，无法提供复杂的应用程序或加密算法保护隐私。

随着芯片技术的进步，比现有标签更加智能并可多次读写的 RFID 标签将会被广泛地应用，这就为解决 RFID 隐私与安全问题提供了更多的可能。基于各种密码技术的方法被应用于 RFID 标签中（包括散列锁协议、随机 Hash 锁协议、供应链 RFID 协议、LCAP 协议、临时 ID 安全协议、重加密安全通信协议等），它直接支持机密性、真实性、完整性和隐私性等；密码技术需要以较强的计算能力为基础，对标签的功耗和成本构成一定的挑战，但作为一种较通用可行的方法，受到了越来越多的关注。

9.3 NFC 近场通信安全分析

近场通信（NFC）是由非接触式射频识别（RFID）演变而来，一种短距高频的无线电技术，以 13.56MHZ 频率运行在二十厘米距离内，其传输速率有 106kb/s，212KB/S 和 424KB/S 三种。

9.3.1 NFC 安全分类

随着互联网终端支付的发展，NFC 技术和 NFC 移动终端及应用因为其安全和便利性，成为运营商、银行、厂商的热捧对象， 由于 NFC 系统和应用可能包含敏感的个人隐私和支付信息等，其安全更加重要。

要做好 NFC 安全从整体上需要做好通信安全、终端安全、系统安全、应用安全这几个层次。

9.3.2 NFC 通信安全

通信安全是 NFC 技术所面临的较传统的安全威胁，主要包括窃听、数据破坏、拒绝服务、中间人攻击等。通过监听数据、篡改数据、重放数据等导致信息中断、信息泄露、金钱损失等严重后果。例如，窃听是指攻击者在 NFC 通信过程中使用特殊设备捕获通信数据的过程，在非支付场景中，攻击者可以利用链路层通信一般不加密，轻易获取 NFC 标签中的内容，此外，虽然 NFC 通信不超过 20cm，但依旧可通过利用定制的特种天线或者增强的信号接收器等扩大近场通信的距离，进而截获通信数据，且窃听者不必完全截获就能够获得还原通信内容，若 NFC 标签存在于身份证、护照等包含个人隐私信息的 IC 卡中，将遭遇窃听导致个人隐私泄露。

为了确保 NFC 技术的通信安全，最有效的方法是建立安全通信，通过秘钥共享和加密传输等手段保证数据的完整性、保密性。安全信道能够防止窃听、数据篡改等保证通信设备之间数据传输的机密性、完整性和真实性。对于中间人攻击建议采用主动通信模式，且主动通信者应该主动监听任何攻击者发出的干扰磁场。

9.3.3 NFC 终端安全

终端安全威胁主要包括终端丢失、设备损坏、SIM 卡克隆、电磁辐射窃听、芯片安全等。终端丢失将可能直接造成用户信息被窃取，这也是终端面临的最大安全风险。此外，设备损坏将导致信息不可用，SIM 卡克隆能够通过复制手机 SIM 卡信息获取用户信息，电磁辐射窃听可获取手机通信的信息，手机芯片可被

植入恶意程序获取用户信息等。

安全元件是存储秘钥、敏感数据、加密运算等操作的安全芯片，在 NFC 的最重要移动支付场景中，它是保障支付安全的核心硬件，目前 SE 的终端有三种类型，但是不管何种方案，在设计过程中均需要考虑 SE 面临的的安全威胁及相关安全措施。例如，SE 与 NFC 控制器之间，SE 与操作系统之间的访问，API 以及访问控制权等，一旦发生权限越界或者其他的威胁安全的操作，将导致敏感信息泄露或金钱损失等。

为了确保终端以及硬件安全，可以通过可信执行环境和移动可信模块来实现。以底层硬件为基础通过层层度量、和认证的方式构建从系统启动到操作系统运行的可信环境。

9.3.4 NFC 系统安全

系统安全威胁包括系统漏洞、恶意软件、系统 API 滥用，权限滥用、系统后门等智能终端操作系统存在大量安全漏洞或后门，系统 API 和权限存在被滥用的风险，恶意软件也能危机系统的安全，这些因素将危及 NFC 依赖的智能系统安全。为确保系统安全性，以 Android 系统为例，一般包括内核访问控制机制、沙盒机制、权限检查机制、数字签名等。不同的操作系统的安全机制不同，需要具体的分析和研究。

9.3.5 NFC 应用安全

应用安全包括漏洞、逆向工程、重打包、恶意软件等、应用软件开发良莠不齐，应用存在大量安全漏洞，由于对安全不重视，通过逆向工程技术或者重打包，能够获取程序的源代码、用户信息，并植入恶意程序，严重危害应用层的安全。例如，攻击者通过捆绑恶意应用程序诱骗用户下载 NFC 恶意支付应用，用户的

手机将成为攻击者的“提款机”。AVL 安全研究团队就曾发现一款利用 NFC 手机攻击公交卡的恶意软件，通过该款恶意软件安装在一个 NFC 手机上，攻击者手持该款手机轻轻靠近圣地亚哥的交通卡，就可任意篡改卡中的余额。

安全加固是保障应用程序安全的主要技术之一，通过对应用程序加密、混淆、加壳等，防止应用程序被执行反编译、二次打包、插入恶意代码等恶意操作。从防御角度，针对以上各个方面的风险，要保障 NFC 安全应该侧重于使用加解密算法、秘钥共享、签名算法、恶意内容检测算法等研究具体的软件和硬件终端的防御系统设计、防御措施等。加解密可以和秘钥共享算法用于保证 NFC 通信过程中的数据安全，防止信息泄露；签名算法用于防止数据篡改、重放等，确保数据的完整性；恶意内容检测算法用于防止通过 NFC 传入恶意内容和数据，确保 NFC 应用程序的可用性和安全性。为了确保 NFC 应用程序等的机密性、完整性、可用性，在 NFC 系统、应用程序等的设计和开发阶段就积极加入安全防御措施。安全漏洞是研究安全问题的生命线，是网络和信息安全的核心问题，提前发现并修复 NFC 安全漏洞是 NFC 系统和应用安全的重要保障。关于 NFC 技术，已知且细节公开的漏洞如下：CVE-2008-5825，CVE-2008-5826，CVE-2008-5827，Bugtraq ID 68470,E 乐充公交卡支付漏洞等。

9.4 无线射频遥控安全分析

无线射频遥控技术主要是利用射频模块将控制信号编码，无线传输，解码再放大来驱动接收方的电器元件，实现无线遥控的技术。无线遥控编码有多种，主要为固定码和滚动码。常用于防盗报警设备、门窗遥控、汽车遥控等场景。

固定码，其特点是廉价、应用广泛、市场大、用户多，但是编码容量仅为 6561 个，重码概率极大，且其编码值可以通过焊接点连接方式被识别，保密性

差，仅是用侦码器就可以获取。攻击者可以通过直接爆破固定码或者通过嗅探信号并进行分析等方式获取固定码，然后进行利用攻击。

滚动码其实就数据经过一种复杂的非线性加密算法的加密所得的动态编码，仅一次有效且编码间无相关性，相比于固定码较为安全一些，因此被部署到需要更强的安全性的设备上。但并不是说使用了滚动码就万无一失了，例如，一个名叫 Tom Wimmenhove 的荷兰电子工业设计师在多款斯巴鲁汽车的钥匙系统中发现了一个严重的安全设计缺陷，即使钥匙使用的是滚动码，但仍然可以通过嗅探信号进行攻击，实现劫持。

10数据和隐私保护

10.1 物联网与隐私和数据保护的关系

在物联网的很多应用场景下，数据采集不可避免涉及到个人信息，甚至是敏感的隐私数据。可识别的个人数据，以及可以直接定位到具体自然人的信息都属于隐私保护的范畴。因此，需要根据隐私和数据保护的原则进行审查并加以保护，保证涉及的企业及人员的基本权利不会受到新技术的侵犯。

在国内外的立法中，对于隐私保护没有统一的名称，存在“个人信息”、“个人资料”、“个人数据”和“隐私”混用的情况。1980 年，经济合作与发展组织（OECD）在《关于保护隐私和个人信息跨国流通指导原则》中揭示了个人信息保护八大原则，即：收集限制原则（Collection Limitation Principle）、数据质量原则（Data Quality Principle）、目的明确原则（Purpose Specification Principle）、使用限制原则（Use Limitation Principle）、安全保障原则（Security Safeguards Principle）、公开性原则（Openness Principle）、个体参与原则（Individual Participation Principle）和问责制原则（Accountability Principle）。这些指导原则对全球各国的立法产生了巨大的影响。

10.2 物联网中的隐私保护的关键步骤

毫无疑问，物联网服务提供方都应该采取适当的技术和组织措施确保对个人数据安全的保护处于合理的级别。同时，在隐私保护中存在一些独特的步骤和要求。

10.2.1 确定在物联网服务中的角色

在个人数据处理中，存在控制者和使用者两种角色。控制者决定处理的内容和方法，而处理者必须严格遵循控制者的指导进行处理。物联网业务的提供者，

作为控制者，承担着保证数据合规的第一责任。在物联网场景下，对于控制者和处理者的认定，需要根据应用的情况来确定[1]。例如，采集的数据发送到物联网提供者的后台服务器上保存，毫无疑问物联网提供者是控制者。同时，如果控制者委托第三方处理收集的数据，如使用云服务提供商保存数据，则云服务提供商是处理者[2]。在某些情况下，因为云服务提供商处于强势地位，对数据的保存处理有较强的话语权并提供了标准的服务，也可能被认定为是联合控制者。如果物联网提供者委托第三方开发了物联网相关软件、硬件，在开发完成后，处于某种目的，开发者需要从物联网提供者处获得相关的个人数据，则开发者也将成为控制者或联合控制者[3]，而这取决于物联网开发者和提供者二者的合作关系。

10.2.2 确定法律管辖

在部署物联网系统时，一定要考虑相关的法律管辖区域的相关规定，保证物联网的使用在相关区域合法合规。在确定相关法律管辖时，会涉及物联网服务商的注册或运营地址，物联网托管的平台或物联网数据的存储位置，物联网数据主体的国别等信息，有时会存在重叠甚至冲突的情景。

对于个人数据的跨境传输，物联网控制者根据不同国家的要求可能有多种方式可以展现数据保护的充分性，这些方式通常包括限制云服务的地理位置，采纳所在国批准的标准合同模板，起草数据传输协议，获取认证，有约束力的企业协议（BCR）等法律认可的方式保证合规。

10.2.3 数据保护影响评估 （DPIA）或隐私影响评估 （PIA）

物联网中的数据保护影响评估主要目标是识别物联网场景中产品或服务的处理活动对自然人权利和自由带来的风险。控制者的评估主要考虑项目是如何收

集、使用、分享、维护个人数据的；确定项目、处理、功能和系统中个人数据的内在风险；确保符合隐私及数据保护的相关法律和法规的要求。

数据保护影响评估应该检查联网场景下的产品或服务中处理活动的描述及目的，确认计划采集的个人数据的合法性、必要性和恰当性，是否与处理活动的描述及目的一致，是否存在超范围采集的情况。同时控制者评估对数据处理对数据主体的权利和自由带来的潜在风险，通过采取适当的风险应对措施和证明合规的安全措施，以及默认和设计数据保护措施时是否可以将相关风险减低到可接受的程度，如果不能则需要修改数据处理目的或咨询数据监管当局。

评估应确定个人数据的接受者清单、数据保存期限、行为准则以及是否需要咨询数据主体并获得同意等细节。隐私保护评估的结果应该签署并记录并根据干系人的不同准备不同明细程度的报告。

10.2.4 隐私政策声明

数据控制者提供的物联网业务涉及个人数据（包含收集、使用、转移、存储等）时，必须向数据主体提供相关产品或服务的隐私声明，描述所收集的个人数据类型、目的、处理方式、时限、风险和建议，内容应该符合相关法规的要求。建议如下：

a）产品提供正常业务时涉及个人数据（包含收集、使用、转移、存储、销毁），必须在产品资料中提供产品处理涉及的个人数据的说明，描述产品处理的所有个人数据类型、目的、处理方式、时限、风险和建议。

b）直接面向数据主体并提供界面的产品，应该可以在界面上要按照数据控制者的要求展现隐私声明。

隐私政策和用户协议可供随时查看。我们建议在提供隐私政策时，在网站上可以层次化展现，便于用户跳转到感兴趣的部分。同时，网站应该可以提供完整的隐私政策，便于用户下载。同时，在隐私政策调整后，应该在网站给予提示，或者给注册用户发送邮件或提供其他形式的提示，保证用户了解相关的变更。考虑到隐私政策的受众，政策说明应当采用平白、易于理解的语言，辅以图标等视觉提示，便于用户了解。

10.2.5 数据主体的同意和选择

个人数据收集应基于数据主体同意、书面授权或其他法定事由，物联网服务提供者应该保存数据主体的同意或授权记录以便核查，给予数据主体选择权并确保数据主体的“同意”是可撤销的：

a) 涉及到系统或应用配置变更、下载软件、对用户系统或软件升级，接入服务等修改用户个人空间的行为，或者收集或使用个人数据前，须明确提示用户，获得用户的明示同意，并且允许用户随时关闭对个人数据的收集和使用。对于直接面向数据主体并提供界面的产品在获取用户同意时，同意须要求用户采取明确的确认动作，不得默认勾选同意；

b) 默认禁止收集数据主体的敏感个人数据，除非业务必需（如：运动健康类业务）或为了满足法律与监管机构要求可收集和处理（包括数据建模），并且同意应该被单独收集。对未成年人提供服务或收集了包含年龄信息的个人信息时，需要实现从未成年人的监护人处获取同意的功能；

c) 数据控制者和数据处理者应提供对用户的同意和撤销同意行为进行记录的机制；

d) 隐私声明内容发生变化时，须告知用户查看并获得用户同意，并允许用户撤销已有的同意；

e) 涉及物联网终端在特定区域运行，应进行路牌、张贴提示等。涉及物联网终端为特定活动提供服务，应采用社交媒体、公告、报纸等即时通知数据主体。物联网终端进行采集个人数据的活动时，应采取措施保持对用户可见，例如终端可以有明亮的色彩或声音。若现场有终端操作员，应保证终端操作员对用户可见。

10.2.6 收集和处理

基于目的相关性、必要性、最小限度收集个人数据。如果从第三方收集个人数据应尽可能确认个人数据是以合法的方式被收集的：

a) 个人数据收集范围、使用目的不得超出隐私声明，且遵循最小化原则，当个人数据的采集范围、使用目的发生变更时，应及时更新隐私声明。个人数据的使用目的、方式和留存期限应与向数据主体的通知、客户授权的范围保持一致。基于个人数据处理目的保持个人数据的准确性、完整性和相关性。要为个人数据提供安全保护机制，防止个人数据被盗用、误用或滥用，防止个人数据被泄露；

b) 数据主体撤销同意之后，产品必须禁止继续收集和处理其相应个人数据；

c) 在设备维修、销毁或云资源回收等场景下，必须提供安全删除的机制或指导；

d) 对于收集和处理个人数据的系统，管理须面对操作人员的个人数据操作行为记录日志。

10.2.7 数据归档和销毁

在用户撤销同意、数据保存达到要求的期限或者物联网服务结束时，需要销毁采集的个人数据。如果因为法律法规要求或处于科学研究目的需要对数据继续

进行风险，除非法律明确要求，否则应该对数据进行匿名化或数据聚合处理，保证处理后的数据是不可识别数据主体的。

10.2.8 数据泄露通知

在发现数据泄露时，数据控制者应根据法律要求在规定期限内向监管机构报告并根据泄露情况和法律的要求向数据主体披露。报告应当包括：泄露的个人数据的性质，记录的类别和大致数量；数据保护官或其他能够获取更多信息的联络人的名称和联系方式；描述个人信息泄露的可能情况；描述采取的或者计划采取的应对措施。

数据控制者应当记录任何个人数据泄露情况，包括泄露相关的事实、影响和采取的补救性措施，帮助监督机构进行核查。

10.3 物联网产品设计中的设计隐私保护(Privacy by Design)和 默认隐私保护（Privacy by Default)

设计隐私保护（Privacy by Design）和 默认隐私保护是隐私保护的基本原则。物联网场景下，产品设计或提供服务时应该实现 ：

a) 主动分析用户隐私威胁，预防不同场景下用户隐私风险；

b) 将隐私保护作为产品或服务的默认设置，限制最小特权，确保知情权以及初始设置为不信任等；

c) 将隐私保护嵌入到产品或服务的设计过程；

d) 确保将隐私保护作为产品的一项功能，并且最终产品的全功能为正和而不是零和，产品功能不以牺牲用户隐私为代价；

e) 保障端到端安全，提供个人数据全生命周期的保护；

f) 确保数据处理过程的可见性和透明度；

g) 尊重用户隐私，以用户为中心。

依据以上原则，可以采取的措施有：

a) 匿名化：进行数据的匿名和聚合；

b) 数据最小化：仅收集必要的数据，并立即删除不必要的数据，提供数据处理的目的描述和必要数据列表，在可能的情况下匿名/聚合部分数据，淡化数据；

c) 假名化：删除所有可直接识别个人的元素（如运动场景下自动化识别个人的步态信息），进行哈希或使用多态伪 ID；

d) 加密：如文件或数据库加密、磁盘加密、传输加密等；

e) 访问控制：物理访问控制、逻辑访问控制、身份认证和鉴权等，提供授权矩阵和可供检查的日志；

f) 默认进行隐私保护：将隐私友好作为默认设置，提供透明的用户界面和权限管理，可在注册时选择加入/退出隐私友好设置和权限；

g) 提供并遵循删除/保留条款：根据条款进行自动删除，标记保留期结束后的数据；

h) 保障并促进数据主体的权利：确保数据主体获悉隐私声明、访问请求政策等，并确保数据主体有权更正和删除个人数据。

11 终端安全

11.1 物联网终端定义

终端是具有数据采集能力和计算及处理能力的终端设备，具有有限的网路连接和传输能力，可以将设备数据转换为 IP 数据或将 IP 数据转换为设备可以处理的数据格式。终端包括三种类型：传感器、数据采集和处理设备以及移动应用。边缘网络接入设备不属于终端。

总的来说，终端有如下特点：

a) 部署在数据采集现场或由使用者操作。根据使用情况的不同，终端可能部署在要控制的设备内部或附近，通过特定的协议与设备交互，采集设备的信息并根据需要对设备发出控制指令；

b) 采用特定的协议与设备交互，这些协议可以是 Modbus、CAN、工业以太网等协议；

c) 采用无线或有线形式进行网络通信。采用的无线协议包括蜂窝(Cellular)蜂窝网络(包括 GSM、GPRS、3G、4G 和 5G)等远程通信，Wi-Fi 的 IEEE 802.11 协议、Zigbee IEEE 802.15.4 或 Z-Wave 等短程至中程通信协议、蓝牙(Bluetooth， LE)、以及 6LoWPAN(low-power Wireless Personal Area Networks，低功耗无线个人区域网)；

d) 不一定具有操作系统。对很多应用程序而言，系统很简单，所以不值得使用，或不允许使用操作系统。例如，用于执行测量并将测量值发送给另一个设备的传感器可能使用 PIC 这种低功耗微处理器，几乎没有使用操作系统的必要性。对处理时间具有硬性要求的更复杂系统通常使用 RTOS(Real-Time Operating System，实时操作系统)，如 VxWorks。非 RTOS 操作系统通常称为通用操作

系统。最常见的是 Linux。用于嵌入式系统的 Linux 与用于桌面系统的 Linux 区别不大。文件系统和体系结构是一样的，主要区别在于外围设备、存储和内存限制。由于存储器和内存较小，因此操作系统和文件系统也都尽量压缩，使用更小的一体化程序 busybox[3] 而不是安装在 Linux 中的常见程序(如 bash、telnetd、ls 和 cp 等)。

11.2 终端物理安全

OWASP 的“IoT Attack Surface Areas Project”分析了物联网常见的攻击面。对于物理安全而言，主要的挑战如下：

对于传感器而言：

a) 操纵测量环境

b) 物理干涉

c) 物理损坏

对于设备而言：

a) 固件导出

b) 用户命令行界面

c) 管理员命令行界面

d) 权限提升

e) 重置为不安全状态

f) 移除存储设备

g) 抗干扰

h) 调试端口

i) 暴露设备 ID 和序列号

因为命令行界面涉及设备内部软件设计，固件导出更多是在连接到调试端口后执行的软件操作，在此不做阐述。

为了提升物理安全，从物联网设备的设计、生产和实施部署及日常维护中，应该做到以下几点：

a) 建立物联网设备安装访问维修维护政策，明确安装标准，确定相关操作规范，并定期检查政策执行情况；

b) 建立物联网设备台账，记录物联网设备的厂家、型号、规格、安装位置和使用目的，建立盘点规则，确认设备的状态并及时更新；

c) 检查设备/传感器是否可以轻易取下，拆开。在硬件设计中尽可能采用防破坏设计，外壳一经打开立刻给予提示或报警，或者不能使用。在安装过程中也要考虑物理加固及封装；

d) 在硬件表面不提供不必要的端口。保证在不拆除设备的情况下无法获取数据；

e) 通过管理界面可以禁止对端口的使用；

f) 确保只有通过本地连接才能使用管理界面。对于管理界面的访问有日志和远程提醒；

g) 设定系统巡检计划，定期检查和校验设备；

h) 终端故障、异常自动报警；

i) 设备信息不显示在设备外部铭牌上；

j) 系统安装中注意防止干扰；

k) 对于数据采集尽可能采取冗余设置，防范因为单点故障导致的数据失真。

11.3 终端系统安全

物联网终端系统安全应该具备的能力：

a) 系统运行时安全：检测终端自身的运行时安全，如 CPU 使用率、进程快照、流量信息、文件改动、远程登录等终端基线安全相关信息。检测来自供应链、设备间东西向攻击的潜在威胁。

b) 防御设备间东西向攻击能力：病毒在内网传播/局域网传播/专网传播，这种设备间的感染行为几乎成了现在 IoT 病毒的必备功能。当一台设备被黑客入侵，黑客可以以该设备为宿主，在内网进行病毒传播或者网络攻击。所以终端需要具备防御东西向功能的能力

c) 固件安全：对于无操作系统的物联网终端，对系统级的检测能力有限，但仍需关注固件本身安全。固件在 OTA 升级过程中可能被间接截取、或者通过通信总线或者编程器直接读取，所以固件应防止轻易被获取，从而被黑客所利用。固件安全主要涉及三个方面：

- 固件可信源验证
- 固件传输安全
- 固件代码安全

d) 移动存储介质使用风险：物联网终端在售后运维、系统升级、或是封闭的工业场景下，经常会使用 U 盘、移动硬盘等移动存储设备传输数据，在此过程中，病毒非常容易在移动介质中进行传播从而感染终端设备。

e) 定期更新自身系统及第三方依赖：关注物联网安全相关的威胁情报，对第三方终端操作系统、开源工程、硬件方案等不断涌现的安全漏洞，及时进行更新和维护。

f) 对操作系统和业务开放的协议和端口进行模糊测试，避免畸形报文导致设备死机、重启或者脱管等异常现象。

11.4 终端应用安全

保证终端对要安装的应用软件进行来源识别，对已安装的应用软件进行敏感行为控制，同时确保终端中的预置应用软件无恶意吸费行为，无未经授权的修改、删除、窃取用户数据等行为。

11.5 客户端应用安全技术

目前物联网设备(智能硬件)大多采用通过手机 APP 作为客户端的方式进行远程控制和设备管理，APP 客户端的安全因此也成为物联网安全中的重要一环。

许多智能硬件 APP 中包含了诸多敏感信息，如通信密钥、云端 API 接口、设备 ID 和 Token 等，稍有疏忽就可能泄露敏感信息，导致整个安全防护体系的沦陷。

客户端 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。

a) 防止 APP 反编译。反编译是将二进制程序转换成人们易读的一种描述语言的形式，是逆向工程中的常见手段。反编译的结果是易读的代码，这样就暴露了客户端的所有逻辑，比如与服务端的通讯方式，加解密算法、密钥、转账业务流程、软键盘技术实现等等。

b) 防止 APP 重打包。对客户端程序添加或修改代码，修改客户端资源图片，配置信息，图标等，再生成新的客户端程序，实现应用钓鱼。

c) 防止 APP 动态调试。指攻击者利用调试器跟踪目标程序运行，查看、

修改内存代码和数据，分析程序逻辑，进行攻击和破解等行为。

d) 防止 APP 代码注入。通过将恶意代码写入到目标进程并让其执行的技术。攻击者可以将一段恶意代码写到目标进程，这段代码可以加载其它可执行程序，进而实施 hook，监控程序运行行为、获取敏感信息等。

12 云端平台安全

12.1 云端平台架构

物联网平台，位于物联网架构中的平台层。依托于互联网、云计算等技术建构，同时需要兼容各类硬件通信模组（3G/4G/5G/NB-IoT/WiFi 等），做到不依赖于特定的硬件模块。功能上满足终端信息的采集、存储、计算、展示、大数据挖掘、增值服务等。实现基于自身的应用场景、终端类型，灵活组合与扩展各功能组件，达到快速构建物联网系统的能力。

云端平台架构主要关注以下两方面内容：一、物联网云平台的设计思路；二、物联网云平台核心功能模块。

12.1.1 物联网平台架构设计思路

a) 可扩展性：

- 云端功能拆分粒度细
- 支持水平横向扩展
- 云端功能多为 RPC 服务，升级平滑
- 根据应用场景灵活集成第三方行业应用

b) 安全性:

- 网络通信安全防护
- Web 应用安全防护
- 数据安全防护
- 云间接口防护
- 运维安全防护

c) 健壮性：

- 功能组件高度解耦
- 核心功能支持负载均衡
- 自动化运维检测

12.1.2 物联网云平台的核心功能模块

a) 设备接入：应支持多种设备接入协议，同时考虑效能。平台支持 MQTT、TCP/IP、CoAP、HTTP、等物联网常用协议，物联网方向最主流的是 MQTT 协议。支持高并发应用及终端接入，同时要保证可靠性；

b) 安全认证及权限管理：平台与物联网终端应具备双向的身份验证。平台的账号需要具备权限管理机制，根据不同的身份账号设置不同的操作权限。针对关键功能的操作，如补丁或 OTA 升级需要进行身份的二次验证；

c) 设备管理：可获取到如下信息：设备业务数据、上下线时间、历史数据、地域分布、告警信息、版本信息等；

d) 业务功能引擎：实时消息、离线推送、用户管理、告警功能、OTA 升级、设备联动、设备分享；

e) 大数据分析:具备设备状态、安全监控、用户画像、数据挖掘 、能耗预测、故障预测、地域分析、安全态势感知等能力方便企业运维，提升数据价值；

f) 运维管理：平台应具备自动化的运维管理能力，针对服务器硬件资源、网络吞吐、WEB 服务、数据库、JVM、进程、应用程序等模块进行运维；

g) 增值服务：研发辅助、运营管理、售后服务。

12.2 云端平台安全威胁

随着近年来云计算的迅猛发展，云已经成为各行各业的基本基础设施。因此

云上的资源和信息越来越集中化，这成为了攻击者的焦点；另一方面由于云自身的虚拟化、多租户等特征导致的安全问题也越来越突出。云安全面临的威胁与日俱增，CSA 于 2016 年发布了云安全顶级威胁报告，主要包括 12 大顶级威胁。具体如下：

数据泄露：随着云的普及，大量数据在云上集中存储，而且通常会包含很多个人敏感数据，因此云厂商成了黑客的新目标。一旦发生云上的数据泄露，组织可能面临罚款或指控，最关键的是企业在客户心目中的形象和地位会受到长期持续的影响。

注意，云上数据保护的最终责任在于云客户，也就是购买云服务的公司，而不是云厂商。建议采用多因子身份验证和加密措施来防止云中的数据泄露。

凭证被盗和身份验证失效: 未严格执行账户控制策略如过期账户未能及时撤销、密码强度控制不够、账户风控缺失、双因子认证缺失、SQL 注入漏洞、对密钥进行硬编码等都可能导致用户凭证被盗。建议采用令牌、手机短信验证码等进行二次验证，定期更换密钥和凭证，通过配置文件读取密钥、禁止对密钥进行硬编码。

管理界面和 API 权限被绕过： 云的安全性和可用性依赖于管理界面（控制台）和 API 的安全性。脆弱的管理界面和有漏洞的 API 会带来很多安全问题。API 和管理界面需要对公网提供访问，因此必须暴露在公网，这样就成了整个云架构中最脆弱的部分。应该将管理界面和 API 都纳入 SDL 生命周期中，在代码审计和安全测试环节都需要重点关注。

系统漏洞利用： 云环境多租户的特征使得系统或程序漏洞的危害更加突出。传统 IT 架构下系统或程序的漏洞只影响一家企业，但是云场景下，这些漏洞可

能会影响所有租户。IaaS 公有云场景下虚机隔离相关的漏洞危害尤其严重。云厂商应该定期漏洞扫描、及时补丁管理和紧跟系统威胁报告。

账户劫持/仿冒：网络钓鱼等攻击手段获取账户凭证的攻击在云环境下仍然适用，攻击者可以利用云服务窃听用户活动、操纵交易、篡改数据。企业应该加强账户管理和审计，采用双因子认证并严禁共享账户。同时完善账户风控机制、对于异常登录尝试进行及时的发现和拦截。

恶意内部人员：人是最大的风险、内部人员尤其是拥有特权身份的内部人员更是如此。你永远不清楚他们心里怎么想。恶意内部人员可以盗取或篡改数据、甚至破坏系统。建议企业实行严格的职责分离机制，最小化用户权限。同时管理员活动进行严格的监测和审计，对于一些敏感操作实行两步验证并及时发送操作提醒。

APT（高级持续性威胁）:高级持续性威胁（APT）因为其攻击的长期性、持续性、隐蔽性、高危害性等特征被广泛关注，云环境下也不例外。云厂商首先应该防止 APT 渗透进他们的基础设施。建议企业加强信息安全意识培训，尤其是反社会工程攻击的培训。

永久的数据丢失: 云厂商的技术缺陷或操作失误、黑客恶意攻击等都可能导到数据永久数据丢失。云厂商需要采用分布式冗余部署、同时应该建立完善的数据备份机制并严格执行。防数据丢失的责任是由云厂商和云客户共同承担的。例如对于客户自带密钥（BYOK）场景，保护好密钥的责任就是云客户的。一旦密钥丢失，数据丢失也就在所难免。

尽职调查不足:企业在上云之前一定要进行充分的尽职调查、充分识别云中的安全风险。包括调查厂商规模与技术实力、公开的故障与历史可用性、厂商整体

经营风险、厂商的安全合规状况、标杆客户、业界口碑、互换性与可移植性（厂商琐定的风险)、是否可以协商合同（包括 SLA、保密协议等)。

云服务滥用: 云服务可能被用于违法目的，比如利用云计算资源破解密钥、发起 DDoS 攻击、发送垃圾邮件和钓鱼邮件、托管违禁内容等。云厂商对这些滥用行为需要具备识别和阻断能力，同时还应该具备一定的惩戒措施，比如罚款等。

拒绝服务（DoS）攻击: DoS 攻击不是新的攻击类型，但它们会影响到可用性，由于云上多租户和资源集中的特性，导致 DoS 攻击的影响范围被放大。云厂商要有足够的资源和技术储备来缓解 DoS 攻击对整个云平台可用性的影响。

共享技术带来的威胁：云厂商提供的是共享基础设施、平台和应用，因此任何一个层级出现漏洞，所有客户都会受到影响。一个漏洞或错误配置，就可能使整个云环境面临潜在的宕机或数据泄露风险。

12.3 云端平台安全解决方案

提供适用于物联网云端平台的全生命周期安全解决方案，包括安全事件事前检测防护、事中监测预警、事后应急恢复等方面，提供覆盖云端平台物理层、平台层、应用层的全方位安全防护机制，并保证云端平台对业务实时性、可靠性的要求。

12.3.1 事前检测防护

对云端平台系统存在的安全隐患通过检测评估的手段事前发现，并采取针对性的防护措施，预防安全事件发生。

检测手段至少包括：

1) 漏洞扫描：采用主动扫描及漏洞匹配方式发现云平台系统漏洞及服务漏洞，并对漏洞危害进行安全等级分析。检测对象至少包括：物理层固件、硬件及软件系统，平台层虚拟化技术实现软件系统，应用层软件系统；
2) 配置核查：依据符合云端平台应用场景的安全基线规则，对云端平台系统、设备及组件的管理配置情况进行合规性检查。检测对象至少包括：物理层系统文件配置及设备集群管理，平台层虚拟化网络管理，应用层软件系统身份认证、访问控制、数据保护、日志审计等；
3) 完整性检测：通过摘要信息比对的方式，对云端平台运行过程中重要进程、文件和配置信息等进行完整性检测，发现云端平台系统软硬件设备及组件的异常变更。

防护措施至少包括：

1) 网络边界防护：在云平台网络接口部署边界保护设备；确保云平台接入连接只能通过指定接口进行；
2) 通信机密性保护：保证通信正确配置，确保通信内容的机密性和完整性；
3) 虚拟机隔离：通过虚拟化策略配置实现虚拟机之间、虚拟机与宿主机之间逻辑隔离；
4) 漏洞病毒防护：通过部署防病毒软件、白名单、黑名单或其他方式，在云端平台网络出入口以及系统、设备上实施漏洞、病毒、恶意代码防护机制；
5) 系统补丁修复：保持系统补丁及时得到更新；
6) 用户身份认证：应对访问用户进行身份标识和认证，保证用户名密码等

身份信息的安全加密传输及存储；

7) 访问控制：根据云端平台用户的业务需要，配置其所需的最小权限；

8) 安全审计：对平台用户在业务应用中的关键操作、重要行为、业务资源使用情况等重要事件进行审计记录，有效期内避免受到非授权的访问、篡改、覆盖或删除等。

12.3.2 事中监测告警

在云端平台网络接入的物理边界、系统关键逻辑边界以及系统内部关键节点上，部署通信监控设施；通过对云端平台网络通讯流量、网络设备运行状况、系统服务运行情况、人员情况等进行实时监控，识别和记录异常状态，具备对非授权用户访问、非授权设备接入、流量攻击、木马后门攻击、拒绝服务攻击、缓冲区溢出攻击、网络蠕虫攻击等安全事件及时发现、告警和阻断能力。

12.3.3 事后应急恢复：

在安全事件发生后采取应急处置措施，抑制、根除安全事件产生的影响，恢复云端平台的正常运行。应提前制定应急响应计划，包括关键系统和组件的安全需求及优先级、应急响应的结构和组织形式，恢复目标和度量指标；在发生安全事件时，确保应急响应计划的实施能够维持云端平台系统的基本业务功能，并能最终完全恢复系统及其安全措施的正常运行。

12.4 云端平台安全认证

云端平台安全认证包含两个方面：对通过界面访问云端平台的用户身份安全

认证、对访问云端平台的终端身份进行认证。

第一个方面：属于传统平台访问身份认证，通过完备的授权/认证体系对访问平台的用户身份进行鉴权和认证。

终端身份认证方面：终端通过云端平台暴露的接口和云端平台进行交互，云端平台需要做三件事：确认终端是归属平台管理的合法终端、终端被授权访问平台、终端被授权访问对应接口。总的来说，就是要处理好终端、平台、用户之间的认证和鉴权关系，需要端到端的考虑认证鉴权体系。

一种解决方案是建立密钥管理平台和身份认证平台。密钥管理平台负责生成和分发密钥给终端与云端平台，同时负责密钥的生命周期管理。身份认证平台负责统一对密钥进行解析和认证，当平台访问终端时，终端通过身份认证平台对云端平台的身份进行认证；当终端访问云端平台时，云端平台通过身份认证平台对终端的身份进行认证。

12.5 云端平台安全服务

云平台安全服务主要为 IoT 应用云平台提供安全性保障，包括安全防护、监控及风险管理服务等。通过云化部署、租户服务的形式提供给 IoT 云端平台进行安全防护、监控以及风险管理。

12.5.1 云安全防护

- 云 Web 应用防火墙

Web 应用防火墙（WAF，Web Application Firewall）可以对 IoT 云平台 Web Portal 进行多维度的检测和防御，应可以避免因 Web 漏洞引发的数据篡改丢失、过度消耗资源、恶意扫描等问题。通过对 HTTP(S)请求的检测，精准识

别出 SQL 注入、XSS 攻击、木马上传、命令注入、文件包含、CC 攻击、爬虫以及 CSRF 等 Web 的 Top 威胁。

- 云主机安全防护

主机安全服务（HSS，Host Security Service），为 IoT 云平台的主机提供资产管理、恶意代码检测、入侵检测、基线配置核查等安全功能，降低主机被入侵以及恶意程序执行的风险。

云端平台提供的安全服务可以通过轻量 Agent 的方式对主机进行集中管理，对主机的攻击行为，如恶意程序执行、漏洞入侵、账户暴力破解进行防御，以及可以对弱口令、异常登录、安全配置等进行监控。

- 云数据加密服务

数据加密服务，可以提供密钥管理、秘钥对管理等功能。密钥管理服务通过使用硬件安全模块 HSM（Hardware Security Module）保护密钥安全，帮助 IoT 用户轻松创建和管理密钥，所有的用户密钥都由 HSM 中的根密钥保护，避免密钥泄露。密钥对管理服务帮助 IoT 用户集中管理 SSH 密钥对，保护 SSH 密钥对的安全。

- 云 Anti-DDoS 流量清洗

Anti-DDoS 流量清洗服务为 IoT 云端平台提供网络层和应用层的 DDoS 攻击防护，Anti-DDoS 通过对 IoT 云端平台云服务器、负载均衡等的业务流量进行实时监控，需要及时发现异常的 DDoS 攻击流量。在不影响正常业务的前提下，对攻击流量进行清洗。至少需要具备清洗 SYN Flood 攻击、HTTP Flood 攻击、SSL DDoS、CC（Challenge Collapsar）攻击、慢速连接、UDP Flood 、TCP DDoS、DNS 反射、DNS Flood 等攻击流量。

12.5.2 安全监控与风险管理

- 认证接入

对于 APP、终端、业务、运维工程师、运营工程师、第三方业务等与云端平台的连接需提供安全的传输通道和可信接入，对关键的接口提供双因素认证确保通信安全。云端平台的运维管理接入可使用堡垒机服务，堡垒机包含用户管理、资源管理、策论、审计等系统。

- 云审计服务

云端平台的审计服务提供云资源操作记录的收集、存储和查询功能，用于支撑合规审计、安全分析等 IoT 安全审计服务。审计服务需做到记录全面，进行的日志记录可以支撑合规、安全分析的要求，日志的访问、存储需要进行加密以及权限控制，做到权限最小化，并防止日志被篡改。

- 漏洞管理

通过 Web 漏洞扫描服务对云端 IoT 平台的 Web 应用，第三方 Web 组件、Web 服务进行扫描，识别相关应用组件的 Web 漏洞，以及第三方组件的漏洞。需要支持丰富的 Web 语言类型，Web 服务类型以及第三方组件类型。

通过主机/数据库漏洞扫描服务对云端 IoT 平台的基础架构，如操作系统、数据库、中间件等进行扫描，及时发现云平台基础架构中网络、主机、应用系统的安全漏洞，并加弥补。

13 物联网安全运营

13.1 设备入网检测与退网安全

物联网有成千上百万终端联网而成，终端安全直接影响整个物联网的安全。

因此必须对入网的设备进行安全检测。检测以批次型号为依据（相同硬件、同版本固件和配置标准）

检测内容至少应包含 ：

a) 物理安全，如是否有外置接口直接访问内部网络或敏感数据；

b) 固件安全，包括固件版本、自完整机制，OTA 安全机制等；

c) 配置安全，包括基线检查、最小化运行、弱口令等；

d) 漏洞检测，包括 XSS、SQL 注入等应用层漏洞检测；

e) 传输检测，包括是否密文传输、敏感信息保护等；

f) 数据安全检测，包括是否存在明文保存的敏感信息，无权限控制的数据获取等；

g) 认证测试，是否需要认证接入，认证过程完备性；

h) 业务逻辑检测，是否存在纵向横向越权，是否存在逻辑漏洞等。

只有经过安全检测的设备型号才允许入网。

物联网终端在各种原因退网时，也需要遵循一下安全原则：

a) 应消除终端上业务数据；

b) 应在网络上和应用系统上消除终端对应认证信息和授权信息；

c) 认证单元和数据删除应采用全覆盖擦写方式。

物联网是由多个子系统组成的复杂系统，其运行和维护通常由不同责任方负责开展，其安全要求包括：

a) 物联网中不同责任方应根据其职责，在物联网系统建设时，对物联网设备和系统的获取做出规定，如规定设备和系统提供方的资质要求、可信赖性等、提供系统文档的详细程度，供应链的安全要求等；

b) 对于物联网系统运行维护中的相关参与人员，应提出人员资质、身份审核、可信证明、诚信承诺等要求，以确保其在物联网系统维护过程中的安全可信；

c) 应对物联网系统运维的时效性、维护工具等提出安全要求，对于远程维护设备的，应对远程维护制定安全守则。

13.2 物联网安全运营监测与防护

13.2.1 物联网安全运营监测

物联网的终端设备有多样化，差异化的特点，因此在对于物联网的安全运营监测和传统网络设备的监测会有区别，物联网的安全运营监测多种多样，本指南中我们主要关注以下几点：

a) 由于物联网终端的多样化，与传统的网络设备的计算资源不可相比拟，对于对应日常安全运营的监测可以通过安全网关来监测设备的访问认证日志以及设备的异常返回日志；

b) 对于物联网终端涉及到的业务，要提前设计好对应的业务基线与正常业务的波动极限，同时，对于异常业务的安全验证机制要提前预留， 如果有异常业务的流量出现，可以通过相应的安全验证机制来判断对应的物联网设备是遭到攻击还是有业务特例出现；

c) 对于处于物理环境恶劣的物联网设备，应及时将性能状态上报，由于对于物理环境的不可控性，对物联网的性能会有一定的影响，但是性能日志的基线要提前设定好，以便于对于攻击有所判断出是真正的性能问题还是由于被操控导致的性能问题；

d) 对于监测，就不得不提到传输，对于传输来讲，一个统一的安全的协议是非常重要的，物联网的设备多种多样，涉及到的协议千奇百态，建议选择安全

的通用的协议来为物联网的设备做通信，由于通用的安全协议具有普适性，安全协议的更新比较快，相对比使用较为冷门或者小众的协议的安全程度略高。

13.2.2 物联网安全运营防护

物联网的安全运营防护主要关注在两个：一个是物联网软件的安全，一个是物联网硬件安全。

a) 物理网软件安全：无论在物联网终端设备的固件中还是控制物联网设备的应用中，都需以对应的规则来提供安全运营防护，如定期对于物联网终端进行漏洞扫描与测试，定期对于应用进行审查等等；

b) 物理网硬件安全：对于物联网终端由于其暴露在不同的物理环境当中，对于硬件的直接攻击与间接攻击成为了物联网设备硬件安全里面尤为重要的一块。

13.3 物联网安全态势感知与预警

物联网的态势感知与预警，首先与物联网设备的监控有着密切的关系，对于传统的计算设备的监控不同的是，传统的计算设备的监控主要依赖于定制化的探针，然后通过对应的探针将对应的日志回传到统一的平台，做平台级别的分析与梳理，并将其可视化成为对应的图形，以方便安全的运营人员进行日常的运维。当探针回传的信息触发特定的规则或者触判到了设定的基线，对应的安全平台会有对应的预警。

对于物联网的态势感知，主要是通过感知层回传的数据以到物联网的统一安全管理平台进行集中的分析，可视化物联网设备的分布，及其硬件与软件的健康数据，同时将性能数据作为一个单项分出，以通过日常运维与审查的方式等等作为态势感知评估的输入，通过对应的态势感知模型输出对应的数值并可视化。

对于物联网的预警，根据我们对应的态势感知评估的数值与对应的数据分析，结合一些基线与对应的触发条件，会得出预警的可能性与损失的预估和预判，从而为物联网安全运营团队争取时间和提供输入，物联网安全运营团队通过对于预警系统给出的结果结合实际的情况进行排查，可以达到事前高效防范，事中高效处置，事后高效取证的三高效的目的。

14关键业务场景应用指南

14.1 车联网安全

14.1.1 车联网安全现状、威胁

车联网起源于物联网的快速发展，是物联网技术在交通领域的典型应用。车联网除了继承物联网的智能、先进、互联的基本特征外，车联网对智能感知终端、通信网络和应用服务等方面都提出了更高要求。

在无线通信网络方面，V2X 无线通信技术代表着汽车网联化发展趋势，也是实现汽车安全预警和智能驾驶辅助的有力支撑，将感知范围扩展到车载传感器不可及的范围。在应用服务方面，车联网通信及应用接口多样，应用服务场景更为丰富，构建车联网大数据和云平台共性支撑服务平台，提高车联网应用服务的开放性和弹性化，是车联网发展的必然要求和未来竞争焦点。

14.1.2 车联网安全通用架构

车联网网络安全防护是车联网能够全面发展及部署的根本保障。车联网的网络安全重点关注智能网联汽车、信息服务平台和智能移动终端等主体的安全，重点关注通信网络安全和应用服务的安全，以及贯穿于整个车联网的数据安全和隐私保护。如下图所示分别从终端、网络和平台的视角，分析提出了车联网网络安全架构。

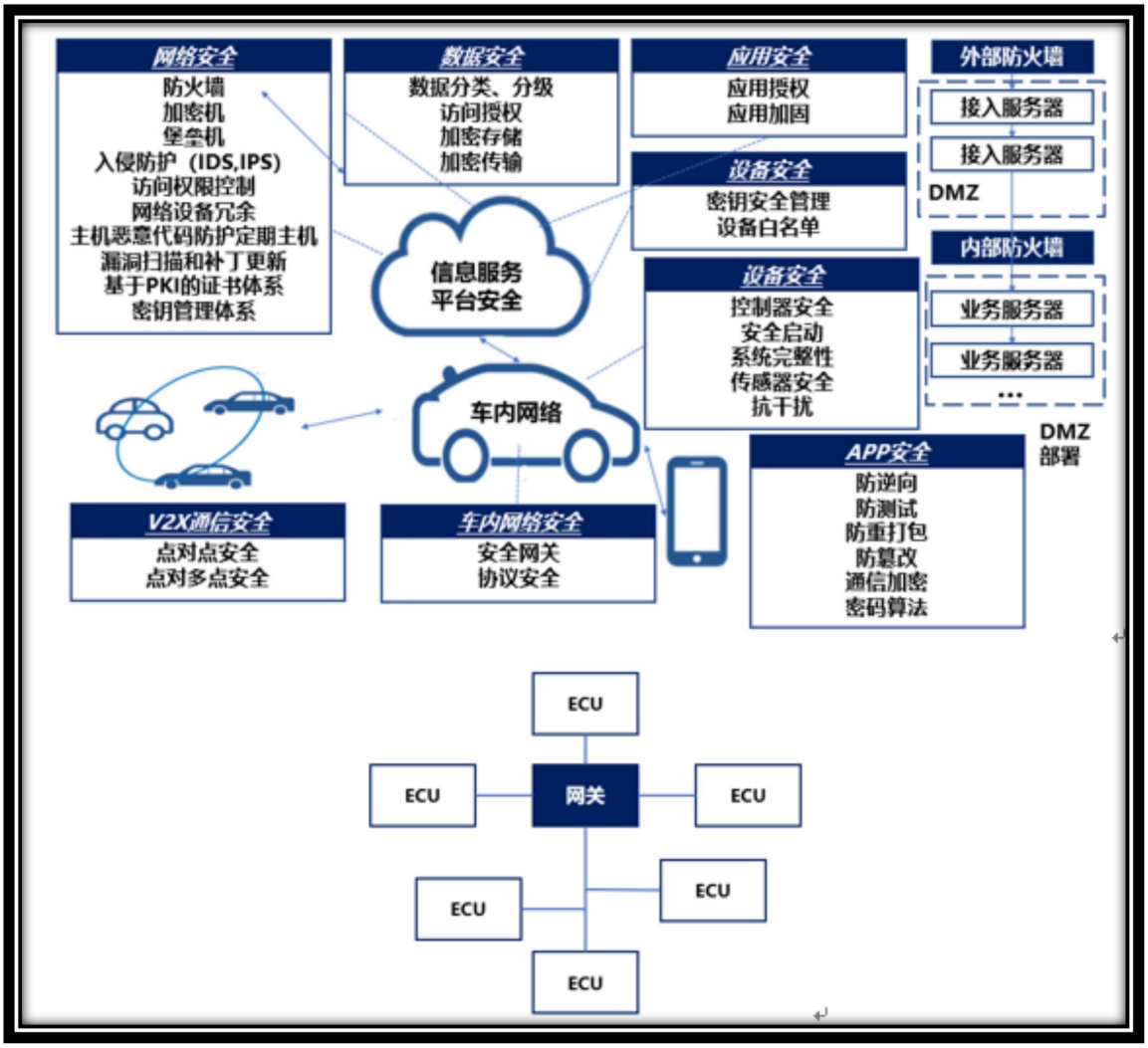

图 14-1 车联网网络安全架构图

其中，智能汽车终端的安全重点关注设备安全和车内网络安全两方面，车内设备又包括控制器安全、安全启动、系统完整性、传感器安全和抗干扰等方面，车内网络安全从安全网关和协议安全两个方面来应对车内网络安全问题；移动终端安全重点关注防逆向、防调试、防重打包、防篡改、通信加密和密码算法；信息服务平台的安全重点关注设备安全、网络安全、应用安全和数据安全四个方面，设备安全手段有密钥安全管理和设备白名单，网络安全的技术手段包括防火墙、加密机、堡垒机、入侵防护（IDS、IPS）、访问权限控制、网络设备冗余、主机恶意代码防护、定期主机漏洞扫描和补丁更新、基于 PKI 的证书体系，以及密钥

管理体系等，应用安全从应用授权和应用加固两方面实施，数据安全包括数据分类分级、访问授权、加密存储和加密传输等方面。车际通信网络安全还需要关注点对点安全和点对多点的安全。

车联网网络安全与功能安全同等重要，而车联网数据安全、隐私保护的重要性也日益凸显，数据安全和隐私保护贯穿车联网的整个云管端安全环节。下面针对车联网 5 个威胁点进行分析，包括车载端、车联网信息服务平台、移动智能终端、无线通信、数据安全和隐私保护，对车联网网络安全技术、网络安全管理和网络安全最佳实践提出 3 点建议。

14.1.3 车载端安全威胁分析

a) T-BOX/IVI 是两种主流的网关形式（车载端无线通信接口），威胁多样成为安全核心环节

T-BOX/IVI 面临来自几方面的安全威胁：一是通过获取加密算法和密钥，解密通讯协议；二是通过 T-BOX/IVI 预留调试接口读取数据；三是对 T-BOX/IVI 的 flash 芯片进行逆向分析。通过上述对控制协议的破解、T-BO/IVIX 固件密钥爆破和逆向分析，可以伪造协议而实施对汽车制动装置的控制。

b) CAN 总线是控制安全核心，OBD 接口设备成为威胁主要来源

CAN 总线是目前普遍使用的总线通信协议，相当于汽车的神经网络，通过 CAN 总线可以建立汽车内控制器局域网，用于连接车内各 ECU (电子控制单元) 和引擎、刹车控制器等重要部件。OBD 和 UDS 是车载诊断系统接口，可以采集车辆总线数据、进行故障诊断，控制指令发送和交互，其中 OBD 面向排放系统，UDS 面向整车 ECU。通过 OBD 接口或者总线节点接入车内网络后，可以实现传感器信息采集、伪造 ECU 控制信息、信息注入，造成 ABS、ESP 等电子系统

故障、紊乱。

c) ECU 事关车辆行驶安全，芯片及固件漏洞是主要威胁

d) IVI 系统应用广泛，或延续传统信息安全风险

e) 远程更新成为必备功能，也成为黑客攻击渠道

f) 传感器是信息采集入口，干扰和拒绝服务攻击成为主要威胁

无线传感器可能因环境差、干扰大而存在无法感知，给车辆安全带来安全隐患。从安全风险来看，干扰传感器或伪造障碍物干扰，都可能干扰整车控制措施，导致逼停自动驾驶汽车或者干扰偏离自动驾驶。

14.1.4 车联网信息服务平台网络安全威胁分析

a) 私有云是远程控制源头，中间人攻击成为主要威胁。

b) 云平台仍将是车联网网络安全的保障。

车联网云平台操作系统可能存在的安全漏洞，以及操作系统自身的脆弱性影响云端服务平台的安全。作为车联网应用服务的中心节点，攻击者通过以智能终端或通信网络为入口，利用安全漏洞实施对应用服务平台入侵、控制等攻击，从而导致大量汽车被非法管控，同时威胁车联网整个网络的信息安全和隐私泄露。在车联网应用层，黑客进行 DOS 等攻击，甚至取得后台的控制权，进而威胁到车联网整个网络的信息安全以及隐私泄露。

14.1.5 移动智能终端安全威胁分析

a) App 逐渐成为智能汽车标配，应用破解成为主要威胁。

b) 移动智能终端成为车联网重要辅助设备，成为影响车联网安全的重要要素。

目前智能终端通过 WiFi、蓝牙等无线通信方式直接连接车载娱乐系统。若

智能终端被控制，攻击者可能进行漏洞分析，或对智能终端植入恶意代码来控制车载娱乐系统。并通过智能终端与车载系统的互联，智能终端中的恶意代码可以利用车载系统中存在的安全漏洞进行恶意代码植入、传播或攻击，造成车载系统异常无法正常使用或进一步实施对汽车的恶意控制。

c) 多功能钥匙逐渐流行，信号中继及算法破解成为主要威胁

14.1.6 无线通信安全威胁分析

a) 通信协议破解和中间人攻击成为车云通信主要威胁

b) 恶意节点成为车车通信威胁，可信面临挑战

c) 协议破解及认证是短距离通信主要威胁

V2X 通信链路稳定性不足，无线通信链路的脆弱性被放大，密钥更新机制有待完善，通信网络存在安全风险。V2X 网络通信自身还存在链路稳定性、可靠性、网络加密、接入认证等方面的安全问题。这些安全隐患的存在，可能导致非法节点入侵破坏网络环境，使车联网通信链路可能面临被窃听、阻断通信、伪造通信、篡改通信和重放攻击等安全威胁。

14.1.7 数据安全和隐私保护威胁分析

a) 个人数据过度采集和越界使用成为车联网数据安全主要问题

b) 数据传输和存储存在潜在破解风险。

车联网各环节中的数据信息有可能被假冒、伪造、篡改，使车联网面临安全风险。车联网中的信息来源于车载单元、ECU、RSU、传感器、云平台等对象的信息产生、加工、传输和接收等各环节，信息类型包括汽车数据、位置信息、统计信息等。车联网的业务应用依赖于数据信息的获取与传递，恶意用户发送的错误信息将直接影响车联网的使用，甚至造成安全事故。攻击者可能假冒、伪造、

篡改信息，例如通过发布错误的、或伪造篡改后的道路交通拥堵信息，相关汽车收到信息后为躲避拥堵而寻找替代路线，使攻击者可以独自占用道路资源。攻击者也可能对收到的信息进行欺骗伪造，从而影响统计数据。

14.1.8 车联网安全建议

车联网的基础网络是互联网和移动互联网、无线网等行业网络，作为承载网的互联网可继续沿用原有的安全策略，而作为接入网的移动互联网和无线网涉及到加密认证、异常流量控制、网络隔离和交换、信令和协议过滤等安全需求。

车载终端安全接入 Internet 是车辆联网安全最基本的需求之一，若不采取有效的安全接入控制措施，不仅导致非法节点入侵破坏网络环境，而且容易带来车内网安全隐患。车联网安全接入技术是指：当有新节点申请接入 Internet 或其他行业网络时，对申请节点的身份合法性进行认证并协商密钥，保障通信的安全性与机密性。安全接入技术发展至今，主要有基于口令认证的安全接入、基于门限密码的安全接入、自组织安全接入、基于身份的安全接入、证书安全接入以及基于密码学的信誉系统。(加密机、CA、PKI、OTA)

车载终端内置了多个无线接口，具备多种网络连接能力，目前普遍使用的无线通信技术有 DSRC、WiMax、WLAN、801．11、3G /4G /5G 等，车辆频繁的网间切换涉及到不同的接入技术和协议转换问题，异构无线网融合技术是车联网发展的必然选择。

隔离是为了防止非可信应用软件侵害原有主体系统，尽可能地保证原有系统功能的完整性。通过研究分析，将车联网环境下的隔离根据其面向对象不同划分为 4 种类型：

- 控制隔离：通过访问控制策略控制外网用户对车内资源的访问权限；

- 系统隔离：将车内网的车控单元和非车控单元进行隔离；
- 网络隔离：在车内网和车载应用模块之间设立隔离区，保护内网数据安全；
- 数据隔离：隔离存储设备，防止控车系统同时访问多个网络，减少病毒传播途径。

对于车联网运营商的安全防护策略，分为监控告警、安全环境和事件处理三个方面

- 监控告警包括：可扩展的监控服务、控技术方案支持、安全事件探测、监控优化、事件告警、历史数据留存等；
- 安全环境包括：受保护的 IP 地址/范围、阻止点对点通讯、防火墙、入侵检测系统、中断 IP 通讯、私有存储、短信功能限制、访问权限控制等；
- 事件处理包括：事件响应联系人、补偿措施、语音/数据黑白名单、网络瞬断功能等。

车联网已经和云逐步进行融合和相互促进，因此虽然车载终端和数据网络层的安全是必不可少的，但一些额外的安全服务需要实时智能的更新，所以系统需要能够连接到基于云的安全服务，在攻击者获得控制权限前，进行监控和防范威胁。这些措施包括：

- 安全认证：利用硬件辅助加密远程监控、软件更新和其他通讯；
- 远程监控车载终端的活动：检测车载终端的异常行为、恶意行为以及隐私数据是否被批量泄露、并远程删除恶意软件；
- 威胁情报交流：在车辆、经销商、制造商甚至政府机构之间进行合作，可以快速的将 0DAY 漏洞的利用和恶意软件警告传输给云端的总控中心、进行漏

洞修复和防范；

- 空中更新：用于固件（FOTA）和软件（SOTA）更新，并适用于智能手机和其他消费者和商业电子。通过适当的用户控制和安全预防措施，当发现安全漏洞时快速的更新系统，大幅降低召回成本和漏洞的暴露时间；
- 凭证管理：用于车辆，所有者和驱动程序身份验证的在线组件，为用户配置文件和帐户信息，联合身份以及相关的加密密钥和服务提供简单安全的管理。凭证的安全性对数据隐私至关重要。

针对车联网企业内部监控体系需要完成以下部分：

a) 漏洞扫描

定期及不定期的使用漏洞扫描工具对新开发的应用、操作系统、网络环境、各类设备进行漏洞扫描，在发现漏洞后进行漏洞威胁分级并执行修复。

定期漏洞扫描的频率不得低于半年；不定期漏洞扫描需定义进入标准，如涉安全性、功能性应用变更、上线时需进行环境、相关设备、代码等安全扫描。

b) 事件记录收集/关联

积极使用 SIEM Platform 即：安全信息、事件监控平台，通过 SIEM 对企业内部各类安全信息与事件进行收集、关联、分析与告警。

c) 主动审计

主动审计有别与监控告警，其更偏向针对人员操作、监控告警策略、监控告警机制等无法直观的从技术层面获取解决方案的流程。

审计内容，可以包括但不限于：操作系统事件日志文件、中间件事件日志文件系统、文件访问日志，资源消耗、监听服务、接收/发送网络连接等。

d) 事件响应

- 改进措施:在安全漏洞被发现后，应在企业内部上报安全漏洞基础信息的同时，实施改进措施。改进措施的修复深度、维度需在事先通过企业内部讨论得出，需形成一定的标准化文件，供漏洞修复过程中遵照。

- 入侵防护系统:入侵防御系统（IPS）是类似的入侵检测系统（IDS）的类似产品。其可以在实现数据包抓取、解析、告警等功能的基础上，进一步阻断恶意数据包，放行正常流程数据。其采用的规则、统计/基线配置等方式恶意行为/攻击/事件。一旦触发相关策略便发出警报，有别于 IDS，入侵防御系统还可以通过预先处理的方式对可能的风险数据进行自动处理。

在管理层面，需要参考 ISO26262 汽车安全国际标准进行管理。