CSA GCR cloud security alliance
GREATER CHINA REGION ®

物联网安全关键技术白皮书

序言

未来的世界是一个万物智联的世界，人们的工作生活将无时无刻被各种物联网设备紧密地绑定到一起。可以预见物联网的安全将是未来现实世界的重要组成部分，不仅关乎信息和隐私，更会关乎人民生命财产。

在本次发布的白皮书中，CSA 大中华区物联网安全工作组从分析物联网的架构、威胁出发，重点对各种物联网安全技术进行深入剖析，从底层芯片到上层 APP 测试，涵盖物联网安全的各个方面，希望能够帮助读者快速的掌握在物联网安全中可以用到的各种关键技术，这些技术可以应用到物联网产品或解决方案中，为提升产品或解决方案安全性、保护用户隐私、提升用户体验起到有效作用。本白皮书还对这些关键技术的应用场景做了分析和建议，以帮助读者在实际场景中选择合适的物联网安全技术，更好的发挥技术的能力，创造一个更加安全的物联网环境。

李雨航 Yale Li

CSA 大中华区主席兼研究院院长

目录

1.概述

1.1.物联网安全概述

Kevin Ashton 早在 1999 年就使用“物联网”（Internet of Things）一词描述一个系统，这个系统中的实体物体可以通过传感器连接到互联网。当时，这样的系统中使用 RFID 标签技术无需人工干预就可以在互联网上追踪供应链中的物品。随着物联网的发展，不同的组织机构给出了不同的解释和定义。例如，电气和电子工程师协会（Institute of Electrical and Electronics Engineers, IEEE）给出的一个定义称“物联网是将可以唯一标识的物体连接到互联网的网络。这些物体具备传感/驱动和潜在的可编程功能，通过利用独特的识别和感知，物体的信息可以被收集，物体的状态可以在任何时间、从任何地方修改 。”

从总体上来看，物联网应该具有这样几个特征：

（1）联网：无论是否连接到互联网，所有的物联网应该保证物体之间的通讯，或者每个物体都是联网的。

（2）可编程：物联网终端设备是嵌入式设备。无论物联网的应用场景如何，使用的终端是什么品牌型号，所有的终端应该具有一定程度的智能，可以进行编程。这种程序可以是写入内存的固件，也可以是 Linux 或其他操作系统，甚至是在操作系统上运行的应用。

（3）可采集：物联网设备需要具有感知的能力，对自身的运行，周边的环境参数进行记录。因此物联网中必然会部署大量的传感器，以满足场景感知的要求。

（4）可修改：修改分为两个方面。首先对于内部的固件、操作系统和应用，应该可以进行升级。升级可以是修补程序中的漏洞和缺陷，也可以是提供新的功能或废弃一部分功能。同时，在一定情况下，可以发布指令，对物联网设备进行操控并改变其运行状态。这种操控可以是基于感知的参数达到预先设定的阈值而自动触发，也可以是人为地下达指令，或者二者兼顾。

1.1.1.物联网的安全要求

随着物联网的发展，物联网安全也提上日程。黑客对物联网攻击的目标或是通过直接控制物联网设备达成，或是以物联网设备为跳板攻击其他设备或系统。前一种情况如使用震网病毒（Stuxnet）袭击伊朗的铀浓缩工厂，后者如利用 Mirai 病毒控制互联网上的物联

网设备（网络摄像头等）构成僵尸网络。有些人更是可以通过分析网络上物联网设备采集的信息发现机密。例如，分析人士通过全球定位系统（GPS）追踪 Strava 公司发布在网上的全球运动热力地图看到了美军在中东地区和阿富汗驻地的活动路线，暴露了此前从未对外公布过的秘密基地。

各国政府对物联网安全都很重视，2019 年 5 月中国颁布的《等级保护 2.0》标准包括物联网的安全扩展要求，针对不同的安全等级给出不同的要求。物联网安全扩展针对感知层提出特殊安全要求，与安全通用要求一起构成对物联网的完整安全要求。美国安全国家标准与技术研究院（NIST）对物联网安全也有专门的项目并发布了相关的指南。

物联网场景对信息安全的要求和传统的互联网存在较大差别。在传统场景下，首要考虑机密性，其次是完整性，最后是可用性。在物联网环境下，优先级发生了变化，可用性的重要性上升。物联网实时采集数据，如果不能实时采集和传输数据，数据将不可使用，在工业场景下这会导致大量次品，在消费品场景下用户会认为系统失效。由于物联网设备功能单一，通常只采集某一种或几种数据，这些数据所揭示的信息有限，基本不涉及机密。因此需要优先考虑数据的可用性，同时还要保证数据的完整性，防止数据被篡改。相比而言，数据机密性的优先级较低。

此外，物联网场景中存在几个特定的信息安全要求。传统信息安全通常是通过用户名密码或其他方式进行身份认证和授权，但是物联网设备没有用户输入界面，大多数时候是持续在线，如何保证采集的数据是从被授权的终端未经篡改地上传是一个挑战。物联网的快速部署以及终端的庞大数量，对于后台如何能稳健支撑物联网系统运行也是一个很大的挑战。某些物联网设备如果处理不当会涉及一些可能带来人身伤害的行为，因此需要考虑的不单单是信息安全，还应包括人身安全、物理安全和隐私保护。

1.1.2.物联网的安全隐患

物联网是一个巨大的市场，目前缺乏统一的标准，存在各种协议和框架。当前使用的框架有：

- OpenHAB (https://www.openhab.org/)
- Eclipse IoT (https://iot.eclipse.org/)
- GE Predix (https://www.ge.com/digital/predixplatform-foundation-digital-industrialapplications)
- Distributed Services Architecture (http://iot-dsa.org/)
- Open Connectivity Foundation (https://openconnectivity.org/)

与此同时，物联网所用的协议也纷繁复杂，一些常用的协议有：

- Wi-Fi
- BLE
- Cellular/Long Term Evaluation (LTE)
- ZigBee
- ZWave
- 6LoWPAN
- LoRA
- MQTT

上述各种各样的物联网框架和协议导致物联网安全的复杂性。与此同时，物联网市场不够成熟，从业人员安全意识薄弱进一步导致物联网的脆弱性，例如：

- 开发人员缺乏安全意识——开发人员通常对 IoT 设备中可能存在的安全漏洞欠缺必要的知识，缺少可操作的安全策略、要遵循的安全编码准则以及针对安全性的清单。
- 缺乏宏观视野——开发人员或安全团队非常容易忘记设备和各种技术的互连可能导致安全问题。 例如，仅查看移动应用程序可能不会揭示安全问题，但是如果将移动应用程序与网络通信结合，可能会发生严重的安全问题。
- 供应链安全——物联网市场存在许多利益相关者，这意味着许多供应商制造的设备其不同组件是由另一供应商制造、组装和分发的，这可能会导致安全问题或后门，从而使整个产品处于危险之中。
- 使用了不安全的框架和第三方库。

与此同时，绝大多数企业仅关心物联网可实现的功能，而对一旦使用不当带来的危害认识不清。常见的问题有：

- 从意识上对物联网设备的作用估计不足，认为其就一个简单地数据采集器，没有什么大不了的。
- 对设备疏于管理。设备安装使用后看不见，想不起。一旦部署，放任自流，不管不顾。

- 使用默认的管理员密码。使用供应商提供的默认密码，不作修改。
- 设备不打补丁不升级。
- 对向设备推送的内容不校验。
- 对设备采集的内容不评估。

下表列出了物联网面临的常见风险：

安全特性	**设备/硬件侧**	**网络侧**	**云/服务器侧**
机密性	硬件攻击	低计算能力设备的加密	隐私
完整性	缺乏证明，非法升级	低计算能力设备的签名	NA
可用性	物理攻击，无线阻塞	网络不可靠	NA
认证	缺乏用户输入，硬件导出密钥	联合身份认证的挑战	缺乏设备识别实施标准
访问控制	物理访问，缺乏本地授权	访问控制的轻量协议	需要用户管理访问控制
不可抵赖性	没有安全的本地存储，低计算能力设备	低计算能力设备的签名	NA

表 1-1 物联网面临的常见风险

物联网建设过程中，安全必须与功能同步设计、同步实现。对于物联网技术的风险，一些专业机构进行了深入的探讨，如 OWASP 的 IoT 项目就从多个角度进行了分析，很多暴露的问题可以通过一定的技术手段应对。

1.2.物联网安全威胁与分析

1.2.1.安全威胁总体分析

物联网的特点是通过大量感知设备对业务进行数据采集后由终端设备（常见形式是终端设备集成或外挂传感器）或数据归集设备汇总后进行打包上传，最终由云端使能平台通过数据汇总、分析实现业务的应用支撑，并且会由使能平台对外提供管理接口实现操作交互（交互界面常见的有 WEB UI 和移动 APP 两种）。我们使用 STRIDE 威胁建模工具进行威胁分析后，结合人工分析对威胁进行归并、提炼，得到了下面的物联网威胁地图：

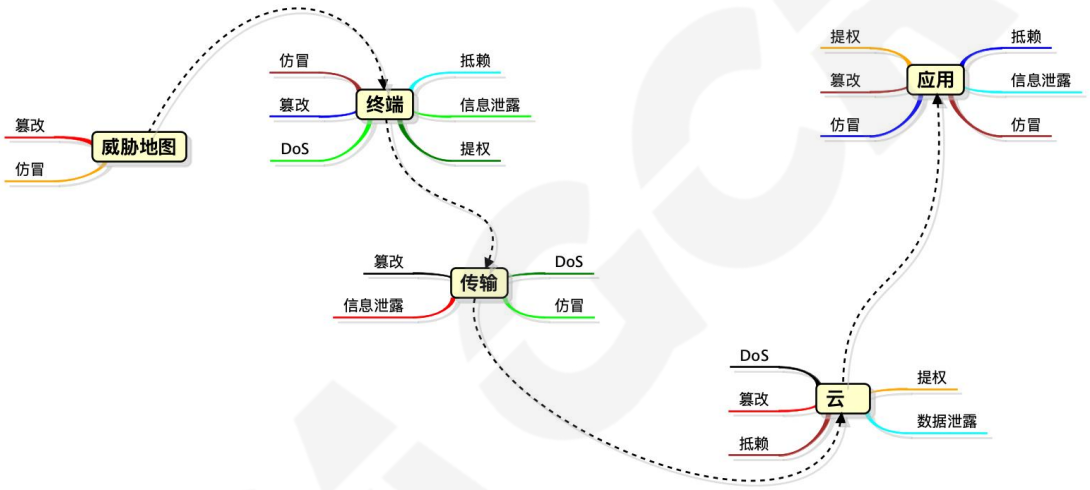

图 1-1 物联网安全威胁地图

在威胁地图上我们可以看到网络传输、云端服务、数据至移动 APP 基本都属于网络安全相对成熟的垂直领域，针对威胁选择成熟方案或快速定制都比较容易达到目标；但由于感知层设备类型碎片化、部署泛在化和网络异构化三大特点，使得物联网边缘侧安全保障需要安全技术上的创新得以落地。

1.2.2.传感器安全威胁分析

传感器作为物联网技术对物理世界实现数字化感知的使能原件直接决定了上层应用实现程度。作为攻击方，针对传感器的攻击方式主要是通过技术手段使得传感器失去感知能力或感知错误信息，以达到通过错误数据引导上层应用得到偏向攻击方预期的结果，进而可能引发物联网系统的错误反馈，比如进行了错误的动作指令决策，导致执行器按攻击设想进行动作而达到攻击目的。

结合传感器实现技术分析，来自攻击者的威胁主要有以下两种方式：

（1）篡改，攻击者针对目标传感器施加外因迫使传感器产生错误数据欺骗物联网系统，例如对 MEMS 传感器施加干扰震动，对温度传感器施加热辐射以及通过物理方式破坏传感器等；以及攻击者通过重放攻击等通讯手段劫持正常数据包对感知数据篡改后重新发送的方式。

（2）仿冒，攻击者通过技术手段仿冒合法传感器直接发送定制的感知数据给物联网系统，例如更换传感器为攻击者特制的同型号传感器或直接通过逆向通讯协议直接发送不存在的伪造数据包等。

1.2.3.感知终端设备/网关安全威胁分析

感知终端设备/网关设备因为需要进行运算，通常具备 MCU 或 CPU，大多数采用了 RTOS、Linux 或 Android 等通用操作系统，但又因技术、成本、硬件性能等多种因素制约使得无法部署上安全能力，导致其攻击面相对较多，成为物联网端侧最易受攻击的目标。

感知终端设备/网关设备的主要威胁有以下几点：

（1）仿冒，攻击者通过仿冒合法设备接入物联网，可能对整个系统进行渗透以寻求更具价值的目标。例如，通过有线局域网组网的场景，攻击者往往可以使用 PC 轻易仿冒成合法设备接入。

（2）篡改，感知终端设备/网关通常具备一定的运算能力，本地很可能会存在敏感、重要的业务数据。加之感知终端设备/网关通常使用了通用操作系统，攻击者很可能通过系统/应用的漏洞获得设备较高的访问权限，进而对设备存储数据、发送的信息进行篡改。

（3）抵赖，感知终端设备/网关虽然通常选择了通用操作系统，但又出于技术、成本等多种原因，通常对审计安全不够重视，当攻击者攻陷设备，并通过感知终端设备对其他目标进行渗透攻击时往往会导致证据链缺失而难以追查。

（4）信息泄露，有些重要的智能物联网终端设备其业务可能涉及敏感信息的采集、存储，如果在设计开发时没有对重要数据进行加密存储，或加密算法强度较弱就可能导致设备失陷后造成敏感信息泄露；另外如果是重要基础设施，攻击者也可能通过侧信道攻击分析芯片运算时电磁辐射变化获取敏感信息，所以感知终端设备/网关在设计时也应当根据业务重要性考虑应用电磁防护手段。

（5）DoS，攻击者通过 DoS 攻击目标对象迫使业务中断，例如通过 DoS 迫使某关键基础设施停止服务；但近年来攻击者更多的通过技术手段如僵尸网络，将海量物联网设备武器化，使其成为对特定目标发起 DDoS 的武器，典型代表是 2016 年的 Mirai 病毒导致美国大面积断网事件。

（6）提权，感知终端设备/网关设备的系统、应用因业务需要通常会保留一些对外接口，从而使得攻击者有可能利用相关漏洞获取超出预期的访问权限，进而达到访问敏感数据甚至获取设备的完全控制权。

1.2.4.数据传输中的安全威胁分析

由于物联网的网络异构特性，攻击者能够在数据传输过程中找到合适攻击点的概率大大增加，通过分析在数据传输过程中可能发生的安全威胁如下：

（1）仿冒，攻击者可能通过技术手段如数据重放或伪造数据包仿冒成合法的控制端或感知设备，与其他接入物联网系统的设备进行信息交互从而达到自己的目的。例如，有安全研究员通过逆向分析自己购买的某智能家电与云端服务器的通讯格式而实现了反射式攻击，成功仿冒控制端对全网同型号家电发送了控制指令。

（2）篡改，攻击者可能通过技术手段修改物联网中传输数据的内容，从而达成自己的目的。例如在网关与云端传输路径上对安防系统的重要数据进行监控，并篡改告警信息使得安防系统认为环境仍然安全，从而可以纵容实施非法行为。

（3）信息泄露，信息泄露通常比篡改数据的攻击成本低很多，并且危害更大，攻击者可以通过中间人攻击对加密数据实现破译，所以物联网数据传输应当考虑链路层完整性检测机制。

（4）DoS，攻击者可能通过 DoS 攻击使得关键通讯节点拒绝服务从而阻断数据传输，这类低成本的攻击最为常见。

1.2.5.云端安全威胁分析

云端安全威胁有以下几点：

（1）篡改，攻击者可能通过接口、服务或系统漏洞直接对数据存储中的特定数据实现非法篡改。

（2）抵赖，攻击者可能通过提权或漏洞使得自己对云端数据或基础设施的恶意操作无法被记录或对记录进行手动删除，从而导致攻击行为难以被发现或难以溯源。

（3）信息泄露，攻击者可能通过接口或系统漏洞实现超出授予权限的访问，实现对敏感数据、重要数据的访问。

（4）DoS，云基础设施、云端服务直接影响物联网业务稳定性，攻击者偏好采用 DoS 或 DDoS 这种低成本的方式阻断系统对外服务，对服务所有者造成直接损失。亦有可能实

现对云基础设施的渗透，控制后将云基础设施变成对外 DDoS 的攻击源，而一旦大带宽、高性能的云基础设施被作为攻击源，其影响将更为严重。

（5）提权，攻击者可能通过接口、服务或系统漏洞实现超出授予权限的访问，甚至实现对云基础设施的完全控制。

1.2.6.应用安全威胁分析

（1）仿冒，攻击者可能通过逆向应用与后台系统的接口通讯，并通过专用工具仿冒合法身份，实现与系统的交互，达成攻击目的。

（2）篡改，攻击者可能通过应用自身或接口漏洞实现数据的非法篡改，如通过 SQL 注入等手段篡改管理员密码而获取管理员权限。

（3）抵赖，攻击者可能通过漏洞使得自己恶意操作无法被正确记录，从而导致攻击行为难以被发现或溯源。

（4）信息泄露，攻击者可能通过接口或系统漏洞实现超出授予权限的访问，实现对敏感数据、重要数据的访问。

（5）DoS，攻击者可能对应用接口进行针对性拒绝服务攻击，或通过技术手段破坏应用接口配置以使得应用后台服务无法正常工作。

（6）提权，攻击者可能通过接口或服务漏洞实现超出授予权限的访问，如通过应用接口远程执行漏洞获取后台系统权限。

2.物联网安全关键技术

物联网面临很多的安全风险，如果处理不当，不仅会造成敏感信息泄露、设备劫持，更有甚者会危害人身安全。目前很多物联网系统缺乏体系化的安全设计，如智能摄像头有Web 访问接口且配置弱口令；智能建筑中的 KNX、ZigBee 协议如果没有安全设计极易被外界入侵；部分共享单车品牌采用蓝牙接口开锁，极易破解；部分智能烟感设备硬件调试接口没有关闭，可以被访问内部数据，进而控制云平台进行恶意告警。再如国内部分智能表类计量系统，大部分数据采用明文传输，也没有严格的认证鉴权控制。用户在建设物联网系统时，首先应该考虑的就是安全问题，但目前的物联网系统大多仅采用一些基本的安全技术，如数据加密、防火墙等，缺乏体系化的安全设计，包括分析所有可能的攻击以及对应的安全措施等，使得整个系统安全存在较大的风险。

同时，物联网安全与传统的计算机信息系统安全相比，有两个难点：

(1) 复杂的部署环境和网络结构。如智能电表系统部署在千家万户，智能手环随身佩戴，智能车载终端随车移动，中间经过各类网络如蓝牙、RF、PLC、运营商网络等。

(2) 受限的计算和网络资源。很多物联网场景中传感器、终端以及部分网关的资源往往非常有限，包括计算、存储及能源，难以运行复杂的安全协议以及部署安全Agent。网络带宽也很有限，很多本地网络运行在几十 Kbps 共享带宽下。

因此，本白皮书将在第二章详细描述针对物联网安全的关键技术，最后一章结合物联网的一些典型应用场景给出具体的安全方案建议。读者可以根据自身情况，基于实际场景中不同的安全要求和资源要求对这些物联网安全关键技术进行选择。

2.1.芯片级安全技术

随着嵌入式技术的发展，物联网设备得到普及。而物联网的硬件基础是超大型集成电路或者芯片，这些芯片决定了物联网设备如何运行，如何处理数据。物联网设备为生活带来便捷的同时，也带来了困扰。当物联网设备遭受攻击时，它可能会泄露个人隐私或商业机密，甚至可能造成大规模的网络瘫痪。而且由于物联网设备本身计算资源有限，系统和硬件高度定制化、不通用、以及网络传输速率和工作环境等限制，难以部署传统的安全防护措施。

针对于物联网设备的安全问题，芯片级的安全技术是不错的解决方案，芯片级的安全技术包括可信平台模块（TPM）、安全启动（Secure Boot）、TEE、内存安全以及侧信道防护等等。这些芯片级的安全技术具有从根本上解决物联网安全问题的能力，芯片级安全技术软硬结合的防御措施，使攻击者难以窃取数据，窃取了也读不懂、读懂了也篡改不了。芯片级安全技术是物理安全的发展方向之一，目前越来越多的芯片厂商在设计的芯片中增加了安全机制，如 TrustZone，同时国际上也成立了可信计算组织 TCG（Trusted Computing Group），以推动安全技术的发展。

2.1.1.可信计算与 TPM 芯片

可信计算是一项由可信计算组织 TCG（Trusted Computing Group）推动和开发的技术。可信计算通过保证计算机操作系统和引导程序的完整性，来保障系统和应用的行为可以按预期执行。所以防篡改是可信计算的核心目的之一，通过基于硬件的安全芯片来校验系统和引导程序的完整性。

2.1.1.1.可信计算的存在背景

物联网是建立在传统互联网上并将海量的 RFID 设备、传感器等终端设备通过互联网连接在一起的终端网络。物联网通过终端设备感知环境信息，并通过物联网将信息进行收集、分析和处理，提取能为上层应用服务的数据信息。物联网环境中，传感器、节点终端等多为嵌入式环境，其系统多样性、计算能力、性能、可使用资源差别巨大，传统的防护手段已经无法解决当前物联网设备所面临的安全问题。

当前大部分信息安全系统主要是由防火墙、入侵检测和防病毒软件组成，这些在计算资源有限、部署环境复杂的 IoT 设备上难以部署，而且这些手段面对越来越系统化、隐蔽化、多样化的攻击方式也逐渐捉襟见肘。在 IoT 设备上，操作系统的不安全配置导致应用软件的各种漏洞层出不穷，引导程序缺乏有效的校验导致恶意固件的刷入。在针对关键信息系统的攻击中，攻击往往初次发起就造成致命的后果，例如在乌克兰变电站攻击事件中，由于缺乏有效的安全手段，导致大部分地区突然停电。

在许多物联网设备上，因为计算资源和开发成本而缺少有效的身份认证。对物联网设备来说，一是用户认证，认证使用者的权限，对于智能音箱、家庭摄像头这类的设备，隐私安全尤为重要。二是设备认证，物联网设备的部署环境复杂，即使在同一个局域网内，也有可能受到恶意设备的攻击，物联网网络中的设备应该要求它们之间进行身份验证，确保攻击者无法使用隐含的信任作为进入系统的凭证。

2.1.1.2.可信计算的使用场景

在物联网设备上，可信计算技术可以用来进行系统保护，当被刷入恶意固件或网站提供修改过的升级包时，设备可以对固件或升级包进行可信校验，从而发现其中错误，并及时拒绝或阻止此类固件或升级包执行。在身份认证方面，用户信息被保存在 TPM 的可信存储区域内，只有经过授权才能读取用户信息，从而防止信息被伪造、窃取。

2.1.1.3.可信计算的机制

可信计算可以在物联网设备中建立起主动防御机制。通过链式校验和专有的可信操作系统确保完成某些操作的应用程序能够按照预期的行为完成任务。在物联网设备上建立整个可信环境，首先需要一个可信根，然后建立一条可信链，再将可信传递到系统的各个模块，之后就能建立整个系统的可信。

可信根是可信系统的底层机制，是系统可信的源头，可信根应具备密码服务功能、针对系统启动工程的度量能力和控制能力，先于其他部分启动。在 TCG 定义的可信计算中，可信根由具备密码服务功能的可信平台模块（TPM）以及系统 BIOS 中的度量代码段（CRTM）组成。TPM 为系统提供了密码服务引擎，CRTM 执行对系统的度量功能并且可以在度量未通过时实施控制。

可信链是由可信根开始，通过逐层扩展的方式实现。首先需要用可信根验证系统硬件和固件的可信性，用固件的验证机制验证操作系统引导程序的可信性，用操作系统引导程序验证操作系统安全部件的可信性，由操作系统安全部件为应用程序提供可信运行环境，从而在系统中构建一个完整的信任链条，保障应用的可信运行。

2.1.1.4.基于 TPM 可信物联网架构

早期可信计算研究主要以可信计算组织（TCG）为主，在可信计算中最核心的部分就是 TPM 硬件芯片。到目前为止，TPM 规范已经发展到 2.0。TPM 1.1b 发布于 2003 年，是第一个得到广泛应用的 TPM 规范。在此之前，TPM 已经提供如密钥生成、存储、安全授权和设备健康验证等基本功能。

当前基于 TPM 安全平台的技术有三种，ARM TrustZone、Intel TXT 和 AMD PSP。

1) ARM TrustZone

TrustZone 提供了一种能够在 SoC 上创建一个虚拟处理器的功能，从而把软硬件资源划分为两部分，一部分叫安全世界（Secure World，SWd），运行执行安全功能的可信软件；另一个叫正常世界（Normal World），运行其他的操作。安全世界和正常世界可以通过一

个叫 Monitor Mode 的模式转换。这两个执行环境被 SoC 的硬件隔离开来，保证主操作系统不会干扰安全世界（SWd）中的程序和数据。这使得用户可以在不能信任整个设备的情况下，保持对安全世界（SWd）中数据的信赖。

ARM TrustZone 技术是所有 Cortex-A 类处理器的基本功能，是通过 ARM 架构安全扩展引入的。

目前，ARM 处理器在物联网中应用最为普及，如智能手机、电视盒子、车载娱乐系统等。

2) Intel TXT

TXT 是 Trusted Execution Technology 的简称，即可信执行技术，是 TPM 2.0 的典型代表。其主要目标是通过使用特定的 Intel CPU、专用硬件以及相关固件，建立一个从一开机就可信的环境，进而为系统软件提供多种方法来实现更安全的系统以及更好的数据完整性保护。

3) AMD PSP

AMD 安全处理器是独立于平台核心处理器的、集成在 SoC 中的专用安全硬件子系统。它可以提供一个隔离的环境，一些敏感组件可以在不受其他软件影响的情况下运行。PSP 可以执行系统工作任务以及可信第三方提供的工作任务。

2.1.2.安全启动 Secure Boot

嵌入式设备的启动流程从芯片上电运行开始，首先运行的是固化在芯片内部 ROM 里的一段代码（ROM Code），然后 ROM Code 加载一级引导，一级引导加载 Bootloader，Bootloader 初始化各种硬件，之后加载并将参数传递给操作系统内核，由操作系统内核启动各种服务。在这个过程中，加载 Bootloader 和加载操作内核阶段往往容易受到恶意的攻击，如篡改内核版本、修改 Bootloader 传递给内核的参数等，或是通过硬件手段往存储操作系统内核的芯片中刷入恶意固件，以达到修改设备功能的目的。因此 Secure Boot 的机制是向物联网设备启动的每个阶段添加校验机制，在加载运行下一级之前，对下一级的代码进行安全校验，校验通过才加载运行，校验不通过则停止运行，这个机制有效的防止未经授权或恶意的修改固件，有效的保护了物联网设备的启动安全。

2.1.2.1.ARM TrustZone 中的 Secure Boot

TrustZone 中 Secure Boot 方案将加密检查添加到安全世界（SWd）启动过程的每个阶段。这个过程用于校验所有 SWd 软件镜像的完整性，从而防止运行任何未经授权或遭受恶意修改的软件。

防止恶意攻击的最简单方法是将所有安全世界资源执行都保留在 SoC 内存位置中。如果代码和数据永远不会存储在 SoC 封装之外的其他芯片中，那么读取或修改数据就变得更加困难，因为对 SoC 封装的物理攻击要比将逻辑探针连接到 PCB 走线或封装引脚困难得多。

安全启动代码通常负责将代码加载到 SoC 内存中，因此，正确地进行身份验证以避免为攻击者引入机会之窗至关重要。假设正在运行的代码和所需的签名已经在安全的 SoC 内存中，则在使用加密方法进行身份验证之前，应先将要验证的二进制或 PuK 复制到安全位置。对镜像进行身份验证然后将其复制到安全内存位置的设计有遭受攻击的风险，攻击者可以在检查完成和进行复制之间的短窗口期中修改镜像。

2.1.2.2.AMD Secure Boot

AMD 在特别的加速处理器(APU)中内置了专属的安全处理器。这套安全处理器是基于 ARM TrustZone 架构的，它运行于硬件之上通过将 CPU 分割为两个虚拟的“世界”来建立安全环境。保密任务将运行于 AMD 安全处理器（即“安全世界”）中，而其他的任务则以“标准操作”方式运行。这样确保了敏感数据的存储和可信应用程序的安全运行。

2.1.2.3.具体技术方案

Secure boot 的解决方案有很多，国内其中一种 Secure Boot 的解决方案是系统软件采用签名认证的方式，在设备出厂前对设备操作系统的 Image 文件进行签名认证，并将基于公钥的 Hash 值写入芯片的一次性可编程模块。由于不同文件计算得到的 Hash 值不同，采用 Secure Boot 方案的设备每次启动时都会先校验系统的 Hash 值，即和芯片内的 Hash 值进行比较，然后对签名 Images 的逐级校验，实现从设备芯片到系统软件的链式校验过程，很好地避免设备出厂后没有得到客户签名认证的非授权操作，从而保护了设备中原有的操作系统和软件版本。

该 Secure Boot 技术方案主要分为三个部分：镜像签名、安全引导程序、镜像下载和上传。

镜像签名是通过公钥加密算法对数据进行签名，以保护数据来源的正确性。主要包含三个算法：密钥生成算法、签名算法和签名验证算法。Secure Boot 方案中的数字签名由 SHA 和 RSA 算法组成。

Secure Boot 的基本思想是从 ROM code 到 Kernel image 的多层链式校验。ROM code 利用 Hash 函数来验证 BSC 的完整性，用 RSA 算法来验证 SPL 的完整性，然后 SPL 将会验证 uboot，最后 uboot 来验证 Boot image、Recovery image、Kernel image 等。

当 Secure Boot 功能 enable 时，镜像需要签名才能下载。在下载的过程中，链式校验的任何环节验证失败都会导致这些镜像不能下载到设备中。设备启动时同样也会对这些镜像进行校验。

2.1.3.可信执行环境 TEE

2.1.3.1.可信执行环境（TEE）与可信平台模块（TPM）

可信执行环境（TEE，Trusted Execution Environment） 是 Global Platform（GP）提出的概念。与 TEE 对应的是 REE（Rich Execution Environment），所有未做防护的设备都可看成是 REE 环境，这些设备通常运行的是通用操作系统如 Linux、Android、VxWorks 等。这些操作系统会为 APP 提供完整的系统调用，应用程序可以不受限制的在内核模式和用户模式切换。因此 REE 下的物联网设备存在着许多安全隐患。设备上运行的操作系统往往是默认配置，对于网络数据包缺乏过滤，这会导致很多网络攻击事件的发生。而基于虚拟化的技术虽然可以实现软件的隔离，却无法保证硬件的安全，同时运行性能损耗较大，这对资源有限的物联网设备来说是难以实现的。而 TEE 可以在低成本的情况下为物联网设备提供保护，很好的平衡了成本和安全性。

2.1.3.2.可信环境所面临的风险

许多物联网设备操作系统通常会对上层 APP 开放所有的系统调用，每次调用都会使操作系统在用户模式和内核模式转换。在用户模式下，每个应用程序的空间是独立的，而在内核模式下，所有的用户程序共用一块内核空间，这会造成恶意应用程序攻击其他程序甚至操作系统内核。而且对于 APP 来说，操作系统作为资源调控者可以访问 APP 所有的数据，这意味着 APP 无法安全的存储密钥和其他敏感信息，因为 APP 不能保证操作系统是否可信。更何况这些通用的操作系统如 Linux、Android，代码量庞大，漏洞频发。

2.1.3.3.TEE 具备的功能

TEE 作为一种安全技术，可以为应用程序提供一个可信的环境。TEE 借助硬件保护机制，使整个可信环境和其他环境隔离开来，只对外提供安全的可供调用的接口，这样既能保证可信 APP 的运行，又能保证普通 APP 的操作不被限制。基于硬件的 TEE 在性能方面可以占用整个 CPU 的性能，TEE 可以访问所有的内存地址，普通环境中运行的 APP 只能访问自己的地址空间。在设计方面，TEE 的目标是保护敏感数据免受不可信 APP 的恶意行为，并且必须以硬件保护机制提供保护，该机制只供 TEE 使用。在加密方面通常采用 128 位的安全强度，并且可抵御一些基于硬件的攻击。TEE 的启动必须基于硬件芯片的安全启动（Secure Boot）流程启动，使控制权限由芯片上电运行的第一段代码 ROM Code 完整的传递到 TEE。基于硬件 TPM 芯片的 TEE 同时具有可信存储的功能，用于保护数据的机密性和完整性。

TEE 主要应用于移动支付、认证、数据保护等方面。主要针对安全要求比较高的物联网设备如自动贩卖机、ATM 机，移动支付等。

2.1.3.4.TEE 设备架构

TEE 是一种执行环境，可提供安全功能，例如隔离执行、受信任的应用程序（TA）的完整性以及 TA 资产的完整性和机密性。

REE 和 TEE 都利用了许多资源，例如处理核心、RAM、ROM、加密加速器等。在任何时间内，这些软硬件资源都由 REE 或 TEE 控制。部分资源的控制权可以在 TEE 和 REE 之间转移。当资源由特定的 TEE 控制时，它便与 REE 和其他 TEE 隔离，除非该 TEE 授权了访问权限。

一般而言，TEE 提供的执行空间比 Rich OS 有更高的安全级别。尽管 TEE 的安全性不如 SE，但它提供的安全性对于大多数应用和设备程序来说已经足够。

2.1.3.5.TEE 的软件实现

1) OP-TEE

OP-TEE，来自 STMicroelectronics，是 BSD 授权支持下的开源项目。OP-TEE 最初由 ST-Ericsson 开发。2013 年，ST-Ericsson 达到了 Global Platform 的认证标准，证明了 API 的表现符合预期。

2) Open TEE

Open TEE，开源实现，来自芬兰阿尔托大学（Aalto University）的一个研究项目。

Open TEE 开源项目的目标是实施符合最新 Global Platform TEE 规范的“虚拟 TEE”。虚拟 TEE 的主要动机是将其用作可信应用程序开发人员和对使用 TEE 或在其之上构建新协议和系统感兴趣的研究人员的工具。尽管基于硬件的 TEE 在智能手机和平板电脑中无处不在，但普通的开发人员和研究人员却无法使用它。尽管新兴的全球平台规范将来可能会改变这种情况，但是功能齐全的虚拟 TEE 可以立即帮助开发人员和研究人员。

2.1.4.内存安全技术

在 Linux 等操作系统运行的硬件平台上，通常会有 MMU 进行虚拟内存地址和物理内存地址的映射和转换，使运行在该平台上的 APP 只能访问自己的虚拟地址，无法访问真实的物理地址，然而这种方式也不是完美的，仍有许多攻击方式可以利用应用的内核空间进行非法访问，篡改其他进程的内存数据。

2.1.4.1.消息校验码

数据完整性校验是一种针对于随机存储器（RAM）的安全服务，即利用哈希函数计算内存数据的哈希值，再将哈希值用密钥加密生成 MAC（Message Authentication Code，MAC），这种数据完整性校验意味着可以以很高的概率检测出对数据未经授权的修改。在密码学中，MAC 就是一小段信息，或是说用于消息校验的标签。如果从计算和概率来看，攻击者不可能伪造一个消息校验码来修改内存数据，那么数据访问方就可以通过检查其是否满足 MAC 来验证数据的完整性。

2.1.4.2.内存加密技术

在用户登录计算机时，很多系统机密信息未经加密就被直接存储在 DRAM 中。通过物理访问 PC，攻击者就能锁定内存，绕过内存清除功能来重置系统，然后读取内容。这样就能提取用于驱动器加密的密钥以及存储在内存中的用户密码。

安全内存加密（SME）和安全加密虚拟化（SEV）是安全处理器上的功能。SME 提供了使用标准 X86 页表将单个内存页标记为加密的功能。从 DRAM 读取时，标记为已加密的页面将自动解密，而写入 DRAM 时将被加密。因此，可以使用 SME 保护 DRAM 的内容免受系统的物理攻击。

SEV 支持运行加密的虚拟机（VM），其中来宾 VM 的代码和数据受到保护，因此解密版本仅在 VM 本身内可用。 SEV 来宾 VM 具有专用和共享内存的概念。专用内存使用来宾专用密钥加密，而共享内存可以使用虚拟机监控程序密钥加密。启用 SME 后，系统管理程序密钥与 SME 中使用的密钥相同。

2.1.5.芯片攻击及对策

加密技术是一种有效的物联网保护机制。1998 年 Paul Kocher 等学者提出侧信道攻击技术，翻开了密码分析技术新篇章。经过网络信息技术的迅猛发展，使用身份认证和金融支付的媒介越来越多，如银行 IC 卡、网银 U 盾、电子护照、手机支付、社保卡、身份证等。侧信道技术因此备受关注、发展迅速，应用范围日益广泛。

侧信道攻击是一种硬件漏洞利用技术，攻击者通过能量变化、时序分析、电磁数据变化等技术来破解芯片中的密钥，然后对目标设备实施攻击。

2.1.5.1.密码设备

信息安全技术的核心是对信息的处理，其根本便是密码集成电路技术，物联网安全对密码集成电路的依赖越来越强，基于加密芯片的硬件解决方案已经成为保证信息安全的可靠途径。随着计算机技术的发展，越来越多的场合开始使用加密芯片，在计算机芯片组、路由器、网关、智能电表、手机中几乎都实现了内置安全控制模块。

芯片级的安全解决方案正成为密码设备的重点发展方向，如可信平台模块（TPM），已经集成在许多计算机的主板上。新型的安全芯片存储了计算机的验证信息，包括计算机的安全、加密和密码管理等信息内容，将这些信息锁定在计算机的状态中，保证这些信息不被攻击者篡改。

密码学包括不同类型的密码算法，这些密码算法按照一定的密码协议可以构成不同的安全解决方案。但是所有的密码都是抽象的数学算法，只有将密码算法以某种形式实现才能形成可用的密码技术或产品。实现密码的方式可以分为软件和硬件。硬件又分为嵌入式实现、FPGA 芯片和专用芯片实现。能够直接实现或支持密码算法实现的硬件称为密码硬件设备，能够直接实现或支持密码算法实现的 ASIC 芯片成为密码芯片。

密码芯片既然涉及密码算法、密钥等信息安全的关键信息，就必然成为攻击者的目标。攻击者对其进行非法的读取、分析等，以获得有用的信息。目前已发现针对密码安全芯片的多种攻击方式如故障注入、能量分析等。

2.1.5.2.侧信道分析和对策及芯片安全

侧信道分析攻击技术按照是否物理损坏芯片来分可以分为三种：入侵式攻击、半入侵式攻击、非入侵式攻击。按照是否干扰芯片正常运行来区分，可以分为主动和被动。主动攻击的目的是使芯片工作不正常，典型的代表是故障注入攻击。被动攻击则不干扰芯片的运行，典型代表是功耗分析攻击技术。

对物联网设备进行故障注入的目的通常是使 CPU 加载操作系统失败或者是使 CPU 产生比如跳过验证等不可预知的动作。与被动攻击不同的是，主动攻击并不需要各种检测仪器来分析设备的时钟、电磁、功耗，而仅仅只需要几根导线和信号发生器便可以实施。针对于密码芯片的侧信道攻击可以通过能量分析来获取密钥。

针对物联网设备的侧信道攻击可通过增加传感器和 PCB 板的合理设计来防御。例如现在的智能卡安全设计通常包括内嵌压电传感器，以防止毛刺导致的过压或欠压现象，时钟频率传感器则可以防止攻击者降低时钟频率来进行静态分析，同时也防止时钟毛刺攻击，光传感器可以防止打开芯片并获取芯片数据。

在对于加密芯片的安全技术中，信息的安全依赖于硬件实现和密钥存储，因此过去几年不断有相关的攻击方式被提出，以提取、克隆非易失性存储器中的数字密钥。近年来，出现了一种基于每个物理对象内在固有的，难以伪造的，独特的无序性的一种安全方法，能够很好的解决之前的安全问题。基于无序性安全性的系统分为两类，独特对象（UNO）和物理不可克隆函数（PUF）。PUF 又分为弱 PUF、强 PUF、可控 PUF、新兴的 PUF。

2.2.操作系统级安全技术

目前物联网设备虽呈现碎片化的特点，但从技术角度来看，物联网操作系统主要由各类嵌入式操作系统改进而来，包括实时 RTOS 操作系统（例如 VxWorks）与精简的通用嵌入式系统，典型应用为采用类 Linux 内核的嵌入式系统。

RTOS 系统通常应用于对处理时间有硬性要求，同时计算能力较为有限的物联网设备中，RTOS 类系统一般有两个特点：1. 其上方应用交互缺乏中间件层；2. 通常不具备文件系统。

采用通用嵌入式系统设计的物联网操作系统与各类嵌入式系统基本相似，主要区别在于其外围设备、计算资源存在限制。由于物联网设备本身体积的原因，物联网计算资源中的内存与存储空间通常较小，因此物联网操作系统与其文件系统根据业务需求也会进行压缩，并尽可能采用一体化程序。

从信息安全角度来看，目前网络攻击多针对于采用通用嵌入式操作系统，如类 Linux 的物联网设备，主要原因在于：

（1）采用 RTOS 系统的设备通常不具备文件系统，一般需要移植第三方系统或自建文件系统，相比传统的通用系统攻击难度更大；

(2) RTOS 系统相对封闭，可研究的网络安全攻击方式较少，且需要丰富的嵌入式经验；

(3) 大部分 RTOS 系统设备漏洞通常存在于协议栈或网络组件方面，利用难度大。

目前借助物联网操作系统发起攻击的安全攻击事件屡见不鲜。攻击者通过物联网操作系统漏洞获取操作系统控制权限，下载安装 Mirai 等僵尸病毒组成物联网僵尸网络（BOT），再向其它网络实体发起 DDoS 攻击已成为现阶段主流网络攻击形势。物联网操作系统由于其安全漏洞多、防护措施匮乏、安全监控缺失等安全风险，以及数量多、拥有一定的算力与网络资源，被攻击者视为网络资产黄金。因此，对于物联网网络安全的防护必须重点考虑物联网操作系统安全防护。

对于物联网操作系统安全防护，主要考虑以下几点：

1.安全设计

由于设计初期对安全性考虑不完整而引入的安全风险，是目前物联网操作系统中最为普遍的。物联网原生安全设计问题包括：弱密码、可猜测的或硬编码的密码、不安全的网络服务、缺少安全更新机制、使用不安全或过时的组件、不安全的数据传输和存储、不安全的默认配置等。因此对于物联网操作系统安全来说，早期设计阶段就引入安全理念就极为重要，重点考虑的内容应该包括：

(1) 身份标识与鉴别，妥善处理身份验证信息

对所有登录访问系统的用户进行身份鉴别，并且应妥善处理身份验证信息。设备出厂或使用前，应对系统中存在的弱口令或空口令账户进行清除或口令强度处理。如果可能，对具备 root 权限的账户采用用户名+证书方式进行验证，并严格限制用户数量，访问证书采用安全存储。

(2) 强制访问控制

设计不同安全和访问权限级别的用户等级，并对不同级别的用户可访问的资源或操作权限进行限制。

(3) 最小化权限

在用户级别上，应取消超级管理员用户类型，并按照系统特权进行细粒度划分，分别授予不同级别的用户；

在进程级别上，应确保系统只授予进程完成任务和功能的最小化权限。

(4) 安全审计

采用安全日志设计，对系统中重要的安全事件进行记录用于后续审计。由于物联网特点，设备日志应简单实用，并具备远距离定期传送的机制。

(5) 数据完整性

在数据方面，应确保各进程数据不会被非授权用户进行篡改或破坏；

在进程方面，各进程应具备相互独立性和完整性，不会彼此干扰。

(6) 可信计算

对于物联网操作系统，可通过可信计算的实施进一步提升系统的安全性。具体的措施包括：采用可信计算的硬件架构平台、TEE 等，这样即使设备的 root 权限被破解，也无法获取安全区的数据，最大限度保障数据安全。

2.安全监测与防御

图 2-1 物联网 EDR 技术

对于物联网操作系统来说，其本身多数物联网设备以嵌入式设备为主，其所使用的软件与硬件资源具有较强的限制性，往往仅能完成少量的计算工作；加之物联网设备的碎片化特点，导致物联网攻击呈现碎片化、变异快和不可预见性等多种特点，传统的防病毒机制在物联网系统中难以利用。

因此对物联网操作系统的防御应考虑轻量级手段，例如通过搜集系统中异常操作行为，通过后端分析结合基线对异常行为进行检查与干预，从而提升系统监测工作的适用性。

具体方法可以通过物联网 EDR 技术实现。一般思路为在物联网嵌入式操作系统中植入安全探针，采集安全数据，然后由后端计算能力强大的分析引擎进行分析，从而实现异常行为的发现和处理。

同样的，物联网 EDR 技术在实施过程中需针对物联网系统的特点进行以下优化：

(1) 多系统、多版本支持；

(2) 安全探针占用资源最小化；

(3) 监控数据安全传输；

(4) 自身可靠性保障。

根据物联网设备系统运行中可能存在的安全隐患，物联网 EDR 应具备以下安全状态信息采集与监控，包括：

(1) 登录监控

(2) 行为监控

(3) 文件监控

(4) 进程监控

(5) 流量监控

(6) 资源监控

3.安全漏洞修复

对于物联网操作系统来说，安全不可能是持久化的，因此系统安全修复机制对于设备自身安全可以起到及时补漏的作用。

对于安全漏洞修复，可以通过固件更新机制进行整体更新，或通过补丁修复机制进行修复。

2.2.1.双向身份认证

物联网安全的首要问题是可信，可信来自于通信双方身份的可信。对于物联网系统来说，设备的身份安全非常重要。物联网如果接入未经认证的终端会形成巨大的安全隐患，存在身份泄露、身份仿冒、终端捕获等安全威胁，具体包括：

(1) 非法物联网终端冒充合法物联网设备与服务器通信；

(2) 非法物联网终端冒充合法物联网设备与其它物联网设备通信；

(3) 非法物联网终端冒充合法服务器并诱骗其他物联网设备与其通信；

(4) 攻击者截取系统通信来获取认证信息，并伪造认证信息获取权限；

(5) 攻击者重放认证信息来冒充合法设备或服务器；

(6) 攻击者冒充合法第三方服务器去访问用户服务器并获取信息。

在实现物联网双向认证中，目前普遍存在的难点在于物联网设备的身份标识，物联网运营者需要从设备情况、业务类型、安全需求、建设成本和安全运营等角度综合考虑选择恰当的身份认证机制。

对于应用平台或云平台来说，一般采用标准的 CA 证书实现平台认证，例如标准的 SSL 证书或可认证的 X.509 证书。

物联网终端的安全防护可以在终端与后台应用之间采用双向身份认证机制实现终端与后台应用的双向身份鉴别，同时完成会话密钥协商，并利用会话密钥完成业务数据交互过程数据的机密性和完整性保护。

端到端应用安全中，身份认证用于物联网终端与物联网业务应用之间实现双向身份确认和安全会话的建立。防止假冒终端或者后台应用对真实后台应用和终端的访问，确保业务数据交互的主体、客体的可信。同时，物联网资源的严重受限使得传统的计算、存储和通信开销较大的安全协议技术无法应用，因此需要采用 SSL 双向身份认证协议。

协议的过程如下图所示：

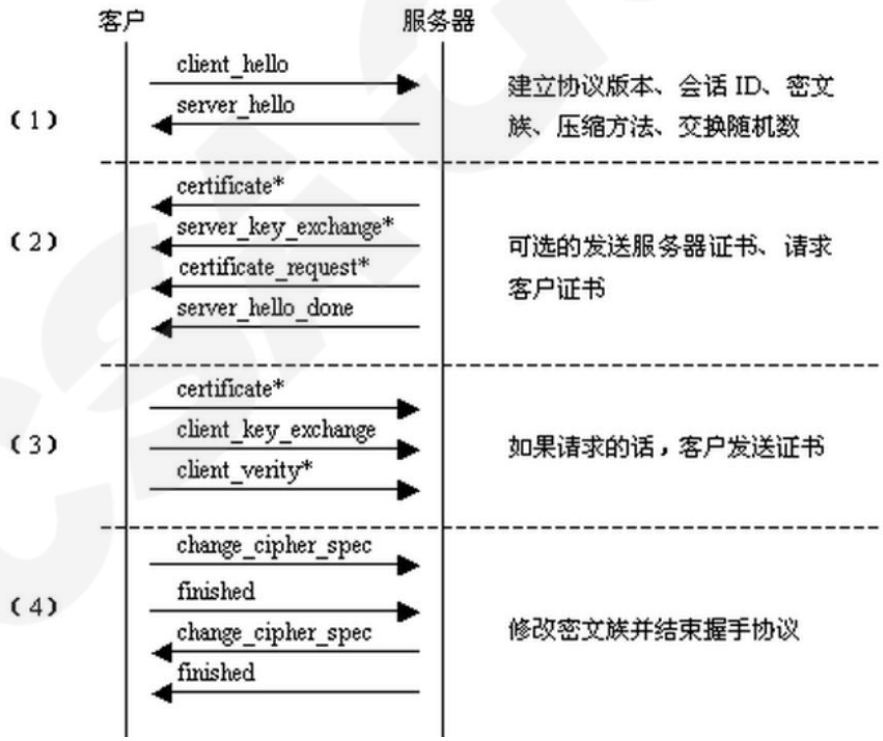

图 2-2 IoT 设备与服务器的双向认证机制

双向认证的步骤如下：

（1）客户端向服务器发送连接请求（SSL 协议版本号、加密算法种类、随机数等信息）；

（2）服务器给客户端返回服务器端的证书，即公钥证书，同时也返回证书相关信息（SSL 协议版本号、加密算法种类、随机数等信息）；

（3）客户端使用服务端返回的信息验证服务器的合法性（首先检查服务器发送过来的证书是否是由自己信赖的 CA 中心所签发的，再比较证书里的消息，例如域名和公钥，与服务器刚刚发送的相关消息是否一致，如果是一致的，客户端认可这个服务端的合法身份），验证通过后，则继续进行通信，否则终止通信，具体验证内容包括：

a) 证书是否过期；

b) 发行服务器证书的 CA 是否可靠；

c) 返回的公钥是否能正确解开返回证书中的数字签名；

d) 服务器证书上的域名是否和服务器的实际域名相匹配；

（4）服务端要求客户端发送客户端的证书，客户端会将自己的证书发送至服务端；

（5）验证客户端的证书，通过验证后，会获得客户端的公钥；

（6）客户端向服务器发送自己所能支持的对称加密方案，供服务器端进行选择；

（7）服务器端在客户端提供的加密方案中选择加密程度最高的加密方式；

（8）将加密方式通过使用之前获取到的公钥（客户的公钥）进行加密，返回给客户端；

（9）客户端收到服务端返回的加密方案密文后，使用自己的私钥进行解密，获取具体加密方式，而后获取该加密方式的随机码，用作加密过程中的密钥，使用之前从服务端证书中获取到的公钥进行加密后，发送给服务端；

（10）服务端收到客户端发送的消息后，使用自己的私钥进行解密，获取对称加密的密钥，在接下来的会话中，服务器和客户端将会使用该密码进行对称加密，保证通信过程中信息的安全。

SSL 双向认证和 SSL 单向认证的区别：

(1) 双向认证 SSL 协议要求服务器和客户端分别拥有对方的证书。

(2) 单向认证 SSL 协议不需要客户端拥有 CA 证书。

2.2.2.FOTA 固件安全升级

由于物联网操作系统存在的漏洞在不断的披露，物联网厂商也需要推出新的系统或补丁进行修复。OTA（Over-the-Air Technology)，即空中下载技术，是利用移动通信的空中接口实现对系统和应用程序进行远程管理的技术。该技术广泛应用于移动终端，特别是 Android 操作系统的设备。FOTA（Firmware Over-The-Air）物联网终端的空中下载软件升级，指通过云端升级技术，为具有连网功能的物联网设备提供固件升级服务，用户使用网络以按需、易扩展的方式获取智能终端系统升级包，并通过 FOTA 进行云端升级，完成系统修复和优化。

FOTA 的本质是固件升级，包括驱动、系统、功能、应用等的升级，和硬件没有直接关系。适用的终端范围很广，基本可以为市场上所有的终端提供升级服务, 无论对于电信运营商还是终端设备制造商，通过集群应用、网格技术和分布式服务端，能够在同一时间内处理大量用户的终端升级需求。FOTA 和 OS 的关系较密切，不同的 OS 版本需要开发不同的 FOTA 适配版本，同时通过 FOTA 模块下载的系统升级包，也要和 OS 进行密切的匹配，不但要进行硬件驱动的调试，还要进行版本的兼容测试，但这样的升级包一般由终端厂商提供， FOTA 更多的是保证将升级包下载，并且安装至终端。在智能物联网时代，FOTA 云升级将成为终端安全的重要手段。

通过空中下载的方式有效而可靠的对用户手中的物联网固件进行升级。利用这种方式，物联网厂商能够更加快速地修复物联网系统中存在的安全漏洞。 FOTA 升级都是 C-S 架构，通过客户端与服务器交互，进行升级包查询与下载。FOTA 升级有两种类型，每一种类型都有对应的用途和优势。由于物联网设备的带宽资源不足，而差分升级更适合低带宽下的升级，如下图所示：

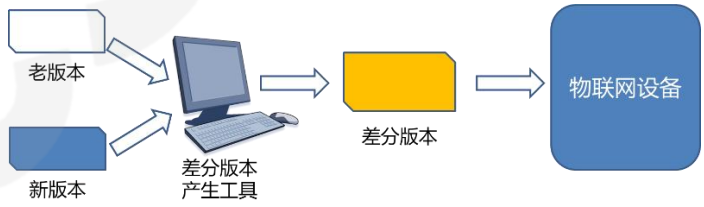

图 2-3 FOTA 差分升级

FOTA 差分升级和整包升级相比，整包的大小比较接近于整个固件的镜像，而差分包并没有特定的限制，可以和整包差不多大，也可以只有几 KB，不过通常情况下，差分包要比整包小得多，这样可以在带宽条件苛刻的情况下完成升级。

2.3.物联网认证技术

2.3.1.概述

物联网的身份认证所面临的挑战比传统互联网更大。主要表现在: 很多物联网设备应用环境恶劣，容易遭受物理破坏、篡改和信息窃取；物联网设备更新升级困难，无法及时修补安全漏洞，攻击者利用漏洞获得身份信息与其它节点进行通信；物联网设备资源和计算能力受限，资源需求较高的安全加密技术可能无法应用。因此，物联网设备在身份认证方面需要解决设备和用户基于身份伪造和泄露的攻击，以及保证认证信息的安全性。

同时，物联网由于应用场景的要求，会存在多种身份认证方式，包括设备与云/应用系统之间、节点设备与边缘设备/物联网网关之间、设备与用户之间及设备与 APP 之间。不同场景下的认证方式及安全要求各不相同。因此，物联网身份认证要综合考虑设备业务场景需求、设备自身状况、安全风险分析及安全技术匹配度等多种因素，综合选择合适的认证技术。

2.3.2.终端与云/业务平台认证

目前在智能家居、智慧安防、智能工业等场景中，大量物联网终端设备直接与云或业务平台连接通信，在这些场景中，需要为每个物联网终端分配唯一身份标识，管理平台通过校验设备标识合法性确定是否与设备进行连接通信。考虑到物联网终端存在数量大、种类多、形态复杂等特点，在建立终端与系统间的认证体系时需选择保障安全前提下适宜维护的技术。

目前常用的终端与云端业务平台的认证技术一般基于密码学的认证技术，包括对称和非对称密钥技术，从认证体系来看包括 PKI、CPK。

1.PKI 体系

PKI 是公钥基础设施（Public Key Infrastructure）的缩写，其主要功能是将证书与对应设备身份和相关的密钥对（通过为公钥及相关的用户身份信息签发数字证书）绑定，实现通信中各实体的身份安全认证，具有完整性、抗抵赖性和保密性的特点。

完整的 PKI 系统必须具有权威认证机构(CA)、数字证书库、密钥备份及恢复系统、证书作废系统、应用接口(API)等基本构成部分。其中，CA 是证书的签发机构，是 PKI 的核心。而证书是 PKI 中最重要的、最基本的数据要素，PKI 提供的各种服务(机密性、完整性、非否认等等)，都需要通过证书来实现。

物联网与 PKI 体系的结合，一般的处理方法为对每一个物联网设备签发数字证书，通过数字证书进行身份安全认证，涉及证书的选择、分发、部署、更新维护等多个环节。

证书类型的对比如下表：

表 2-1 证书类型比较

书类型	标准 SSL	自定义证书
尺寸	较大	自定义，根据标准证书进行裁剪
条件	设备具备一定的计算资源	可根据设备情况自定义资源占用
计算资源	较大	较少
成本	高	低
更新	困难	容易
应用场景	预算高、对安全性要求强的设备	对安全性要求低的设备，设备资源有限

证书分发方式如下表：

表 2-2 证书分发方式比较

分发方式	预分发	实时分发
方式	预先安装至设备中	实时分发给设备
难度	一般	困难
实现方式	预先烧录在设备或芯片中	通过内置安全模块与管理中心交互
优势	管理方便	可定义更新时间，安全性强
劣势	一般不更新，且认证材料可能存在被盗取风险	管理、更新等难度大，对设备有损耗

2.CPK 体系

组合公钥（Combined Public Key，简称 CPK）通过建立一个以种子密钥为核心的架构，将密码算法（如 ECC、 SHA1 等）加以组合解决规模化标识认证这一世界难题。

CPK 系统建立在标识公钥体制上，能够直接用标识生成公私密钥对，用户利用对方的标识，通过对外公布的种子公钥就可以直接计算出对方的公钥，计算过程即为证明过程，从而将复杂的证书管理简化为对标识的管理。

目前物联网系统中大量的设备无法通过证书方式实现身份认证，因此通过 CPK 的标识体系可以很好的解决该问题，但是需要解决 ID 仿冒、丢失及废除等问题。

现有阶段 CPK 采用预分配标识+证书等方式实现身份认证，在物联网设备中采用内嵌身份标识 ID 的硬件组件，或通过软件 SDK 集成证书等方式预设置设备身份标识 ID，由身份认证系统对设备进行身份认证，其中采取证书方式从技术角度来看与 PKI 体系基本一致。

表 2-3 PKI 与 CPK 体系比较

体系	PKI	CPK
技术原理	采用证书，由第三方机构进行认证	基于设备标识，无需第三方参与
组成	CA 机构、证书库	核心公钥算法、认证协议
优势	完整的认证过程，流程清晰可控	无需证书管理，可管理超大规模设备
劣势	证书管理难度大	ID 废除困难，不适用于无序环境认证

2.3.3.终端与设备/网关

目前在工业、智能家居等场景中，存在边缘网关+子节点设备的组网方式，例如智慧家居中智慧家庭网关可以下接门锁、温度器、智能开关等多个设备，由网关统一与云平台进行通信，网关具备一定的管理和业务能力。

设备与网关或者两个设备之间通信前，首先应进行身份认证。由于在这类场景下，设备间的通信大多采用近场通信方式，例如 ZigBee、LoRa、蓝牙等，因此在进行设备认证时，必要情况下应采用近场认证+设备认证组合方式。

2.3.3.1.近场认证

1.ZigBee

ZigBee 网络中，网关节点将建立一个信任中心，由信任中心对发起连接的子设备进行初始信息验证，初始信息一般厂商预分配在设备中的主密钥，信任中心通过验证后，将为通过验证的设备分配网络地址，并执行权限分配、密钥下发等步骤，建立安全连接和通信。

物联网设备厂商在预分配设备初始信息时，要注意信息存储和使用安全。

2.蓝牙

蓝牙是短距离射频通信的开放标准之一，主要用于建立无线个人区域网络建立。

目前商业领域包括物联网中有多个版本的蓝牙在使用，这些不同版本的蓝牙标准均提供了相关的安全模式及建议。

(1) 建立物联网设备根据对应蓝牙版本，在协商时采用最高安全级别的模式进行通信，保障通信安全。

(2) 蓝牙配对过程中由于物联网设备无屏幕（例如智能穿戴类设备），应在产品设计初期考虑无屏幕配对模式，禁止非安全连接建立；

2.3.3.2.子设备认证

对于安全需求较高的场景，可预先在平台录入子设备身份认证标识 ID，在子设备通过网关与平台进行通信前，由网关将子设备 ID 信息转发至平台进行身份认证，实现对子设备进一步身份确认。

子设备身份 ID 可以根据设备类型选择证书方式或其它标识信息。在使用传输过程中，要注意身份认证信息相关安全防护，可以采取的措施包括：

(1) 安全存储，例如安全芯片或 TPM

(2) 数据加密后传输

2.3.4.终端与用户

例如智慧电网中的 DTU、充电桩设施等物联网设备在业务运行中，会存在用户直接操作终端设备的需求，在用户对设备进行操作前应首先进行用户身份认证。目前针对用户的身份认证方面可以采取口令、多因子、生物特征等方法。

1．口令认证

口令认证方式主要是借助用户名和用户密码实现用户身份验证。由身份认证系统保存用户名和用户密码（哈希），当用户登录设备前需输入用户名和用户密码进行验证，系统会将用户输入的二元组信息和系统事先保存的二元组进行比较，作为验证用户合法身份的依据。

2．多因子认证

多因子身份认证在已有的身份认证技术上增加了辅助认证因素———例如短信验证码、身份认证、智能卡等。多因子身份认证下，用户在登录的过程中需要通过静态口令和动态口令的同时验证，只有所有认证均通过的情况下才能真正确认用户身份。

多因子身份认证方式可以划分为挑战相应方式、事件同步方式和时间同步方式三种类型。以短信验证码为例,该方式要求认证服务器在同一时间，以同一方式和同样的算法生成当下时刻合法认证验证码。与此同时，用户的验证码要和认证服务器上的验证口令在时间上保持一致，只有用户发来的验证码和服务器的验证口令码一致，用户身份才能确定。验证码还需要具有不可预测性和变化性。

3．生物特征身份认证

生物特征身份认证方式是通过提取人脸、瞳孔、指纹等人类生理特征或者特殊行为方式来作为验证途径。完整的生物特征身份认证需要经历提取生物特征、生成特征模板、测量特征和进行特征匹配等几个步骤。

在智慧门禁场景下，用户可预先录入人脸、指纹等特征数据，并以此作为合法身份认证的凭据，只有符合录入特征库下的人脸可以通过认证。通常此类验证会同时确认生物活体状态，防止通过伪造实现非法认证。

2.3.5.终端与 APP

在蓝牙场景下，例如智能门锁等设备需要通过 APP 与门锁建立短距离通信后进行数据交互，实现开门等动作。一般情况下，只有合法的 APP 可以操作与之对应的门锁，因此两者建连通信前需确认双方之间的身份合法性。

通常情况下需通过第三方管理系统维护 APP 与设备间的合法关系，例如物联网设备管理平台。设备在初期与 APP 配对时，通过预定义的唯一设备 ID 由手机 APP 向管理系统进行配对认证，认证成功后由 APP 下载对应的身份认证 ID 或证书经蓝牙传输至设备，APP 与设备间均持有互相认证的身份信息。在后续建立通信前，APP 与设备通过已下载的身份认证信息进行互相认证，从而确认身份合法性。

2.4.基于大数据的安全威胁分析

与传统 IT 设施信息安全相比，物联网系统在安全大数据方面，数据来源更分散、类型更多样；为实现对物联网系统的全面安全分析，需要从全局角度获取安全分析所需数据，包括：网络数据包、日志、资产状态、业务信息、漏洞信息、身份认证与访问信息、用户行为信息、配置信息等，可能还需要来自互联网的外部情报信息等数据。这些数据产生的速度越来越快，且数据类型涵盖结构化、半结构化和非结构化，数据量极为庞大。传统网络安全检测方法受数据源保留时间、数据分散和数据处理能力的限制，无法有效应对。

同时，物联网网络攻击手段不断更新，技术复杂性增加，僵尸网络、特种木马与蠕虫、APT 攻击等网络攻击目标性和趋利性增强，显示出长期性、多路径性、复合性、隐蔽性等攻击特征，此外由于物联网的开放性和互联性，其面临的数据安全风险也不断增加，如智能锁通过开放接口可获取住户敏感数据等，而传统网络攻击检测技术难以有效检测具有长期性、隐蔽性的新型网络攻击。

对于物联网系统的安全风险分析来说，大数据技术解决巨量的异构数据集的存储、处理与分析，解决传统网络安全风险分析的问题，其中包括：

1．解决物联网安全数据源（设备状态、流量数据、安全日志、系统日志、平台日志、APP 行为信息等）和外部威胁数据（漏洞信息、威胁情报信息等）的大规模数据的采集、预处理与存储问题；

2．解决物联网实时数据分析和大规模历史数据的离线分析问题，实现数据与网络安全态势智能洞悉，主动、弹性地应对新型复杂的威胁和未知多变的风险；

3．解决采集日志、网络流量、威胁情报、设备状态等不同类型数据的关联分析与深度检索，实现多维度、细粒度、精细化、综合化的安全分析与风险跟踪。

物联网安全大数据风险分析从过程上可分为以下几个步骤：

1. 数据源获取；

2. 数据预处理；

3. 数据存储；

4. 安全分析；

5. 威胁告警与可视化；

2.4.1.数据源获取

物联网系统中自行产生的安全数据，根据来源可分为

（1）感知层：感知层设备运行期间产生的安全数据，包括通信安全、行为安全、流量安全、数据类型、系统安全等安全数据，具体可分为加解密情况、异常流量、关键数据流向异常、嗅探次数、数据劫持、系统行为等；

（2）网络层：网络设备及安全设备相关的统计数据、日志数据、流量数据、传输日志、网络设备异常告警数据等；

（3）平台层：云安全数据、系统安全数据等；

（4）用层：接口安全数据、APP 安全日志、应用安全日志等。

其中，网络层、平台层、应用层相关安全数据可通过日志的方式直接获取；感知层由于设备的特殊性，可以通过以下几种方式获取安全数据：

（1） 规定安全日志格式、记录事件等要求，由设备自主生成并定期发送；

（2） 通过流量镜像或者 agent 等方式获取流量数据；

（3）通过探针方式或 SDK（内嵌于设备系统或外置）获取设备安全数据。

2.4.2.数据预处理

由于各类安全数据在格式、语法、字符段等方面的差异性，需要进行预处理才能进行下一步分析应用。通过采用 ETL（提取，转换，加载）操作。

ETL 全称是 Extract-Transform-Load 的缩写，即数据抽取转化装载规则。它主要完成数据源数据向数据仓库数据的转化过程。具体包含三个步骤：

（1）抽取：将数据从各种原始的业务系统或网络设备中读取出来，这是所有工作的前提。

（2） 转换：按照预先设计好的规则将抽取的数据进行转换标准化，使本来异构的数据格式能统一起来。

（3）装载：将转换完的数据按计划增量或全部导入到数据仓库中。通过 ETL 操作，能够对安全数据中不完整的数据进行补充或者删除，消除冗余数据，然后再采用规范化操作为后面的分析模块提供统一的数据源格式，同时将大量相同的攻击类重复告警数据进行聚合分类，方便后续对其进行关联分析。

2.4.3.数据存储

根据数据分析的需求，采取不同的数据处理和存储机制。

（1）批数据处理：用于网络全流量分析、日志分析等历史数据分析，一般采用 Hadoop 和 Apache Spark 批量处理架构。

（2）流数据处理：适用于处理必须对变动或峰值做出及时响应并且关注一段时间内变化趋势的数据分析，一般采用 Storm、Apache Spark Streaming、Flink 处理架构。

（3）交互式处理：需要对安全数据进行交互式查询，精细度可到秒级检索，一般采用基于 HBase、Hive、MongoDB、ElasticSearch 等 NoSQL 类型的数据存储，构建相应的数据索引，使得基于历史数据的交互式查询通常的时间跨度为数十秒到数分钟，能够支持 PB 级日志数据的秒级检索。

2.4.4.安全分析

当数据经过预处理完成后，即可进入后续分析阶段，总体上可分为行为分析、关联分析、异常检测及态势感知等多方面。

2.4.4.1.行为分析

行为分析包括感知层、平台层、应用层中设备、用户的行为分析。

1.设备系统行为分析

建立设备系统行为基线，通过实时采集的行为数据与基线对比，发现其中存在的安全异常行为，进而有效检测出即将发生或正发生的安全威胁。通过需关注的行为包括

(1) 基线状态

(2) 网络流量

(3) 文件变动

(4) 用户登录

(5) Shell 记录

(6) 数据流动记录

2．网络行为分析

网络行为分析通过监测网络流量，关注网络流量异常和偏离正常操作的行为，以增强网络安全性。一般基于源 IP 地址、目的 IP 地址、源端口、目的端口、通信协议、包数量、流字节数、涉敏数据类型、等属性构成的特征向量刻画网络用户行为，通过对网络的分析和持续自动评估，检测网络攻击、网络异常、高级威胁、不良行为和数据泄露风险。

3．用户行为分析

用户在使用物联网应用与服务时，会在系统中留下大量用户行为日志记录，包括网络流量、日志记录、审计跟踪记录、数据访问记录、业务操作记录等，通过有效分析用户行为，发现不合规的安全隐患。

2.4.4.2.关联分析

随着物联网落地应用，网络安全事件呈指数级增长，物联网安全事件相互之间往往存在错综复杂的关系。例如，小区中智能门锁安全事件由同一个攻击行为产生，有些存在因果关系，还有的安全事件是由一系列的攻击行为组成的复杂攻击，例如物联网僵尸网络发起的 DDoS 攻击。

通过关联分析技术将各种不同网络安全事件进行充分关联，挖掘其中存在的内生关系，及时发现网络攻击者的入侵行为。通过深度关联分析可实现基于历史数据的宽时间周期内多类型安全事件智能关联分析和复杂事件处理。

物联网中常见的安全关联分析包括：

(1) 安全告警关联分析：物联网系统入侵告警可能是由于其中一台设备被入侵导致产生异常流量引起的全网告警，通过有效关联分析找出病毒宿主机实现精确告警；

(2) 网络和设备关联分析：物联网 DDoS 僵尸网络组成分析；

(3) 不同领域间的安全关联分析：利用外部威胁情报、网络主机 IP 信息、告警信息之间 IP 相关性关系识别高级安全事件。

(4) 攻击链溯源分析：使用攻击图、攻击树或攻击序列的方式描述已知攻击事件的因果关系、时序关系等，将事件的关联分析转化为图模式匹配、子树匹配或字符串序列匹配等，实现网络攻击检测、网络态势评估与预测。

(5) 联动协同响应分析：使用管控设备如防火墙封堵 IP、waf 过滤异常访问等方式获取的数据与之前遭受的网络攻击进行联动分析，确保攻击和响应的闭关回馈关联，可以有效定位攻击源和处置有效性等方式来提高协同响应各数据融合效率。

2.4.4.3.异常分析

物联网异常分析要从海量数据中分析出异常事件，定位异常攻击、终端并加以处理。主要包括：

1．APT 攻击检测

物联网风险中，APT 攻击在基础设施领域及其常见。例如伊朗核设施安全事故、乌克兰电力安全事件等。由于 APT 攻击隐蔽性强，其攻击空间路径和攻击渠道不确定，大多数传统的安全解决方案无法抵御这种新型攻击。

通过采用海量网络安全数据的深度关联分析，发现以往会被忽视的策略违背与恶意软件感染，并根据 APT 攻击多个阶段的行为与正常通信存在细小的行为差异，关联检测到的看似孤立的事件，发现攻击者 APT 入侵的证据，从而有效识别出 APT 攻击。

2．恶意流量检测

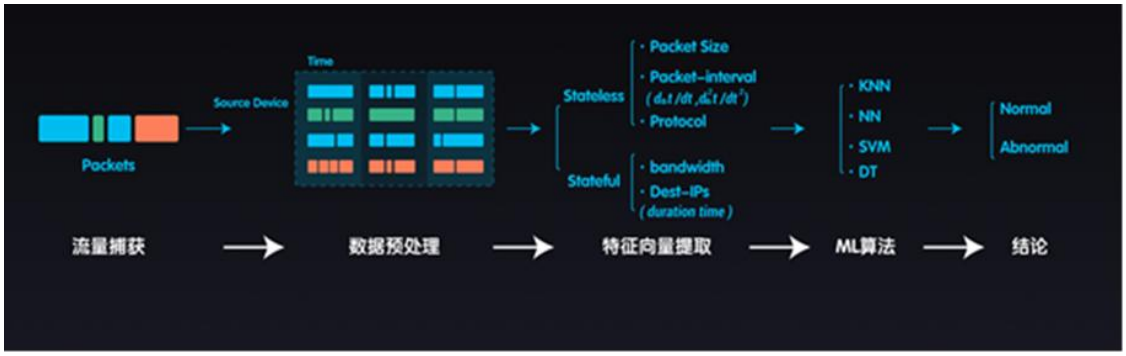

图 2-4 物联网异常流量分析过程

如何识别物联网恶意流量攻击是目前物联网安全风险防御中重点关注的领域之一。如图 2-4 所示，基于行为特征和机器学习的方法可实现网络异常分析建模和异常检测过程的自动化，通过应用深度学习的大数据分析技术对数据特征进行快速自动抽取，结合物联网流量威胁模型及算法有效识别物联网流量合法性，进而发掘物联网网络中存在的恶意流量。

(1) 特征向量的维度：正常流量与攻击流量的数据包大小对比、正常流量与攻击流量传输间隔对比、正常流量与攻击流量的一次求导、正常流量与攻击流量的二次求导、正常流量与攻击流量的协议分布模型对比、正常流量与攻击流量的网络带宽对比、正常流量与异常流量的源 IP 对比。

(2) 选取理由：选择流量监控技术可以快速检测出系统中隐含系统中的 TCP、UDP 流量攻击，记录异常流量的目的地址、目的端口、源地址、源端口等详细信息，做到可见、可溯。

2.4.5.安全可视化

安全数据可视化可以帮助安全运营人员快速直观洞悉数据背后隐藏的信息，提高对物联网系统的安全管理水平，对物联网进行整体安全态势分析。

网络安全可视化可采用数据可视化图表、地理分布、动态数据、实时告警、安全威胁情报、响应联动等建立物联网安全可视化感知体系，进而帮助运营管理人员对安全实现可见、可知、可管与可控。

2.5.物联网轻量级加密技术

在物联网通信过程中，需保护数据的机密性、完整性、可用性和不可否认性。这个要求需贯穿物联网感知信息采集、处理、传输、应用全过程。

由于物联网本身的特点，传统互联网采用的安全保护机制在物联网环境下不再适用。尤其是物联网数据通信过程中，由于不安全的数据通信会导致物联网设备隐私泄露、指令劫持、数据破坏及 OTA 升级异常等情况，造成极大的问题，所以物联网通信需采取恰当的安全防护机制确保通信安全。

从通信加密的角度来看，物联网系统的传输加密应遵循以下原则：

(1) 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；

(2) 通过数字签名等技术确保数据的完整性；

(3) 加密算法应采用公开的算法，具备一定的安全强度；

(4) 加密密钥应采用合适的方式进行协商或更换。

加密技术选择

对物联网设备来说，应在考虑安全需求、设备资源、业务要求和成本等情况下，选择采用合适的加密方式，包括：

1．证书加密

采用证书方式进行加密适用于计算资源相对冗余的物联网设备。采用证书方式通常与身份认证相结合，例如 SSL/TLS 证书机制。

2．无证书加密

对于资源有限的物联网设备，证书方式可能无法直接应用，因此需要采取无证书加密措施。目前主流的无证书加密措施为在设备的 MCU 中部署加密模块或内置 SDK，模块或 SDK 与密钥管理系统进行交互获取密钥，实现通信加密。

3．新型 SIM 卡加密

SIM 卡加密适用于采用运营商网络进行通信的物联网设备。这种方式有别于传统的 SIM 卡，是由 SIM 嵌入安全芯片或通信模组组成的一体式安全方案，厂商仅需购买全套产品即可实现安全传输，无需考虑相关技术细节。缺点是数据一般需通过运营商物联网平台转发。

4．轻量级加密

采用对标准加密算法的裁剪或改进，在不大幅降低加密算法安全性的情况下，保持加密算法的安全性。

目前主流加密算法包括：

(1) AES

高级加密标准（英语：Advanced Encryption Standard，缩写：AES），在密码学中又称 Rijndael 加密法，是美国联邦政府采用的一种区块加密标准。AES 算法包括五种模式：ECB、CBC、OFB、CTR 和 CFB。密钥长度支持 128、192、256 位等。AES 算法运算速度快，对内存占用低，适合安全性要求不高且资源有限的物联网设备。

(2) RSA

RSA 是目前使用最广泛的非对称密码体制，它包括一对公私钥对。RSA 算法既能用于加密，也能用于数字签名。RSA 的密钥长度通常为 1024 位及以上，因此其具备极强的安全性，但是对设备的资源占用有一定的要求。RSA 算法一般与证书联合应用，其适用于对安全性要求较高且资源充足的物联网设备，用于设备身份认证和数据加密传输。

（3）SM2

SM2 算法由国家密码管理局于 2010 年 12 月 17 日发布，是我国自主设计的公钥密码算法，基于椭圆曲线密码机制。SM2 算法与 RSA 算法一样，是一种非对称加密算法机制，一般用于设备身份认证和数据保护。

（4）SM4

与 AES 算法相似，国密 SM4 算法是一种分组加密算法，是我国国家密码管理局发布的商密算法。SM4 算法密钥长度为 128 位，可用于设备数据加密保护。

在资源受限的物联网终端设备上，因其计算能力、存储能力（包括 MCU、RAM 与 ROM）都非常有限，因此在物联网终端设备上的加解密不能完全照搬互联网上的算法套件，如 TLS1.2、TLS1.3、AES256 等，而建议使用轻量级密码算法套件。

轻量级加密技术在物联网安全架构中作用的范围，如图 2-5 所示，粗线条的部分就是适合轻量级密码技术的通道，即从物联网终端到物联网云平台或从物联网终端到物联网网关的部分。

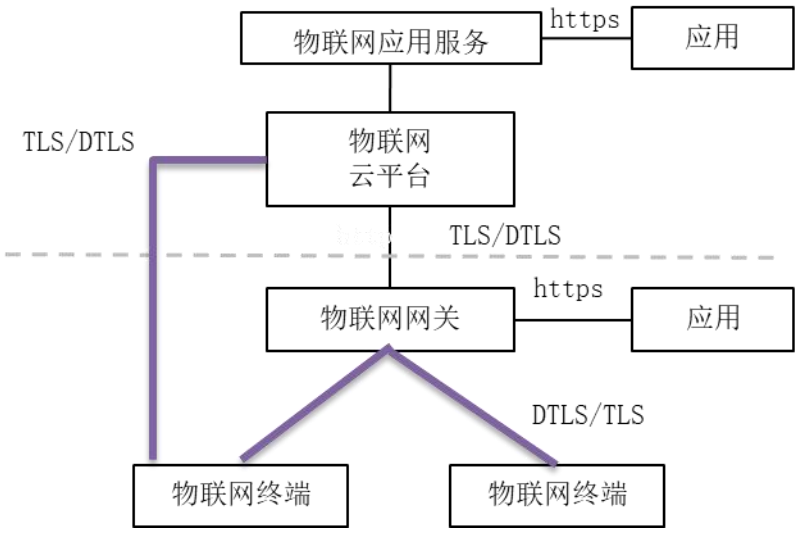

图 2-5 轻量级密码算法 IOT 应用方案

同时，为了让使用轻量密码算法的终端设备能和物联网网关、物联网平台进行通信，需要在物联网网关和物联网平台上使用的 OPENSSL 库里集成轻量级密码算法套件，实现

互联互通，轻量级密码算法套件作为该库的可选项实现，当使用轻量密码算法的终端节点和网关、平台进行通信时，网关和平台就使用相应的轻量密码算法套件来进行加密通信。

嵌入式设备和物联网设备同样面临资源受限的问题。MBED TLS 是专门为了嵌入式设备而开发的一个 TLS 协议的轻量级实现，其旨在令低性能的设备也能流畅运行 TLS 协议；其 API 的实现旨在简单易用。MBED TLS 是为嵌入式设备而开发，但它也能被用于其他各种平台，因此也常常被用作 OPENSSL 的一个轻量级替代，能够在物联网上得到较好的应用。在实际使用中，可以将密码算法套件集成到 MBED TLS 库里，再根据场景需求裁剪 MBED TLS 库的大小满足终端设备的资源需求，灵活使用，减少代码的体积，提升运营速度。

DTLS：即 Datagram Transport Layer Security，面向无连接的传输层，如 UDP。TLS 不能用来保证 UDP 上传输的数据的安全，因此 Datagram TLS 试图在现存的 TLS 协议架构上提出扩展，使之支持 UDP，即成为 TLS 的一个支持数据包传输的版本。

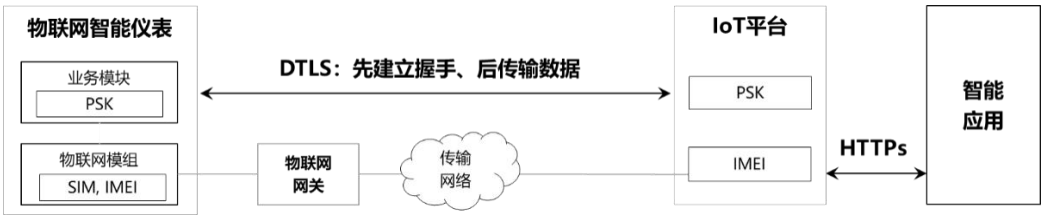

图 2-6 DTLS 物联网加密通信

NB-IoT 终端和应用在传输层一般采用无连接的 UDP，相应地，安全协议也采用 DTLS 进行如下操作：

（1）PSK 由模组厂家生成，并预置在终端仪表和物联网平台中；

（2）在 DTLS 握手过程中，终端和物联网平台校验 PSK 的一致性，从而验证双方身份，并派生 PSK 会话密钥；

（3）在 DTLS 数据传输过程中，应用层的报文，应用 PSK 会话密钥，进行加密和完整性保护。

2.6.物联网安全管控技术

2.6.1.密钥证书管理

2.6.1.1.密码基础设施

密码基础设施是物联网安全的基础，密码基础设施的建设应符合国家密码管理局相关标准和规范，并参考国家相关职能部门指导意见，整体规划和设计的密钥管理和密码应用类产品。密码基础设施利用密码技术保障密钥全生命周期的安全，满足以对称密钥体系和非对称密钥体系为主的物联网安全密钥管理服务需求。

密码基础设施包括以下内容：

(1) 加密机或加密机集群，实现本地或云端的密钥存储与密码运算功能；

(2) 密钥管理与发行系统，实现系统的密钥管理与密钥初始化，以及对终端的密钥管理与发行功能；

(3) 终端安全元件（Secure Element），实现终端的密钥存储与密码运算功能；

(4) 密码服务云及密码模块接口 API 及 SDK，其中密码服务云为物联网应用系统提供数据加解密服务，为传输安全提供加解密及认证相关的密码服务，为物联网安全网关及跨域安全提供密码服务；密码模块接口 API 及 SDK 为物联网终端设备提供访问终端安全元件的方法与接口。

密码基础设施遵循平台化、组件化、对象化、模板化于一体的原则，实现多元化的密钥管理模式和需求。密码基础设施提供物联网第三方系统和设备接入规范，便于第三方系统能够顺利接入，接受统一管理和监控。

2.6.1.2.密钥管理

物联网所有的安全机制当中，密钥系统是信息与网络安全保护的关键。由于物联网设备资源有限的特点，其通信密钥管理要求更为严格。在设计物联网密钥管理过程中，要求密钥管理系统需要适应物联网系统的网络环境，也需要适应整体网络运营管理。

密钥是加密技术的关键信息，而对密钥进行管理就被称为密钥管理，包括信息加密、解密等。密钥管理过程包括从密钥的产生到密钥的销毁的各个方面，一般可分为密钥生成、密钥分发、密钥存储、密钥更新和密钥销毁。

1．密钥生成

在进行生成密钥时首先要确定密钥的类型和长度。

目前主流算法的标准密钥长度可以避免穷举攻击推算出密钥。但是结合物联网设备本身的特点，如果密钥长度过长，会造成密钥空间过大，导致加密解密时计算量的增加。

对于物联网场景下的密钥，应根据设备情况选择合适的密钥算法，避免简单密钥。

目前主流的加密算法有对称算法和非对称算法。

(1) 对称算法

对称密钥采用相同的密钥对数据信息进行加密和解密操作。目前使用广泛的对称加密算法包括 AES 算法(高级加密标准算法)和我国自主研发的 SM1、SM4 等算法。

(2) 非对称算法

非对称加密算法需要两个密钥：公钥和私钥。公钥与私钥是一对，如果用公钥对数据进行加密，只有用对应的私钥才能解密。目前使用广泛的非对称加密算法包括 RSA 算法、ECC 算法(椭圆曲线加密算法)和我国自主研发的 SM2 等算法。

2．密钥存储

密钥存储包括设备密钥存储和集中密钥存储两种方式。

设备密钥存储：

(1) 安全硬件模块：采用安全芯片、安全 TPM、安全 TEE 等硬件保护密钥存储安全，例如国密 SM1 安全芯片。

(2) 安全软件模块：安全模块或第三方安全 SDK，由软件模块对密钥进行安全存储，通过接口调用对数据进行加解密。

(3) SIM 卡：运营商直接将密钥存储于 SIM 卡中，实现密钥保护。

集中密钥存储：

(1) 安全硬件：如加密机、硬件加密系统；

(2) 自建密钥中心：自建密钥中心存储密钥要保证密钥的安全性，例如采用加密、加盐哈希等方式保护密钥安全。

密钥存储同时应考虑分量、密码信封、保险箱机制等对密钥自身保护和管理措施。

物联网安全与认证体系中的密钥需按安全域进行密文安全存储。根据安全级别，平台端采用集中密钥存储，存储于加密机或专用安全密钥中心，终端采用设备密钥存储，存储于安全芯片或可信存储区。除此之外，密钥存储载体需具备访问控制、可销毁等特性，以保证使用中和使用后的密钥安全

3．密钥下发

密钥下发是指密钥生成后下发至设备端的过程，一般采用密钥预分配，密钥后分配及混合模式。

密钥预分配是指密钥在设备出厂前即灌装在设备中，例如存储于设备安全芯片或安全模块中，一旦设备联网可以直接通过密钥进行通信。这种模式一般应用于采用安全芯片或SIM卡方式的设备中，预分配的密钥一般禁止硬编码在设备的程序中。在一些场景中，预分配的密钥只是用于设备交换真实通信密钥时加密使用。

密钥后分配指密钥在设备由中心验证身份后分配，一般与身份认证体系关联。设备中的安全模块需具备与中心交互的能力，通过验证后，管理中心下发与设备身份绑定的唯一密钥至设备，该密钥用于后续通信加密使用。

4．密钥更新

为保证密钥的前向性安全，在一些场景下需要对设备密钥进行定期更新。

密钥更新机制可以与会话机制相绑定，例如设置安全会话有效期，一旦设备会话到达有效期后，设备必须重新发起身份认证请求，请求通过后由中心下发密钥用于下一个有效会话期的数据加密。通过以上的手段有效防止黑客在极端可能性下破解设备密钥，导致前向数据破解和泄露。

5．密钥销毁

要防止密钥被穷举破解，需要设置密钥有效期，但是太过频繁的密钥更新有可能造成设备性能和流量损耗。因此需要根据业务场景设定合适的密钥更新有效期。在密钥有效期结束且无需归档需求时，需要对不再使用的密钥进行正常销毁，销毁的关键要求在于任何人无法以任何方式重新获得被销毁密钥的任何信息。在密钥保护的机密信息泄露或者面临极大泄露风险的时候应立即对密钥进行应急销毁。

6．主要密钥类型管理说明。

物联网安全体系的密钥类型图3所示。

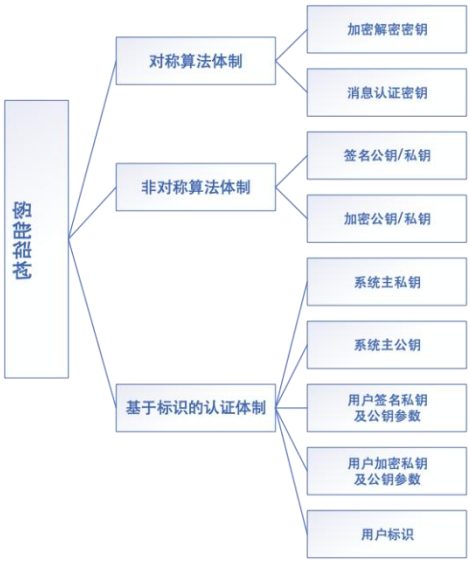

图 2-7 物联网安全的主要密钥类型

密钥管理系统根据密钥用途将系统所管理的密钥分为以下两类：管理密钥和业务密钥。说明如下：

管理密钥用于保护智能终端的发行安全和远程管理安全，由安全平台生成，保证密钥随机性和所需的关联性（例如：与用户标识绑定等）。初始的管理密钥在安全芯片中进行初始化时，由密钥管理系统统一生成管理密钥，并灌装至可信区或安全芯片中。更新的管理密钥在分发过程中，由之前的管理密钥进行安全保护。终端侧的管理密钥存储在可信区或安全芯片中；平台侧的管理根密钥或主密钥由平台安全存储。

业务密钥用于保护业务应用的安全。业务密钥包括签名密钥和加密密钥，签名密钥在密钥管理系统的控制下，由终端的安全芯片本地生成，私钥保存在安全芯片中；加密密钥可由密钥管理系统生成，私钥安装至安全芯片中。业务密钥基于管理密钥建立的安全管理通道传输，能够远程安全分发，并保证机密性和完整性。终端侧的业务密钥存储在安全芯片中；平台侧的业务密钥存储在业务平台中，或由安全平台托管。

2.6.2.IoT 平台安全管理

在物联网设备方面，需要一个能够随时承接、汇聚物联网产品厂商的端到端互联互通平台。借助该平台，物联网产品操作的安全技术和流程就能够无缝地嵌入到每一个环节，从物联网终端设备及其嵌入式组件，到多形态网络，再到用于控制最终应用产品的移动终端应用。为了在物联网设备中实现端到端安全，作为无缝集成承接以及汇聚的平台安全至关重要。在 IoT 平台安全构建方面，要重点明确以下几个方面的支持和要求：

（1）数据安全：数据存储的冗余支持，数据访问管理流程，数据传输（包括云主机之间数据传输和数据中心之间数据传输），数据删除管理（当删除数据，保证这些数据不会再被恢复和使用）、物理安全（数据中心访问、物理磁盘访问、USB 访

问和网络嗅探的控制）。

(2) 网络安全：租户间的网络流量相互隔离。

(3) 云堡垒机：针对云主机、云数据库等运维权限、运维行为进行管理和审计的工具，通过账号管理、单点登录、访问控制、行为审计等模块解决虚拟资源运维问题。

(4) 数据中心安全：遵循 ISO 2700X 系列规范的安全设施及管理流程（机柜安全、读卡器管理、7*24 监控等机制）。

(5) 安全测试：支持安全渗透测试和应急响应演练。

2.7.物联网安全测试技术

2.7.1.硬件接口安全测试技术

通常为了便于终端维护，设备生产厂商会预留相应的硬件或者软件调试接口，以便于进行运维过程中的本地调试或者远程调试。如果能在硬件层面实施主动篡改保护功能，就可对终端内部各硬件模块和物理接口进行一定程度的安全保障。但是基于成本考虑，大多数物联网智能终端不具备如此高强度的安全保护手段，也可能没有任何保护措施，这意味着攻击者可以很容易地访问终端的内部硬件，接触到预留的硬件接口，例如 USB 接口、JTAG 接口、串口、网口、芯片引脚等。

当前，多数生产厂商在预留接口上并未做安全保护，例如接口禁用、认证和访问控制等。攻击者可以利用暴露的物理接口直接访问设备，或者利用远程的软件调试接口进行非授权访问，实施系统层面的操作，更改系统或应用配置。甚至部分终端还遗留了生产调试接口或开发接口，为恶意攻击者深入物联网智能终端内部核心提供了便利。因此进行硬件接口的安全测试对于发现物联网设备的安全隐患是至关重要的。下面介绍了几种常见硬件接口的安全测试方法。

2.7.1.1.USB 接口

如今的 USB 接口功能出奇的丰富，几乎无所不能，由于 USB 当代的使用如此广泛，所以 USB 设备也就成为了恶意程序传播的重要载体。USB 设备存在很大的安全风险，可能造成病毒感染、数据泄漏、任意代码执行等。

针对这些安全风险，有以下几种安全测试技术：

（1）模拟 HID 人机设备（例如键盘鼠标等输入设备）对 U 盘固件进行重新编程，将虚拟键盘输入转为协议约定的字节指令集成进固件中，让主机将 USB 识别为一块键盘，并

执行事先编写好的虚拟键盘输入。USB RUBBER DUCKY 简称 USB 橡皮鸭，是最早的按键注入工具，可根据对应要求定制硬件。使用测试工具 USB RUBBER DUCKY（USB 橡皮鸭）测试终端设备是否允许 USB 接口注入键击序列。Teensy 是拥有芯片且功能完整的单片机开发系统。可模拟键盘和鼠标。经开发的 Teensy USB 设备可被电脑识别成键盘或鼠标，所以除了可以测试终端设备是否允许 USB 接口注入序列外，还可以测试是否能执行编程进去的恶意代码，价格亲民，开源性强，可和 Kali 配合使用。

（2）模拟以太网适配器，测试流量和数据包是否能被恶意劫持。可以使用 DNS Override by Modified USB Firmware 修改了 USB 闪存驱动器的固件，并用它来模拟 USB 以太网适配器，劫持本地流量进行分析。

（3）使用 USB 引导扇区，测试是否能注入程序。方法是修改 U 盘固件能够识别的系统的 BIOS，当 BIOS 访问 U 盘时，首先显示一个隐藏的 Linux 系统，然后就可以启动要注入的程序。

目前国外已有了一些针对 USB 接口 Fuzz 安全测试工具。普渡大学的 Hui Peng、瑞士联邦理工学院洛桑分校的 Mathias Payer 所带领的研究团队，通过一个由他们创建的新工具 USBFuzz 发现了不同平台上的 26 个新 USB 安全漏洞。USBFuzz 是一种专门用于测试现代操作系统的 USB 驱动堆栈的新型模糊器，由多款应用程序的集合，能够帮助安全研究人员将大量无效、意外或者随机数据输入其他应用程序。USBFuzz 计划作为一个开源项目在 GitHub 上发布。

2.7.1.2.串口

串行接口（Serial Interface）简称串口，也称串行通信接口或串行通讯接口（通常指 COM 接口），是采用串行通信方式的扩展接口。串行是指数据一位一位地顺序传送。串口一般有四个引脚 VCC、RXD、TXD、GND，可通过查看主板上的引脚，一般来说，VCC 的引脚是方形的，其他引脚是圆形的。如果串口在不断的输出数据，那么 TX 引脚的电压肯定不断在变化，可以利用这种方法探测 TX 引脚。RX 引脚的探测和 TX 引脚探测思路相同，通过不断在串口输入数据，检测引脚电压的不断变化。上面三个引脚确定后，GND 引脚就可以确定了，进一步验证可以使用电压表测量 GND 和 VCC 的电压差，无论串口输入还是输出，电压差都不会变动的就是 GND 引脚。

CommMonitor 可分析串口安全，是测试 RS232/422/485 串行端口的专业工具。该工具能监听、拦截、记录、逆向分析串行通信协议，还可以对指定的进程进行 HOOK，分析进程通信。

2.7.1.3.JTAG 接口

JTAG(Joint Test Action Group，联合测试工作组)是一种国际标准测试协议（IEEE 1149.1 兼容），主要用于芯片内部测试。现在多数的高级器件都支持 JTAG 协议，如 DSP、FPGA 器件等。标准的 JTAG 接口是 4 线：TMS、TCK、TDI、TDO，分别为模式选择、时钟、数据输入和数据输出线。

典型的 JTAG 系统是 TMS、TCK 和 TRST 连接到 JTAG 的设备上所组成的链，每个组件的 TDO 连接到下一个组件的 TDI，从而会形成一种菊花链拓扑结构。研究者们考虑在 JTAG 系统的一个恶意节点攻击其他节点或欺骗测试者，并测试恶意节点通过强行控制信号来接劫持总线的可能性，用 2 个节点同时驱动总线，观察谁会赢得控制权。研究表明，当 JTAG 总线较短时，攻击节点有很高的概率劫持总线；当 JTAG 总线较长时，由于传输线路的脉冲特征，攻击者一定能劫持总线。

2.7.1.4.网口

允许接入物联网设备网口，给攻击者网络接入提供了便利，可能被网络入侵，危害很大。这种安全测试方式是对某内/外部网段，以及尝试对另一网段/VLAN 进行渗透。这类测试通常有以下几种方法：

1.IP/端口扫描

通过对目标地址的 TCP/UDP 端口扫描，确定其所开放的服务的数量和类型，这是所有渗透测试的基础。通过端口扫描，可以基本确定一个系统的基本信息，以及可能被利用的安全弱点，为进行深层次的安全测试提供依据。一些物联网设备是通过网关接入，利用 IP/端口扫描，找出网关地址，便可测试网关是否能被控制，甚至可能控制这个网关上连接的所有设备。

2.远程溢出

这是当前出现的频率最高、威胁最严重，同时又是最容易实现的一种安全测试方法，利用溢出脚本就可实现远程溢出测试。

3.口令猜测

口令猜测也是一种出现概率很高的风险，几乎不需要任何攻击工具，利用一个简单的暴力攻击程序和一个比较完善的字典，就可以猜测物联网设备上各种应用或协议的口令。

4.访问控制绕过

测试身份认证模块，是否能利用非法用户、固定用户绕过身份认证。

2.7.1.5.芯片引脚

芯片引脚，又叫管脚，英文叫 Pin，就是从芯片内部电路引出与外围电路的接线。所有的引脚就构成了这块芯片的接口。引线末端的一段，通过软钎焊使这一段与印制板上的焊盘共同形成焊点。芯片引脚若存在安全漏洞，除可能造成敏感信息泄露外，物联网设备的安全性也会受到严重影响。安全测试方法包括故障注入、功耗分析等。

1．故障注入

故障注入的基本原理是通过暂时改变芯片的工作频率、供电电压、光照、温度等，使芯片的处理器、ROM、RAM、寄存器等部件在工作过程中产生随机错误，导致输出错误的值，通过理论分析错误的输出，可以得到芯片内部的用户隐私、密钥等机密数据。故障注入分析检测是目前 IoT 芯片安全性测评的关键方法。故障注入在实践中可以通过断路故障注入、短路故障注入、阻抗故障注入、信号幅度故障注入、信号延迟故障注入、信号占空比故障注入、信号跳变斜率故障注入，以及数据替换故障注入这些故障注入类型中的一种或者多种对硬件接口进行安全测试，可以突破接口的访问控制，得到敏感目录文件信息，获得芯片密钥等。

故障注入的强度由故障注入参数控制，若故障注入强度较小，则待测芯片可以正常工作且输出正确结果；若故障注入强度中等，则待测芯片可以正常工作但输出错误结果；如故障注入强度高，则待测芯片需要重新启动后才能正常工作。建立一套自动化故障注入检测方法和装置可以快速测评 IoT 芯片的安全性。目前，国内外现有的此类故障注入检测设备适用于通用的有 reset 复位方式的芯片。

故障注入的有关参数，主要包括故障注入范围、故障注入强度、故障注入个数、故障注入偏移时间，在上述参数区间内随机生成一个故障，然后把故障注入到芯片，随后芯片响应一个结果。芯片响应的结果可以分为四类：正常结果、错误结果、预期结果、无响应。如果芯片无响应的话，故障注入检测设备输出 reset 复位信号，芯片接收到 reset 信号后热启动。芯片热启动后，故障注入检测设备继续向芯片中注入故障，直到得到有效的错误输出响应。

2．功耗分析

功耗分析最早是由 Paul Kocher 等人提出的，由于该技术简单而有效，是所有侧信道分析技术里发展最为迅速的。其主要分析方式有简单功耗分析、差分功耗分析、相关性功耗分析、高阶差分分析。功耗分析常用的简单方法是在芯片和实际电源间串联一个小电阻，

通过测量这个小电阻上的功耗情况，即可推测出芯片内部的功耗变化，从而猜测出芯片内部的情况变化，推测和计算出芯片的密码、密钥等重要信息。

目前功耗分析技术，尤其是简单功耗分析和差分功耗分析技术已经发展得非常成熟，出现了一些专用的分析仪器仪表。

2.7.2 应用安全测试技术

在物联网设备中，常常使用 Web 应用和移动应用实现对设备的远程访问、管理、信息交互或实现某些功能的操作。物联网设备应用的功能也十分强大，存在远程代码执行漏洞的产品可能会对用户的人身安全造成影响。因此探究物联网应用安全测试技术也是至关重要的。物联网中的应用测试技术与传统应用测试技术类似，可以分为业务逻辑安全和代码安全两部分安全测试。

2.7.2.1 业务逻辑安全

物联网中应用逻辑安全测试与传统应用逻辑测试技术类似。业务逻辑安全漏洞是使用正常的业务流程中的程序逻辑设计缺陷进行攻击所造成的漏洞，一般是由于只注重实现功能，而忽略了在用户使用过程中个人的行为对应用程序的业务逻辑功能的安全性影响，比如登录验证的绕过、交易中的数据篡改、接口的恶意调用等，都属于业务逻辑漏洞。业务逻辑漏洞危害很大，一般防护手段以及安全设备如果无法防御，会造成非常严重的后果。

业务逻辑安全测试主要依靠基于应用类型的自动化扫描工具的检测，辅以人工测试，发现如任意文件上传、命令执行等传统类型的漏洞，更需重点关注业务系统的业务流程设计缺陷、业务逻辑、业务数据流转、业务权限、业务数据等方面的安全风险。在进行业务安全分析的时候，要深入了解应用的业务特点，重点分析业务部署情况、功能模块、业务流程、数据流、业务逻辑以及现有的安全措施等内容。

在安全测试中需要先识别风险点，根据这些风险点所需的安全测试技术在以下内容中列出：

1.业务环节

业务环节存在的安全风险指的是业务使用者可见的业务存在的安全风险，如注册、登录和找回等身份认证环节，是否存在完善的机制、数据一致性校验机制、Session 和 Cookie 校验机制、接口调用机制等，是否能规避绕过、暴力破解等。

2.支持系统

支持系统存在的安全风险，如用户访问控制机制是否完善，是否存在水平越权或垂直越权漏洞。系统内加密存储机制是否完善，业务数据是否明文传输。系统使用的业务接口是否可以未授权访问/调用，是否可以调用重放、遍历，接口调用参数是否可篡改等。

3.业务环节间

业务环节间存在的安全风险，如系统业务流程是否存在乱序，导致某个业务环节可绕过、回退，或某个业务请求可以无限重放。业务环节间传输的数据是否有一致性校验机制，是否存在业务数据可被篡改的风险。

4.支持系统间

支持系统间存在的安全风险，如系统间数据传输是否加密、系统间传输的参数是否可篡改。系统间输入参数的过滤机制是否完善，是否可能导致 SQL 注入、XSS 跨站脚本和代码执行漏洞。

5.业务环节与支持系统间

业务环节与支持系统间存在的风险，如数据传输是否加密、加密方式是否完善，是否采用前端加密、MD5 算法等不安全的加密方式。还包括系统处理多线程并发请求的机制是否完善，服务端逻辑与数据库读写是否存在时序问题，导致竞争条件漏洞，以及系统间输入参数的过滤机制是否完善。

2.7.2.2 代码安全

在物联网设备的代码包含了几乎所有传统应用代码类型，而且探究相对较多的是二进制代码。程序代码中存在安全缺陷，可以恶意构造的数据（如 Shellcode）进入程序，改变程序原定的执行流程，从而实现破坏或获取超出原有的权限，能够造成溢出、命令执行、代码执行等安全漏洞，可能导致设备内存破坏、系统崩溃、病毒入侵等后果。代码安全在计算机系统中占有重要的地位。针对软件源代码进行安全性分析的工具和方法大量出现，对加强软件的代码安全起到了很好的作用。然而大量使用的商业软件是以二进制代码形式存在的，这使得以源代码为分析对象的软件代码安全分析技术无能为力。二进制代码作为软件的最终表现形式，在现阶段也是很多软件的唯一表现形式。源代码安全性分析以静态分析为主，而二进制代码安全性分析以动态分析为主，除此外还有一些其他的测试技术。

在进行安全测试时，主要有以下几种技术：

1.手工分析

手工分析分为静态分析和动态调试。静态分析主要分析代码逻辑、程序路径、输入消息、文件内配置信息等等。在找到消息输入的风险点后，就可以对风险点填充各种畸形数据。其中包括超长字符串、畸形字符、边界值数据等等。根据长期的测试经验来看，其中超长字符串的效果更好。并且超长字符串一般都为堆栈溢出，该漏洞一般情况下都是可以利用的。还可以使用反汇编、汇编级调试器等逆向分析工具深入分析，如 WINDBG、IDA、OLLYDBG 等反汇编工具，找到异常原因，判断风险类型以及危害。动态调试则是利用调试器跟踪软件的运行，寻求破解的途径。动态调试的工具有 OllyDbg 和 GDB，OllyDbg 通常称作 OD，是反汇编与调试工作的常用工具。OD 附带了脱壳脚本和各种插件，功能非常强大；GDB 不是一款图形化调试器，但其功能更为强大，可谓独具特色。

2.自动化分析

自动化分析可以分析源码和二进制代码。主要有 Fuzzing 技术、符号执行和插桩技术。

Fuzzing 技术源于软件测试中的黑盒测试技术，其基本思想是自动产生和发送大量随机或经过变异的输入值给软件，一旦发生失效或异常，便可挖掘出软件系统存在的薄弱环节和安全漏洞。

符号执行（Symbolic Execution）是一种程序分析技术，它可以通过分析程序来得到让特定代码区域执行的输入。顾名思义，使用符号执行分析一个程序时，该程序会使用符号值作为输入，而非一般执行程序时使用的具体值。在达到目标代码时，分析器可以得到相应的路径约束，然后通过约束求解器来得到可以触发目标代码的具体值。通过此方法可以找出程序中可能存在的安全漏洞。

插桩就是在代码中恶意插入一段自定义的代码，从而实现程序分析，例如函数的调用信息。二进制插桩可以分为静态二进制插桩和动态二进制插桩。静态二进制插桩发生在程序运行之前，采用改写可执行的二进制文件的方法进行插桩。而动态的二进制插桩发生在程序运行时，分析代码可以被监测程序插入到被检测进程，也可以在另一个进程中执行。

源码自动化分析工具主要有符号执行开源项目 KLEE 和 coverity 等工具，源码 fuzzing 最有代表性的工具是 AFL。二进制的符号执行工具有 angr 等工具，二进制的 fuzzing 技术有很多项目是集多种技术集成的，如借助二进制插桩技术进行 fuzzing 跟踪，借助符号执行和污染跟踪获取 fuzzing 数据。源码插桩发现漏洞的项目有 google 的 Asan 工具，二进制的有 valgrind 工具等。

2.7.2.3Web 安全

物联网大部分平台都采用了 Web 接口，因此 Web 安全也是平台安全的重点。譬如，特斯拉早期被攻击正是从它的云服务作为入侵入口攻入进去的。攻击者并没有破解汽车中的软件系统，而是找到云服务的漏洞来远程控制特斯拉汽车。物联网平台要避免攻击者通过开放的云服务接口进入到平台内部，窃取数据或影响所连接的物联网设备的正常工作，有些还会涉及到用户隐私信息。

1.静态分析技术

WEB 常见的静态分析方法主要包括词法语法分析、模式匹配分析、数据流分析、补丁比较分析和模型化分析等。

2.动态分析技术

动态分析技术是模拟恶意用户的行为对 Web 应用进行安全评估，针对 Web 应用中可能存在的代码缺陷、逻辑设计错误等问题进行测试，最终发掘其中的安全漏洞。开放式 Web 应用程序安全项目将 Web 应用渗透测试分为被动阶段和主动阶段，被动阶段需要尽可能地去搜集被测 Web 应用的信息，如通过使用 Web 代理观察 HTTP 请求和响应等，了解该应用的逻辑结构和所有的注入点；主动阶段需要从各个角度、使用各种方法对被测 Web 应用进行渗透测试，主要包括配置管理测试、业务逻辑测试、认证测试、授权测试、会话管理测试、数据验证测试、拒绝服务测试、AJAX 测试等。

3.模糊测试技术

Web 应用安全的模糊测试技术的基本思想是模拟恶意用户行为，有目的地构造大量异常、非法、包含攻击载荷的模糊测试数据并提交给 Web 应用，同时监测 Web 应用的行为，判断 Web 应用中是否存在安全漏洞

很多 Web 扫描器都已实现集以上技术于一体，进行风险预测和漏洞扫描，相关的商业化的软件和工具非常多。Web 的相关安全测试类工具也是种类非常多，例如 sqlmap 是一个自动 SQL 注入工具，检测和分析 SQL 注入漏洞；Burp Suite 是用于攻击 web 应用程序的集成平台，可以漏洞扫描、拦截代理、抓包改包等。

2.7.3 通信安全测试技术

物联网的通信安全是物联网安全的基础，为传输信息的正确、可靠传输提供了保障。若通信数据被劫持篡改，导致物联网产品接收错误指令，可能会对用户的生命财产安全造

成严重危害。常用的物联网通信方式可以进行归纳总结分为三大种类：无线电通信、有线传输通信、传统互联网通信。

其中有线传输通信包含在硬件接口内，在前面章节已探讨过了，这里就不赘述了。

2.7.3.1 无线电通信

无线电通信是将需要传送的声音、文字、数据、图像等电信号调制在无线电波上经空间和地面传至对方的通信方式，利用无线电磁波在空间传输信息的通信方式。无线电通信包括移动空中通信和近距离无线通信。

1.移动空中通信

常见的移动通信有 GPRS、3G/4G/5G、NB-IoT。

GPRS（General Packet Radio Service）是通用分组无线服务技术的简称，它是 GSM 移动电话用户可用的一种移动数据业务，属于第二代移动通信中的数据传输技术，介于 2G 和 3G 之间的技术，也被称为 2.5G，可说是 GSM 的延续。

3G/4G/5G 分别指代第三、第四代和第五代移动通信技术。4G 是集 3G 与 WLAN 于一体，能够快速高质量地传输数据、图像、音频、视频等。4G 可以在有线网没有覆盖的地方部署，能够以 100Mbps 以上的速度下载，满足几乎所有用户对于无线服务的要求，具有不可比拟的优越性。5G 是最新一代蜂窝移动通信技术，也是继 4G（LTE-A、WiMax）、3G（UMTS、LTE）和 2G（GSM）系统之后的延伸。

NB-IoT 是指基于蜂窝的窄带物联网（Narrow Band Internet of Things, NB-IoT）构建于蜂窝网络，只消耗大约 180KHz 的带宽，可直接部署于 GSM 网络、UMTS 网络或 LTE 网络，支持低功耗设备在广域网的蜂窝数据连接，也被叫作低功耗广域网(LPWA)。

物联网场景下，NB-IoT 是主要采用的通信网络协议。

由于移动空中通信接口的开放性和 D2D 通信（Device to Device Communication）系统本身的特点，系统中用户可能成为恶意用户攻击的目标，例如窃听数据、散布错误信息或者侵犯隐私，甚至受到非授权用户进入。

针对以上移动通信技术有以下几种安全测试方法：

通过创建伪基站来进行中间人（MITM）嗅探 SIM 卡和后端服务器之间的流量。可以通过组合 BladeRF、树莓派和电池组，建立伪基站，就可以劫持流量进行分析。

使用 SDR 嗅探监听可以嗅探 GSM 网络的通信流量，只要调到特定频率，就可以使用捕获到无线电波。可捕获的频率范围和带宽随不同的 SDR 设备而不同。可以使用 RTL-SDR 来嗅探 GSM。RTL-SDR 是一个低廉的家用消费档次的 DVB-T USB 接口的接收机，这些 DVB-T 接收机基于 Realtek 的 RTL2832U 芯片外加一个诸如高频头而构成，是目前最低廉的 SDR 硬件设备。

2.近距离无线通信

近距离无线通信无主要有 Wi-Fi、蓝牙、Zigbee、Z-ware、IPv6/6Lowpan。因为使用了无线介质进行数据交互，那么这条无线链路可能被监听、解密、重放、欺骗、劫持。

可以使用与目标无线系统运行频率相同的监听设备对全量无线报文进行捕获。如监听 WIFI 使用无线网卡；监听蓝牙使用蓝牙嗅探设备，比如 Ubertooth、NRF Sniffer；监听 Zigbee 也可使用嗅探器，如 SmarRF Packet Sniffer；监听无线钥匙则使用 SDR 设备。

通过对无线设备代码及数据包进行逆向分析、解密，将无线报文数据通过相应的方法解密后，可以深入了解整套无线系统的运作原理，找出关键的无线指令。如果目标系统的无线通信协议没有设立有效的时间戳或随机性等防信号重放机制，那么当使用相应的无线设备截获一段合法合规的无线指令时，就可以通过将这段信号指令直接重放出来。还可以通过掌握目标无线协议的报文构成及关键密钥、校验方法等，直接构造合法的可通过协议认证的无线报文，发送给物联网设备，测试物联网设备是否对无线发送信息端有严格身份验证。

无论是移动空中通信还是近距离无线通信都需要用到 SDR（软件无线电）技术，就是采用数字信号处理技术，在可编程控制的通用硬件平台上，利用软件来定义实现无线电台的各部分功能：包括前端接收、中频处理以及信号的基带处理等等，即整个无线电台从高频、中频、基带直到控制协议部分全部由软件编程来完成。

USRP 是数款流行的 SDR 硬件中功能和应用都相对成熟的一款产品，能够支持从 WIFI 协议、ZigBee 协议、RFID 协议、GSM 通信系统、LTE 4G 通信系统到飞机通信、卫星通信等。安全工程师用它来测试、研究相关的无线通信协议。

2.7.3.2 传统互联网通信

传统互联网通信存在着多种风险，如数据破坏、数据伪装、重传、丢失、乱序和延时，甚至被入侵、被控制。常见通信方式包括 HTTP、HTTPS、WS、WSS、TCP、UDP、COAP、MQTT，甚至有的还有 FTP 等。

在测试过程中最常见的就是使用一些 BurpSuite、Fiddler、Tcpdump 等抓包工具抓取通信报文，测试是否存在明文传输通信信息。还可以截取通信报文，进行重放、篡改等的操作，测试是否存在这些安全风险。可以使用 Kali Metasploit 或一些其他网络测试工具，测试是否存在 ARP 欺骗和 DNS 欺骗漏洞等。

在使用了 SSL/TLS 的通信中，伪造的 CA 证书是能够获得客户端和服务器端信任的关键。通过这种手段捕获到通信报文，然后可以对报文内容进行分析和重放、破解加密等操作，测试客户端和服务器是否有双向认证机制。Openssl 也存在一些安全漏洞，可以使用 Kali Metasploit 或一些其他脚本工具测试是否存在心脏滴血等漏洞。

3.物联网安全关键技术应用场景

3.1.智慧家庭

智慧家庭是智慧城市的重要组成部分，利用物联网、云计算、移动互联网和大数据等新一代信息技术，将家庭智能控制、信息交流及消费服务等家居生活有效地结合起来，目的是创造高效、舒适、安全、便捷、智能的个性化家居生活。智慧数字家庭由传感器、智能设备、手机应用程序和用户网页界面等组成，涵盖家庭自动化、家庭安全、人身健康、能源管理和家庭娱乐等多个方面。

典型的智慧家庭模式如下图所示：

图 3-1 智慧家庭典型组网

在智慧家居场景下，物联网安全技术和应用的关键方向如下：

1.传感器及终端安全

传感器设备和物联网终端容易受到信息篡改等方式攻击。可以通过 Zigbee/Z-Wave 等近场通信协议，提供基于共享密钥方式的加密通信通道，实现端点和网关的安全连接，在安全性、成本、便捷性上取得较好的平衡。对于特殊的安全敏感场景，建议采用更安全的基于 PIN 的设备配对认证方式。另外，针对资源受限的物联网设备，采用专用的轻量级密码算法来替代传统的加密算法，可进一步降低硬件成本和功耗。

2.家庭网关安全

家庭网关类产品很容易被攻击导致“变砖”或成为“僵尸网络”，是安全防护的重点。家庭网关可以采取内置单独的 TPM 芯片实现安全启动。检测软件、固件被篡改和植入恶意程序的风险，可信状态可以上报到云端，实现所有网关设备安全状态的云端可视。家庭网关汇聚传感器和智能设备采集的实时信息，通过 TLS/DTLS 等安全协议传输到云端的物联网平台，保证信息传输过程中的安全性。

3.智慧家庭云平台安全

对于视频等敏感的数据，由云端统一的密钥管理系统 KMS 负责基于用户分配唯一的加解密密钥，实现云端视频数据存储的加密，只允许用户管理自己的加密数据，同时密钥管理 KMS 和加密数据存储的管理维护分离，进一步提升内控管理的安全性。云平台提供基于大数据和机器学习技术的安全分析中心，通过采集和分析各种日志、事件、流量信息，可以实现对物联联网设备状态异常、终端用户行为异常、云平台状态异常的分析，及时识别和管控针对端侧设备发起的入侵攻击、用户帐号、云平台被入侵的风险。

4.移动终端 App 安全

移动应用为消费者提供管理家庭内部智能设备的界面和接口，但仅基于帐号+密码的方式无法提供足够的安全保障，可以提供基于终端绑定的额外安全机制，降低密码泄漏带来的风险。

3.2.智能穿戴

物联网的应用场景中，和普通消费者关系最密切的包括智能家居和智能穿戴。两者面临的威胁和挑战不完全一致，产品和解决方案的形态上也各不相同，因此，安全的控制措施和关键技术有不尽相同的应用模式。

智能穿戴将个人携带和使用的设备由 1 扩展到 N，业务功能上聚焦于个人体验的进一步丰富和个人使用场景的进一步完善。智能家居则聚焦于家庭环境的感知和操作，提供不仅包括个人，还包括环境的融合体验。因此，智能穿戴的安全技术应用，应该以“人”为核心，针对穿戴设备的功能和体验，做相应的安全、隐私的保护。

常见的普通公众使用的智能穿戴设备，可以分类如表 3-1 所示：

表 3-1 智能穿戴设备分类

类型	**说明**
智能手表	手表样式的计算和通信设备。一般提供无线连接。也可能通过近端蓝牙连接等方式与手机等设备配对。提供额外的屏幕显示和信息通知。现代的智能手表新增多种传感器，提供运动追踪、血压和心率记录等功能
智能显示	包括虚拟现实（VR）、增强现实（AR）、混合现实（MR）和头戴显示（Head-up display）等
运动跟踪	一般为腕带型、胸佩型或者耳戴型。可以记录室内和户外的运动数据，如步数、跑步距离、呼吸、心率和睡眠习惯等
可穿戴相机	具备移动性和灵活性的特点。适合拍摄第一视角的视频和照片。如，可以固定在帽子上或者头盔上的小型可穿戴相机
可穿戴医疗设备	一般是指使用非侵入方式，使用传感器收集各类生理数据，以预防、检测或者诊断疾病的设备
智能衣物	涵盖范围很广，包括鞋子、袜子、头盔、帽子等。对运动竞技场景和特定行业工作（消防、建筑、交通运输）非常有用

1.智能手表：

从业务功能和安全架构上更类似于传统的智能手机等设备。相对其他智能穿戴设备而言，其计算和存储能力较强。因此，在智能手表的安全技术上，推荐类似智能手机的安全技术实现。包括：

a) 芯片级安全技术：如 TPM 芯片、安全启动、TEE 可信执行环境、设备证书等；

b) OS 安全技术：如资源访问控制、存储加密、OS 加固、网络协议加固等；

c) 数据安全技术：如数据分类保护、多因子身份认证、传输通道加密等。

此外，需要注意的是，智能手表的部分功能，如果涉及到健康类的数据和金融支付类的数据，需要按照产品使用地区适用的监管要求，做额外的安全和隐私保护设计。

2.智能显示：

智能显示类设备尚未完全普及。对其安全性和隐私保护的研究仍在进行中。但是就 AR/VR 设备功能本身已经引发了一些隐私风险的担忧。VR/AR 中的广告商完全有能力跟踪用户眼球的关注；黑客的入侵和破解将使智能显示类的设备变成智能监控类的设备；对显示内容的篡改会导致“所见未必真实”；迅速而强烈的白光和频闪是否会诱发癫痫也有争论。

综合上述的风险与挑战，在下述层面需要物联网安全技术的支撑：

a) 防入侵：OS 的加固、网络协议的加固、设备状态的态势感知；

b) 防泄密：数据传输保护；数据存储安全；多媒体加密协议；身份认证技术；

c) 防滥用：数据和应用权限机制；保证用户对数据的可控；

d) 内容安全：显示内容的安全性。比如儿童使用的 VR 设备如何防止出现色情内容。

3.运动跟踪：

随着智能穿戴设备的迅速发展，该类设备经常会集成到智能手表等其他类型的可穿戴设备中。值得注意的是，该类设备处理和传输非常敏感和私密的数据，但设备本身的安全能力比较弱（例如，可能没有 TPM 或者安全芯片）。在设计上，需要保证通过配对设备的控制或者用户的参与，以确保数据使用和传输的机密性、完整性和可用性。

在数据上传到云的场景，对于敏感数据（如心率、血压），建议使用智能设备上的认证凭据，做端到端的加密。

4.可穿戴相机

该类智能可穿戴设备更像是传统摄影或者摄像设备的小型化。在设备安全、数据安全维度，继承原有的最佳实践即可。对于部分具备实时数据上传能力的设备，在数据传输通道加密，端云双侧身份认证上，需要落实相应的安全技术。此外，流媒体传输的安全协议，需要同时考虑实时性和安全性。

可穿戴医疗设备和智能衣物两类，可以比照上述的智能可穿戴设备类型，实施相应的安全控制措施和安全技术方案。此处不再赘述。

3.3.智能抄表

智能抄表类业务包括智慧水表、智慧电表、智慧气表等业务，由于智能抄表终端是数据采集、嵌入式设备，因此容易受到攻击进行数据篡改或者个人隐私数据窃取。智能电表目前正在中国、欧洲和美国及其他地区的电力网络中大量安装。国外有研究报告表示智能抄表类业务可能导致两个方面问题：第一是隐私问题，甚至允许从计量数据中识别个人活动规律隐私，第二个是“计费问题”，即使第三方也可以轻易改变数据传输，从而可能伪造消耗的用量。

抄表类业务有以下的业务特点：

a) 计费类业务，数据篡改会造成收入损失；

b) 海量终端，成本敏感；

c) 安装在楼道，无人值守，容易发生物理接触；

d) 计算资源受限，部分场景电池供电；

e) 和人员的日常生活习惯关联。

根据业务特点， 抄表类业务的安全诉求有：

a) 防止逃费等欺诈手段；

b) 被攻击可能性多，需防范大规模恶意利用，安全防护要求低成本；

c) 需要重点防范物理攻击及进场攻击，终端安全需要规范化；

d) 传统安全机制不适合，要求轻量化；

e) 需要进行数据保护，防止造成隐私泄露。

当前基于 NB-IoT 的智能抄表物联网解决方案，如图 3-2 所示：

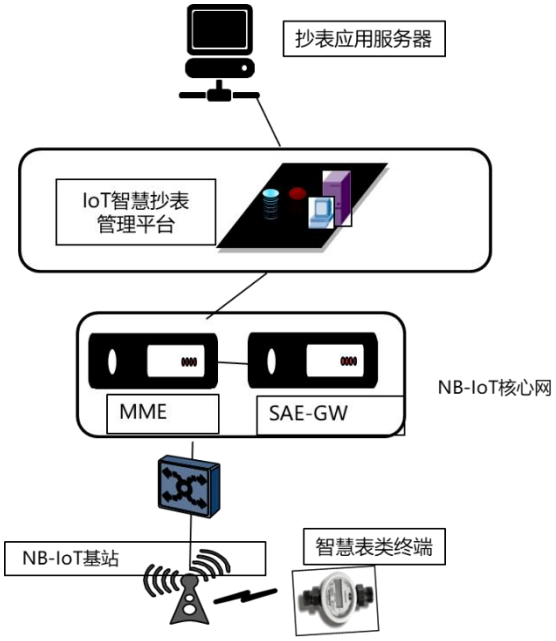

图 3-2 智慧抄表解决方案

在智慧抄表场景下，建议采用物联网安全技术和应用位置如下：

1） 抄表终端

基于 3GPP AKA 认证，保证合法设备接入合法网络。抄表终端与 IoT 管理平台之间采用 DTLS 预置共享密钥、双向认证，确保终端和 IoT 平台的合法性。抄表终端芯片内置 TPM 可信计算能力，一旦被篡改，能够进行检测并通过实现恶意设备的远程修复。一旦固件被恶意篡改，抄表终端采取 FOTA 差分升级，对终端进行修复，减少终端的安全问题。

2） 物联网云平台

通过物联网大数据安全威胁分析技术，对抄表终端上报数据异常、连接次数过多、上报内容异常等行为进行画像，确定异常的进行上报，确认后隔离。

3.4.智能汽车

智能汽车或智能网联汽车是指搭载先进的车载传感器、控制器、执行器等装置，并融合现代通信与网络技术，实现车与人、车、路、后台等智能信息交换共享，具备复杂的环境感知、智能决策、协同控制和执行等功能，可实现安全、舒适、节能、高效行驶，并最终可替代人工操纵的新一代汽车。

和传统汽车相比，智能网联汽车具有智能化、共享化、网联化等特点。智能网联汽车通与蜂窝网络和基站通信，帮助用户获取导航服务，实时获取路况，从而提升驾驶的智能化水平。

智能网联汽车的智能有两种，一种是 V2X，另一种是自动驾驶。

V2X 意为 vehicle to everything，能够实现车与车、车与人、车与路边设备进行信息交互的技术，使车辆能够实时获取路况信息、拥堵信息、行人信息等，从而提高驾驶安全性和交通效率。

自动驾驶又称无人驾驶，是通过计算机控制车辆的行驶的技术，是智能网联汽车的发展方向之一。自动驾驶技术依靠人工智能，传感器，车载雷达，GPS 等装置，让计算机可以在没有人操作的情况下，控制车辆的行驶。自动驾驶有两种控制方式，一是本地计算的方式，所有决策由本地计算机发出。另一种是将决策交给云端的计算机，通过蜂窝网络将决策下发到车辆。随着 5G 的发展，无人驾驶技术是未来车辆发展的趋势。

汽车在智能化网联化发展的过程中创造并使用了大量新技术、新功能，同时为车辆引入了相应的攻击面，也为传统汽车技术带来了安全挑战。例如汽车领域最常见的 CAN 总线，因为特有的灵活性、可靠性、实时性在汽车设计中大量采用，然而 CAN 协议在设计之初并没有考虑机密性、完整性等信息安全风险的防护。在传统汽车中，只有通过物理接口才能接入 CAN 总线网络，所以 CAN 总线安全风险较小；但在智能网联汽车中，攻击者可以通过 TBOX、网关、IVI 等部件利用 4G、5G、WiFi 通过远程网络接入 CAN 总线，这使得 CAN 总线的安全风险变得尤为巨大。

此外，智能网联汽车转化吸收了大量的传统信息技术，并采用各种各样的电子电器设备作为硬件支撑，这使得其除了拥有传统计算机网络所面临的风险外，还引入了新的硬件安全问题。例如汽车电子电器设备中常见的 IVI、T-BOX 部件：

（1）车载娱乐系统（IVI），IVI 通常是 Android 系统，配有麦克风、GPS、车载雷达总线等外设。这些设备如果不加以防护，便会造成车主隐私泄露，谈话被监听等。

（2）T-BOX（Telematics Box）是用于实现车内网络和外网通信的设备，负责将数据发送到云端，许多 T-BOX 厂商为了方便调试，会预留许多调试接口，如果完整地分析 T-BOX 的硬件结构、调试引脚、WiFi 系统、串口通信、MCU 固件、CAN 总线数据、T-BOX 指纹特征等，攻破 T-BOX 的软硬件防护将会特别容易。

和传统计算机安全相比，汽车安全影响不仅仅是隐私信息的泄露，还有可能危及车主和乘客的生命安全，因此汽车安全的重要性极高。

智能网联汽车场景下的安全可划分为车辆安全、网络安全、云平台安全以及移动 APP 安全，其中智能网联汽车移动 APP 安全与通用移动 APP 安全的解决方案类似，这里就不再赘述。

3.4.1.车辆安全

车辆安全主要包括固件安全、操作系统安全、数据安全、密钥安全、FOTA 固件安全升级和硬件安全模块。

1.固件安全

在芯片选型时优先选择支持加密算法、具有保护寄存器以及可以设置 Read-only 模式对存储器进行保护的芯片。此外，建议将固件存储在微处理器内部自带的存储单元中，并去除或禁用微处理器上的 JTAG、RS232 和 USB 等调试接口，减少固件被读取的风险。固件代码反汇编，一方面可以通过修改编译器的方式，自定义指令集，尽量避免使用微处理器或微控制的通用指令集；另一方面可以在对固件代码进行混淆或加入花指令，在不改变功能逻辑的前提下，降低代码的可读性。

2.操作系统安全

操作系统应能监控全部应用、进程对资源的访问并进行必要的访问控制，确保每个行为的可控和可管，支持最小权限原则对应用权限进行控制。应确保只有已严格定义并明确格式的 API 可以与汽车硬件层通信。应确保只有 OEM 签名的应用可以访问汽车硬件驱动。应提供白名单机制，限制车辆行驶过程中可以允许的应用。应定期收集更新操作系统漏洞列表，扩大漏洞收集途径，确保在第一时间内发现、解决并更新已知所有漏洞。对操作系统源码进行静态审计，快速发现代码潜在的 BUG 及安全漏洞，提高代码健壮性及操作系统的安全性。

3.数据安全

涉及数据的全生命周期，首先要遵循最小化原则，只采集与业务相关所需的数据，其次将数据分类分级，分别保护。再次要保证密钥安全，包括硬件安全模块或者密钥白盒等技术，硬件安全模块安全性高但成本高。

4.安全升级

当前固件空中升级（FOTA）技术已经非常成熟，但升级过程的安全性仍然需要格外重视。智能网联汽车 ECU 升级时需要配合安全升级机制，通过数字签名和认证机制确保增量升级包的完整性和合法性；可按照时间、地区、设备数量等信息动态调整升级策略；在

增量升级包传输过程中，通过通信加密保证整个升级包的传输安全。并时刻监控升级进程，确保 ECU 升级后能够正常工作，同时需要具备相应的固件回滚机制，保证即使升级失败 ECU 也可恢复到原来状态。

1) 硬件安全模块

HSM 是 MCU 中一个拥有计算能力的子模块，它通过安全启动校验来保证整个系统的安全性。HSM 与 MCU 中的其他普通内核及外设不同，它有自己专门的安全内核、随机数发生器、AES-128 加速单元、安全 Flash、安全 RAM、定时器及中断控制等模块，从而组成一个封闭的子系统。在这个子系统中，安全内核执行的固件和所需的 KEY 存储在安全 Flash 中，执行安全任务期间产生的缓存和 RAM_KEY 都存储在安全 RAM 中

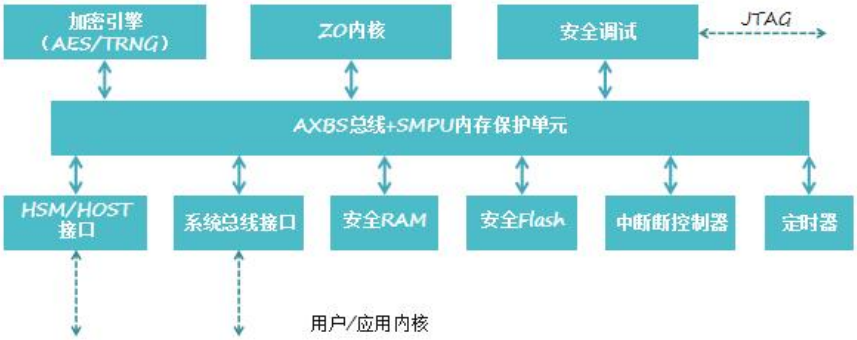

图 3-3 HSM 结构

3.4.2.网络安全

智能网联汽车的网络可分为车内、车际和车云网络，网络拓扑复杂多样，确保数据在网络传输时的安全性尤为重要。同时，安全边界的扩大、分散导致无法找出明确的边界，难以实施边界隔离。当前，智能网联汽车的网络安全主要从传输安全和边界安全进行防护。

智能网联汽车传输安全主要体现在三个方面：

a) 实施网络加密技术。基于网络的层次性结构，加强 TCP/IP 协议各个层次的防范措施，在网络加密结构设计时注意加密采用的密码体制，选择合适的密钥。对网络接口层加密时，相邻节点之间需要加强在线传输的保护形式，加强加密的透明程度。对传输层加密时加强节点和传输数据的保护机制；

b) 对传输信息实行安全防护策略，严格落实安全保密体系，按照信息的安全程度划分网络，同时对网络的安全控制实行全面的保护和控制，加强网络安全监测，实现边界防护。加强对网络信息的安全管理，实现信息传输的有效性和安全性；

c) 加强可信计算机的实施。建立可信计算平台，从可信的基础性数据出发，以密码的形式，实现计算机网络系统的安全性。可信技术平台能够确保用户身份的唯一性、工作空间的完整性，同时能保证环境配置的安全性，从根本上阻止黑客的入侵，提高数据传输的可信度。这种信任扩展到计算机系统中，能够增强网络环境的可信性，实现网络信息的安全性传输。

智能网联汽车极强的移动性和网络种类的复杂多样性，使得网络边界消失殆尽，传统的边界安全解决方案不再使用，传统的边界安全开始向微边界甚至无边界转换。针对这种现状可以从以下方面进行加强：

a) 在车辆体系架构设计中采用网络分段和隔离技术。对不同网段（如车辆内部不同类型网络，车辆与外部通信、Wi-Fi 等）进行边界控制，对车辆内部控制总线的数据进行安全控制和安全监测。同时车辆端关键网络边界设备需提供边界安全防护功能。

b) 在终端接入智能网联汽车网络前，需增加对终端设备的认证机制，确保终端设备的可信，避免未经认证的终端设备接入智能网联汽车。

c) 在车云网络中，车辆与云通信除了采用安全接入以及对业务进行划分，还需采用 PKI 或者 IBC 的认证机制对车辆与云平台进行双向认证，保障信息接入和传输的安全。

3.4.3.智能汽车云平台安全

智能网联汽车云平台安全保护两个部分，一是云平台自身的安全防护，二是利用云平台的可视化技术预警感知智能网联汽车的安全态势，更加主动的应对复杂多变的威胁和风险。

智能网联汽车 TSP 云平台的安全架构与通用云平台安全相似，主要包括一下几点：

a) 物理环境安全：通过门禁、视频监控、物理访问控制等措施实现环境安全。

b) 计算存储安全：对服务器主机/设备进行安全配置和加固，部署防火墙、IDS，以及恶意代码防护、访问控制等技术手段，确保主机能持续稳定的提供服务。

c) 可信计算：保障硬件、软件系统的行为/执行安全。

d) 网络安全：采用分域隔离、纵深防御等策略，结合防病毒、访问控制、流量监测等技术手段，通过整体防御保障网络通信安全。

e) 安全管理：制定安全管理制度、规范和流程，保证系统得到有效管理。

f) 信息安全：从数据隔离、加密、防泄漏及数据库防火墙、审计等方面加强数据保护，离线、备份数据的安全。

g) 应用安全：保护应用的程序安全，同时采用电子邮件防护、WEB 防火墙、WEB 网页防篡改、网站安全监控等应用安全解决方案确保特定应用的安全。

h) 可信安全管理平台：包括建设基于 PKI、身份管理等安全基础支撑设计；利用成熟的安全控制措施，保障系统的良好运转，提供满足各层需求的安全能力。

云平台可视化管理是指将车辆安全风险和威胁实时上报至厂商云平台，将整个车辆的安全态势呈现给用户，帮助用户快速掌握车辆安全状况，识别异常、入侵，把握安全事件发展趋势。利用高效的交互挖掘分析工具，将分散的信息要素进行集中、统计、检索、过滤、挖掘、分析，帮助用户洞悉智能网联汽车安全的态势。更加主动、弹性地应对复杂多变的威胁和风险。

3.5.智慧工厂

智慧工厂是一种灵活的系统，可以在更广泛的网络中自我优化性能，实时或接近实时地自我适应新条件并从中学习，并自动运行整个生产过程。这是一种技术驱动的方法，目标是发现自动化操作的机会，并使用数据分析改善制造性能。智能工厂是从传统的自动化到全连接的灵活系统的演变，不仅涉及货物的实际生产，还包括计划，供应链物流甚至产品开发等。智慧工厂利用物联网技术和设备监控技术加强了信息管理和服务，可以清楚掌握产销流程、提高生产过程的可控性、减少生产线上人工的干预、即时正确地采集生产线数据，并能合理编排生产计划与安排生产进度。

智慧工厂网络具有以下特点：

a) 终端安全手段难以部署

b) 无人值守，高自动低智能

c) 停机维护不可接受

对于智慧工厂的攻击形形色色，下面是一些常见的挑战。

1.漏洞攻击

一个智慧工厂通常含有数量众多的设备，全都连接到同一个网络。所以，只要其中任何一个设备含有漏洞，就可能让整个系统暴露在攻击风险当中。震网（Stuxnet）攻击事件中蠕虫就是利用系统的某些漏洞在网络上散布。

2.植入恶意程序

工业网络一旦遭黑客植入恶意程序，很可能将使得工业控制系统(ICS)遭黑客入侵，例如 BlackEnergy 和台积电案例。黑客会利用各种恶意程序发动攻击，例如：Rootkit、勒索病毒、木马程序等。此外，还会想尽办法来有效散布这些恶意程序以造成最大的损害，或者使用 APT 攻击。社交工程（social engineering）、鱼叉式钓鱼（spear phishing）、水坑式攻击等都是发动攻击的手段。

3.DoS 与 DDoS 攻击

大量遭到入侵的设备可以组成僵尸网络(Botnet)攻击某个目标系统致其瘫痪。例如，IoT 僵尸网络 Mirai 让不少知名网站和线上服务瘫痪。未来必将有更多针对智慧工厂与其他 IIoT 基础架构的攻击出现。同样地，遭到入侵的 ICS 系统最后很也可能变成僵尸网络的成员，变成黑客用来攻击其他企业的工具。

4.中间人(MitM)攻击

一个智慧工厂的运作需要使用多个通讯管道。通讯管道一旦遭到侵入，黑客除了能窃取资料，还能在通讯当中插入自己的代码或资料。由于智慧工厂的网络通讯大多位于组织内部，因此很多组织往往掉以轻心。确保网络通讯管道安全，也是系统防护的重点之一。

5.资料窃取

黑客可以暗中监视系统并窃取资料。通过暴露在网络上的人机界面(HMI)系统，很可能泄露组织的资料，让黑客趁机窃取一些公司机密和个人身份识别信息(PII)。

因此，智慧工厂的安全防范场景下，建议采用物联网安全技术如下：

1.终端安全

可以使用基于硬件的 TPM，或者可信执行环境（Trusted Execution Environment, TEE）提供一个隔离的环境，提升物联网终端机密性和完整性。智慧工厂终端需要有唯一的的识别信息，根据信任级别的不同，可以采用不同的识别信息，例如数字证书、IP 地址、MAC 地址、RFID、密码、生物识别或二维码，建议采用安全性高的数字证书作为识别信息。除此之外，还需要可信启动机制实现终端的完整性保护，保证引导的镜像未受篡改，引导过程不可以中断，并可以监测引导过程中的异常。

2.通信安全

智能工厂系统中的通信功能支持端点之间的信息交换，促进组件间的集成。根据交互的信息不同，可以采取不同的保护级别。交互的信息可以是传感器更新、遥测数据、命令、警报、事件、状态更改或配置更新等。IIoT 应用程序采用加密控制措施，例如应用于传输层的 TLS 或 DTLS 或中间件层的 DDS（Data Distribution Service, DDS）。端点之间通信应采用双向身份认证机制，强制执行访问控制授权机制，支持加密的机制，确保所交换信息的机密性和完整性。智慧工厂内部，根据业务做好分区分域控制，为每个网络段分配一个信任级别，并保护通过网络边界的通信和连接。

3.安全智能防御

采用基于大数据的安全威胁分析技术，利用关联分析、智能检索、溯源等功能，实现物联网攻击的实时发现和呈现。同时建立协同联动机制，采用威胁响应编排，辅助响应决策，实现物联网攻击的快速响应闭环。

3.6.平安城市

平安城市是一个超巨型、强综合性的城市管理系统，通过三防系统（技防系统、物防系统、人防系统）和管理系统共同建设城市的平安和谐。不仅需要满足治安管理、社会防控、道路管理、人员管理、应急处理等需求，而且还要兼顾灾难预警、安全生产监控等方面对图像监控的需求，同时还要考虑各系统之间的联动以实现平安城市的建设。

目前公安系统对于公共监控视频系统制定了多种安全要求，其中《公安视频传输网建设指南》对视频监控系统安全提出了明确要求。其中对于应用系统、边界防护、安全运维、网络分域等方面进行了详细的说明，有效地阻止了对视频监控系统的大量外来网络攻击。

然而，作为视频监控系统重要组成部分的前端接入设备——摄像机设备，由于缺乏相关的安全标准和安全技术，目前存在大量的安全隐患摄像机设备在现网中运行，这些设备面临着多种安全攻击，如图 3-4 所示：

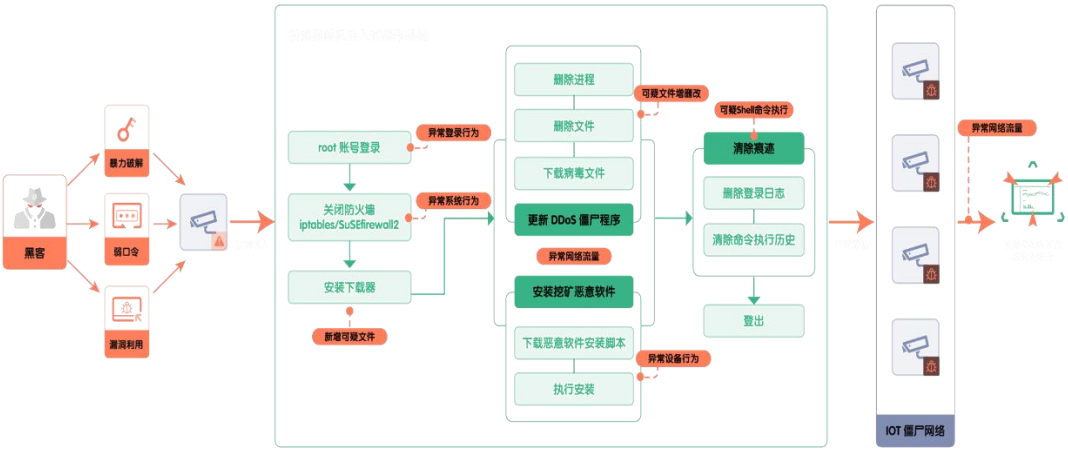

图 3-4 平安城市视频监控

这些攻击包括：

1.设备入侵

通过摄像机嵌入式系统或控制命令行等安全漏洞，入侵设备并进行病毒植入，将摄像机做为跳板，攻击其它网络实体或视频监控系统。

2.身份破解

通过暴力破解等方式对摄像机的口令（常广泛使用弱口令、默认口令）进行非法截取，实现设备入侵，进行图像窃取或设备破坏等行为。

3.视频窃取

在视频通过网络向视频监控服务商、网络服务商和运营商传输的过程中，非法人员可以截取网络信号，获得视频。

4.非法控制

通过破解摄像机控制指令，随意控制摄像机。

5.视频篡改

篡改视频源数据，造成监控失效。

为解决视频防控系统暴露出的问题，公安部连续发布了 GB/T28181-2011《安全防范视频监控联网系统信息传输、交换、控制技术要求》、GB/T 35114-2017《公共安全视频监控联网信息安全技术要求》等国家安全标准。这些标准的推出对解决平安城市、雪亮工程等大规模联网环境下设备、系统和数据安全所面临的威胁有重大意义。

其中，GB/T 35114 主要集中于前端摄像机设备通信过程中关于设备身份、数据方面相关安全防护措施。35114 标准首先将设备分为 A、B、C 三级：

1.A 级技术要求

实现前端设备基于数字证书与管理平台双向身份认证。

2.B 级技术要求

实现前端设备基于数字证书与管理平台双向身份认证，及视频数据签名，防止数据被篡改。

3.C 级技术要求

实现前端设备基于数字证书与管理平台双向身份认证、数据签名和数据加密，防止数据被篡改及窃取。

摄像终端应采用的具体技术措施包括：

a) 摄像头应内置保密安全芯片或安全模块；

b) 身份认证、视频数据签名采用 SM2 国密算法；

c) 视频流加密采用 SM1、SM4 国密算法；

d) 管理平台和视频摄像头之间采用带密钥的杂凑算法 SM3，对设备遥控等重要的会话启动协议（SIP）控制信令做认证。

同时，根据摄像机隐患分析，我们可以发现针对摄像机操作系统的安全防护需补足，需要对摄像机设备运行安全进行相关防护，可以通过安全行为监控等方式进行保护，例如采取 EDR 技术等。

端点检测和响应（EDR）是一种主动式端点安全解决方案，通过记录终端与网络事件，结合已知的攻击引擎、行为分析和机器学习技术来监测任何可能的安全威胁，并对这些安全威胁做出快速响应。

相比于传统端点安全防护采用预设安全策略的静态防御技术，EDR 加强了威胁检测和响应取证能力，能够快速检测、识别、监控和处理端点事件，从而在威胁尚未造成危害前进行检测和阻止，帮助受保护网络免受 0day 威胁和各种新出现的威胁。

对于摄像机设备的终端安全检测与响应措施，一般包括部署在设备终端上的轻量级终端安全软件(Agent)和管理平台。

Agent 通过部署在设备内部的操作系统中实现监控内的安全事件，对已知威胁精准定性，对未知威胁初判告警、捕获上报，对各类威胁进行阻断拦截，对已遂威胁清除处置，执行管理中心下发的多重安全策略。

管理平台主要面向安全管理人员，其存在形式可以为软件、硬件或云服务形势。管理平台提供对终端资产的统一安全管理，集中监测分析终端安全事件，制定和下发相关安全策略。

终端安全监测与响应主要的优点包括：

a) 智能检测，洞察威胁本质；

b) 迅捷灵动处置，及时响应威胁；

c) 一体化管理，终端资产全面识别；

d) 未知威胁的搜索和取证；

e) 可视化管理能力。

对于视频监控前端设备的系统安全，以下指标需要重点关注：

a) 账号监控：账号安全情况，包括账号盗取非法 IP 登录等；

b) 口令监控：口令安全情况，例如爆破登录、非法用户登录等；

c) 行为监控：用户操作的行为记录，实时定位异常操作，可回溯审计；

d) 文件监控：敏感文件的增、删、改等操作；

e) 进程监控：安全基线内进程监控，识别各类新增异常进程；

f) 流量监控：结合机器学习算法，快速检测设备的 TCP、UDP 流量攻击

g) 资源监控：CPU、内存、存储使用情况

h) 基线监控：基于设备业务制定的基线指标，实时对比判断是否出现异常。

对于视频前端设备，一旦发生各类异常，EDR 将有效识别并进行判断分析，通过实时告警、隔离处置等手段及时处理与防御，避免各类设备劫持、病毒感染等问题发生，保护前端设备的运行安全。