物联网安全体系的分析与技术研究

曹 侃
（联通数字科技有限公司 南京 210000）

摘 要 随着物联网业务的快速发展，物联网安全问题也越发凸显。近年来，国内外出现了多起物联网安全事件，如摄像头被攻破造成 DDoS 攻击、水表数据传输未加密被篡改等，对其安全体系的研究已经到了刻不容缓的地步。物联网业务包含云、管、端、边、用等多个层面，文中试图从安全防护体系和安全技术研究两方面入手，研究了物联网的安全风险点和应对措施，并将其应用到了实际业务中。

关键词：物联网安全；安全防护对象；安全管理体系
中图法分类号 TN915.03

Analysis and Technical Research on IoT Security System

CAO Kan
（Unicom Digital Technology Co.，Ltd.，Nanjing 210000，China）

Abstract With the rapid development of the Internet of Things business，the security problem of the Internet of Things has become more and more prominent. In recent years，there have been many Internet of Things security incidents at home and abroad，such as DDoS attacks caused by cameras being breached，and tampering with unencrypted water meter data transmission. The research on its security system has reached an urgent level. The Internet of Things business includes multiple levels such as cloud，tube，end，edge，and use. This paper attempts to start with the security protection system and security technology research，study the security risk points and countermeasures of the Internet of Things，and apply them to practical business.

Keywords IoT security，Security protection object，Security management system

0 引言

近年来，物联网安全事件频出，如 Hide'N Seek 僵尸网络感染了 9 万台物联网设备、IoTroop 对金融机构设备发起了多次 DDoS 攻击、20 万台路由器被黑导致内网设备恶意挖矿等。这些攻击手段各异，对象有别，防范起来属实不易。

物联网业务一般由物联网终端、传输网络、云平台 3 个部分构成。其中，物联网终端与手机终端相比，存在门槛低、计算弱、业务模型简单的特点。传输网络呈现泛在连接的特点，具有使用蜂窝制式（2/3/4G，授权频段）、短距制式（Wifi、LoRa，非授权频段），以及短距＋蜂窝制式。云平台的服务商众多，且具有与设备商绑定、设备接入高、频次低、数据量大等特点。每个层面的安全风险都会对整体端到端业务产生很大的影响。

行业缺乏统一规范，导致物联网业务的碎片化程度要大大高于互联网业务。因此，物联网安全更需要从体系出发，建立一套安全防护机制和安全管理体系，实现物联网安全的全覆盖。

1 物联网安全体系分析

物联网安全实施为“5＋1”基本框架，其中“5”为安全防护对象，即设备、网络、平台、应用、数据，而“1”为安全管理，通过安全目标、安全策略、风险评估、监测处置等，逐步构建物联网安全联防体系。

1.1 设备安全

设备安全防护致力于实施分层、分域安全策略，构建多技术融合安全防护体系。

其关键在于确保物联网边缘侧的设备安全，从而实现设备的安全防护。采取固件安全增强、漏洞修复、终端可信接入等安全策略，可以确保物联网系统内的生产设备、单点智能装备器件与产品以及成套智能终端等智能设备的安全。

收稿时间：2023-04-02

1.1.1 借助芯片安全增强物联网设备固件安全

物联网设备地理位置分散、暴露，多通过物理隔离进行保障，普遍缺乏身份认证与数据加密传输能力，安全防护水平不足。攻击者容易对设备进行物理控制和伪造，并以此为跳板，向其他设备与系统发动攻击。用户可采取安全的芯片对设备固件进行安全增强，阻止设备被抄板，保护设备敏感数据的安全性。

(1)基于安全元件(Secure Element)的密钥保护技术

SE包括安全层、COS层及应用层，与之对应的是在MCU下提供了安全的SDK工具、库函数、安全驱动等。SE可提供密钥存储、密码运算、敏感信息存储、固件完整性校验、可信身份认证、可信连接、应用数据加解密、可信应用更新等功能[1]。

(2)基于可信执行环境(TEE)的密钥保护技术

TEE可以为物联网应用控制终端提供可信的计算环境，提供TEE系统的开发服务及基于TEE环境的可信应用开发。TEE是集成内存分区、读取终端唯一ID、加解密库、校验等功能和机制于一体的代码块，因此其只能在软件上进行安全存储，无法实现硬件级别的安全存储。

(3)基于TEE+SE的密钥保护技术

SE安全级别较高，但存一定局限性，即没有UI交互界面，无法满足某场景丰富的人机交互需求。TEE的安全级别次之，其基于TrustZone硬件安全隔离技术，相当于EAL2+安全级别，支持丰富的UI交互。TEE与SE的结合能满足金融支付EAL4+级别的安全要求[2]。

1.1.2 利用专用漏扫平台有效治理物联网设备的漏洞

专业漏洞扫描平台支持对西门子、施耐德、GE、AB、霍尼韦尔、三菱等主流厂商的SCADA，DCS，PLC等系统进行漏洞扫描，扫描对象多样化。其全面覆盖了多种控制系统，可针对控制系统网络环境中存在的设备进行漏洞检测。

1.1.3 通过一机一证机制保障物联网设备的可信接入

一机一证机制指利用安全证书、根证书及发证系统能力，实现设备端的可靠认证和合法接入。其流程包括证书下发保存、公钥传输、私钥加密、对称加解密等，如图1所示。

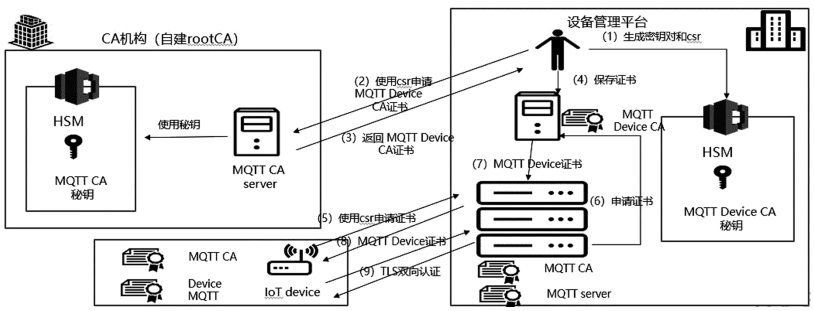

图1 一机一证的端云验证流程

1.2 网络安全

网络是物联网数据传输的载体。在网络环境复杂、端到端防护存在短板效应的情况下，需要重点考虑网络身份标识、可信安全链路、数据传送效率等，有效加强网络安全防护。

1.2.1 标识解析是物联网设备网络传输的唯一身份认证

标识解析体系是物联网尤其是工业互联网重要的网络基础设施，是实现工业企业数据流通、信息交互的关键枢纽。标识解析是设备在网络间的唯一身份识别器，可以解决私有标识导致的数据孤岛问题。另外，其还可以实现一物一码、防伪仿冒、动态追溯和防窜管理。标识解析的全流程接入鉴权、身份认证、传输加密流程如图2所示。

图2中，①② 标识为解析二级节点↔终端。

(1)身份认证：公私钥技术、质询响应(challenge-response)机制。(2)访问控制：定义与终端属性有关的访问控制信息，如增、删、改、查等。(3)传输加密：通过Diffie-Hellman共享加密密钥，实现安全加密Session。

③⑥为设备管理平台↔终端 。

(1)身份认证：客户端使用SHA256或SM3生成Token签名，携带Device_id，Device_key，Product_key，Device_secret至服务器端进行认证。(2)传输加密：通过Mqtts等协议实现传输通道加密。

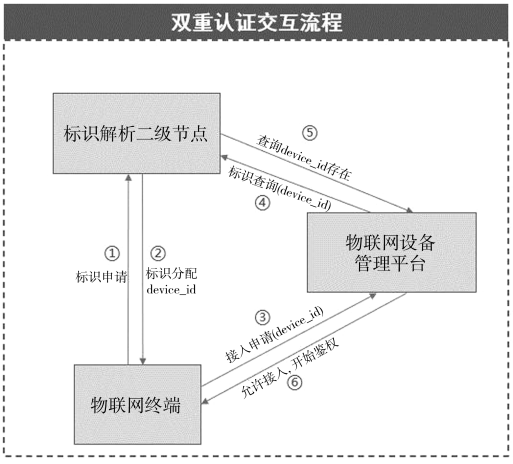

图2 标识解析双重认证流程

④⑤ 标识为解析二级节点↔设备管理平台。

(1)接口安全：接口鉴权、权限控制和操作审计。(2)传输加密：通过Https实现加密传输。

1.2.2 蜂窝网络＋APN专线保障用户网络通道的安全接入

(1)运营商APN：解决移动终端侧接入运营商PGW后的指定用户数据中心线路。(2)运营商VPDN：解决运营商PGW与用户数据中心的安全通信问题，可采用专用物理线路或公共互联网线路。

利用运营商级的APN和VPDN专线方案，可以保证物联网终端与云平台之间网络传送的私密性，确保数据在传输过程中的安全性，使其不被篡改。

1.2.3 5GC网络切片解决高实时与非实时的数据同传需求

物联网终端传输的数据有很多种，如实时业务类数据、离线业务类数据、控制类数据等。对于实时业务和控制类数据而言，存在因网络拥塞导致的数据延迟甚至丢失现象，使用5G网络的切片特性，可以解决该问题。

5GC核心网控制面和用户面通过镜像的方式采集信令消息，感知和分析通信网络运行状态及设备和核心网间的信令连接质量。同时，其可以采集用户面信息，分析生产环境设备运行状态、探测感知生产安全风险。一旦网络服务出现拥塞现象，就可以通过切片保障高优先级业务的正常运行，同时触发告警，及时通知网络保障人员进行抢修恢复。

2 平台安全

考虑物联网终端接入数量大、增长速度快、潮汐现象明显等因素，物联网平台以云平台部署为主，可支持弹性扩缩容、快速部署拉起等应用。云平台技术可分为虚拟化和云原生两部分，下文主要考虑云原生安全技术。

2.1 云原生安全技术赋能平台可控开发运维

以容器为核心的云平台，可从云原生基础架构安全、容器生命周期安全、微服务安全治理、云原生研发安全4个方面，夯实云平台原生安全体系。

(1)云原生基础架构安全

云平台底座安全能力基于云平台VPC等提供容器网络隔离能力，提供IaaS层的软、硬件安全防护能力，同时提供主机安全防护、云数据全链路加密能力、资源访问控制能力和审计能力等。通过整合主机网络的安全能力，为开发者提供安全可靠的开发环境和数据存储服务。

(2)容器全生命周期安全

1)仓库安全：基于自定义ACL规则的镜像仓库网络访问控制；2)容器构建：基于CVE的容器镜像扫描、镜像签名和验签能力；3)部署安全：提供高风险镜像识别和阻断分发、部署能力；4)运行安全：容器进程异常行为检测、逃逸攻击检测、恶意程序检测等；5)链路追溯：应用交付全链路追踪的可观测性。通过开放容器安全能力，可以为部署人员提供稳定、直观的容器构建与追溯服务。

(3)微服务安全治理

1)微服务协同调用：提供微服务接口安全验证、协同调用、安全通信能力；2)微服务运行监测：对微服务行为安全进行实时监控；3)接口审计管控：对调用第三方微服务接口的通信进行审计和管控。通过开放微服务治理能力，可以为运维人员提供服务检测、管控、审计等能力。

2.2 边缘云助力“云边端”一体化协同防御

在很多物联网场景中，物联网终端不具备直接接入云端的条件，需要借助边缘云作为网关统一接入。边缘云作为部署在云与海量终端的中间环节，对构建“云边端”一体化的协同防御体系有着承上启下的关键作用。边缘云安全能力体现在如下几点。

(1)基础安全防护。提供传统云计算中心的基础安全防护能力。(2)接入及权限控制。对海量多源异构终端流量进行筛选和过滤，提供零信任场景身份认证、细粒度动态授权等创新技术能力。(3)终端管理能力。面向海量多源异构终端提供OTA补丁及更新管理能力。(4)业务与平台的协同防御。由安全微服务和引擎管理微服务构成，南向采集UEBA用户行为数据、威胁感知数据、攻击诱捕蜜罐数据，北向对接云中心大数据分析引擎，对行为、威胁、蜜罐等多维度攻击数据进行分析预判及提前阻断，实现“云边端”一体化的协同防御体系。

3 应用安全

物联网应用主要包括APP与应用程序两大类，其范围覆盖智能化生产、网络化协同、个性化定制、服务化延伸等方面。目前面临的安全风险主要包括数据泄露、权限控制异常、系统漏洞利用、账户劫持、应用接入安全等。对应用程序而言，最大的风险来自安全漏洞。

3.1 传统物联网应用安全防护对象及安全风险

(1)代码审计，指检查源代码中的缺点和错误信息，分析并找到这些问题引发的安全漏洞，并提供代码修订措施和建议。应用程序在开发过程中，应该进行必要的代码审计，发现代码中存在的安全缺陷，并给出相应的修补建议。

(2)应用漏洞发现，漏洞发现基于漏洞数据库，其通过扫描等手段对指定应用程序的安全脆弱性进行检测，是发现可利用漏洞的一种安全检测行为。在应用程序上线前和运行过程中，要定期对其进行漏洞发现，及时发现漏洞并采取补救措施。

3.2 APP安全实现威胁闭环管理

在传统检测、加固能力的基础上，提升对APP安全威胁预测与侦测的感知能力，加强对已知或未知的各类安全事件的响应和应对能力，充分利用大数据技术进行安全系统建设。建立威胁闭环管理机制，实现对已知威胁、未知威胁的主动响应，打通从APP数据采集、挖掘到数据决策、数

据应用的所有环节，精准赋能 APP 安全。

4 数据安全

物联网数据是贯穿物联网产业的“血液”，其已成为提升制造业生产力、竞争力、创新力的关键要素。随着物联网业务的发展，数据安全已成为保障物联网安全的主线，一旦数据被泄露、篡改及滥用，将会给国计民生甚至国家安全带来重大威胁。

(1)数据分类分级

物联网数据安全关乎国计民生，关键数据如设备运行数据、设备维护数据、集成测试数据、物联采集数据、平台应用与服务数据、平台运行数据等，均为核心敏感数据。企业需加强数据安全意识，落实实践数据分级分类管理举措。

(2)内外数据交互准则、权限控制和数据确权

在物联网时代，业务与生产数据深度交互、生产与企业管理数据相互流通，不同安全域之间的数据互访需求，为物联网数据在传输、存储等过程中造成了极大的安全风险。区块链具有可信协作、隐私保护等技术优势，可与物联网实现深度融合，尤其在数据的确权、确责和交易等领域，有着广阔的应用前景，可为构建数据资源管理和服务体系提供坚实的技术基础。

5 安全管理体系

物联网安全防护体系具有一整套安全管理体系。该体系系统地描绘了物联网安全从安全目标→风险评估→安全策略→检测感知→威胁防护→处置恢复这一螺旋式上升的环节和流程。该方法论可以有效指导日常安全工作，推动安全防护体系不断走向新阶段。

6 结语

物联网安全是一个系统性工程。在终端层、网络层、平台层、应用层、数据层等中，任何层面的安全风险都可能引起雪崩式的连锁反应。同时，物联网业务在终端和应用层门槛较低，厂商碎片化明显，缺乏行业规范和标准，安全现状堪忧。随着我国对网络安全和数据安全的重视程度的提高，物联网安全也被纳入了国家总体考虑范畴。各种类型的物联网安全白皮书也纷纷出台，但距离标准落地尚需一段时间。如今，人们已意识到安全的重要性，是否具备安全治理能力，已成为人们选择物联网服务时的重要考量。随着社会的发展，物联网安全理念将会深入人心，从而实现端到端管控，为业务的持续发展保驾护航。

参考文献

[1] 亢洋，孙健，李刚.智能仓储物联网中前端感知处理系统架构设计用[J].警察技术，2013(2)：12-13.

[2] 沈苏彬，毛燕琴，范曲立，等.物联网概念模型与体系结构[J].南京邮电大学学报(自然科学版)，2010，30(4)：1-8.

(上接第 185 页)

可信计算技术的要求。此外，针对数字化基础设施，《中华人民共和国网络安全法》指出，国务院和省、自治区、直辖市人民政府应当推广安全可信的网络产品和服务，《国家网络空间安全战略》提出的战略任务“夯实网络安全基础”强调，应强调尽快在核心技术上取得突破，加快安全可信产品的推广应用。

4 结语

产业界重塑网络安全观，需要以可信计算 3.0 技术体系为抓手，在基础设施层面进行加固，从而形成底层的自主免疫防御体系，为相关领域保驾护航。

参考文献

[1] 曹国彦，马彦慧，吴越，等.浅谈工业互联网云平台安全防护技术[J].保密科学技术，2020(10)：42-46.

[2] 刘强.一种工业互联网云平台交互搭建方式[J].信息技术与信息化，2021(9)：124-126.

[3] 佟国毓，尚文利，陈春雨，等.工业互联网云平台信息安全关键技术[J].自动化博览，2019，36(S2)：80-85.