服务生态系统的

物联网安全指南

物联网服务生态系统的物联网安全指南

版本 2.0

2017 年 10 月 31 日

本文档是 GSMA 无约束力永久参考文档

安全密级：非机密

对本文档的获取和分发限于安全密级允许的人员。本文档是协会机密信息，受到版权保护。本文档仅用于所述目的，未经协会事先书面批准，不得向安全密级允许人员以外的其他人员披露文档信息或以任何方式令其获取，无论是整个文档还是文档部分内容。

版权声明

免责声明

GSM 协会（以下简称“协会”）不做与本文档信息相关的任何陈述、保证或承诺，不接受相应的责任，对本文档信息的准确性或完整性或及时性概不负责。可能变更本文档中包含的信息，恕不另行通知。

反垄断通知

本文档中包含的信息完全遵守 GSM 协会之反垄断合规政策。

目录

1 简介

1.1 GSMA 物联网安全指南文档集介绍

本文档是 GSMA 安全指南文档集的一部分，该文档集旨在帮助发展初期的“物联网”(IoT) 行业获得对物联网安全问题的一般了解。本指南文档集不具约束性，旨在倡导发展安全物联网服务的方法，以促进在整个服务周期中执行最佳安全实践。本文档就如何应对物联网服务中常见的安全威胁及薄弱环节提出建议。

GSMA 安全指南文档集结构如下所示。建议先阅读概述文档“CLP.11 物联网安全指南概述文档”[1]，然后再阅读其他支持性文档。

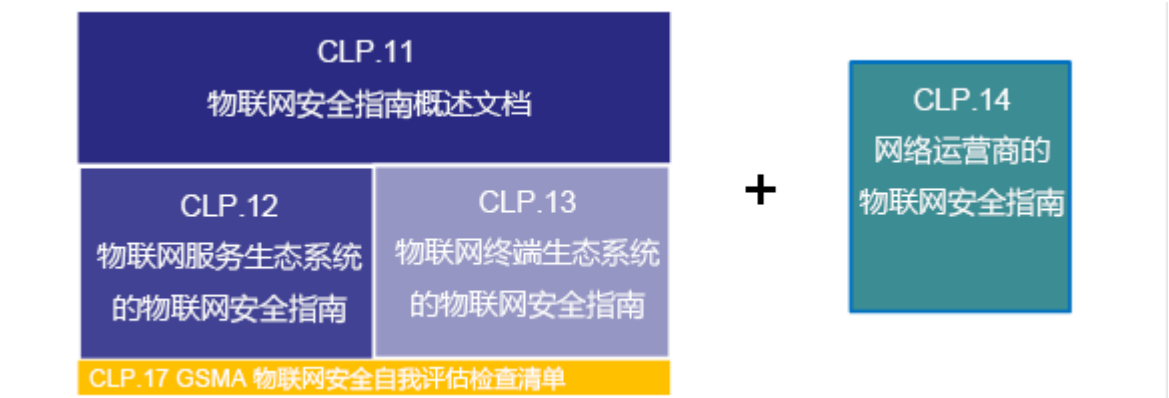

图 1 - GSMA 物联网安全指南文档结构

建议网络运营商、物联网服务供应商及物联网生态系统的其他合作伙伴阅读 GSMA 文档 CLP.14“网络运营商的物联网安全指南”[4]，该文档为志在向物联网服务供应商提供服务的网络运营商提供顶级安全指南，确保系统安全和数据隐私。

1.1.1 GSMA 物联网安全评估检查清单

文档 CLP.17 [13] 中提供一份评估检查清单，借助该文档，物联网产品、服务和组件的供应商可自主评估其产品、服务和组件是否符合 GSMA 物联网安全指南。

通过完成 GSMA 物联网安全评估检查清单 [13] 中的项目，实体可以说明他们为使自己的产品、服务和组件远离网络安全风险所采取的安全措施。

完成之后可向 GSMA 呈递一份报告作为评估声明。请参阅 GSMA 网站上的相关流程：

https://www.gsma.com/iot/future-iot-networks/iot-security-guidelines/

1.2 文档目的

从服务生态系统的角度而言，本指南应用于评估物联网产品或服务中的所有组件。服务生态系统包括组成物联网基础设施核心的所有组件。该生态系统中的组件包括服务、服务器、数据库群、网络元素和用于驱动任何产品或服务内部组件的其他技术。

本文档仅限于限于提供与物联网服务和网络元素设计及部署相关的建议。

本文档并非旨在推动建立全新的物联网规格或标准，而是参考现有的解决方案、标准和最佳实践。

亦非有意加速淘汰当前的物联网服务生态。如果网络运营商现有的物联网服务足够安全，应保持对这些服务的向后兼容性。

请注意，必要时，特定地区的国家法律法规可能要高于本文档中所述的指导原则。

1.3 目标受众

本文档的主要受众包括：

- 物联网服务供应商 - 致力于开发创新互联的全新产品和服务的企业或组织。物联网服务供应商的部分运营领域包括智慧家庭、智慧城市、汽车、交通运输、健康、公共设施和消费电子产品。
- 物联网终端设备制造商 - 为物联网服务供应商提供物联网终端设备以实现物联网服务的供应商。
- 物联网开发人员 - 代表物联网服务供应商构建物联网服务。
- 网络运营商 - 为物联网服务供应商提供服务。

1.4 定义

术语	描述
访问控制列表	随附计算对象的权限列表
接入点名称	终端设备连接的网络连接点标识符。与服务类型相关，每个网络运营商通常配置一个接入点。
攻击者	黑客、威胁代理商、威胁执行者、诈骗者或物联网服务的其他恶意威胁。此类威胁可能来自个体犯罪、组织犯罪、恐怖主义、敌对政府及代理、工业间谍、黑客组织、政治活动分子、业余黑客、研究者以及不小心违反安全和隐私的行为。
云	互联网远程服务器网络，可担当主机、存储、管理并处理应用程序及数据。
容器	能够在一台主机上运行多个隔离系统或容器的技术。
嵌入式 UICC (eUICC)	根据 GSMA 规定，支持对网络或其验证的服务订阅进行远程配置的 UICC。
终端客户	物联网服务供应商所提供的物联网服务的客户。终端客户和物联网服务供应商可以是同一操作者，例如公共事业公司。
终端生态系统	低复杂性设备、富设备和网关的任何架构，这些设备和网关以新颖的方式将真实世界与数字世界连接。有关详细信息，请参阅 CLP.11 [1]。
正向加密	安全通信协议属性：如果对长期密钥的入侵并未攻击之前的会话密钥，则称安全通信协议具有正向加密性。

术语	描述
物联网	物联网是指不同机器、设备和家用电器都可以通过不同网络连接到互联网。这些设备包括日常用品，包括平板电脑和电子消费产品、以及其他机器，如具有发送和接收数据的机对机 (M2M) 通信功能的汽车、监视器和传感器。
物联网终端	复杂物联网终端设备或物联网网关设备的通用术语。
物联网服务	利用物联网设备数据执行服务的任何计算机程序。
物联网服务生态系统	服务、平台、协议及其他技术组合，可提供相关功能并从现场部署的终端中收集数据。有关详细信息，请参阅 CLP.11 [1]。
物联网服务供应商	致力于开发创新互联的新物联网产品和服务的企业或组织。
网络运营商	将物联网终端设备连接至物联网服务生态系统的通信网络运营者及所有者。
组织信任根	一系列密码政策与流程，控制如何为身份、应用程序和通信安全加密。
安全组	控制一个或多个虚拟服务器实例流量的虚拟防火墙。
可信计算基	可信计算基 (TCB) 是产品或服务中算法、策略和机密的集合。通过 TCB 模块，产品或服务可以测量自身的可信度，衡量对等网络的真实性，验证产品或服务所发送或接收消息的完整性。TCB 是安全平台基础，可以在它的基础上构建安全产品及服务。TCB 的组件会根据背景（终端硬件 TCB 或云服务软件 TCB）发生变化，但抽象目标、服务、程序和策略应当非常相似。
UICC	ETSI TS 102 221 规定的安全元素平台，可支持以密码区分的安全域中多个标准网络或服务验证应用程序。可体现为 ETSI TS 102 671 标准中指定的嵌入式设计规格。
虚拟专用网络	允许某一特定客户服务组专用的逻辑独立的安全网络。其名称源于 VPN 与网络其他部分相互隔离，因此可作为一个独立的虚拟网络

1.5 缩略语

术语	描述
3GPP	第 3 代项目合作伙伴
ACL	访问控制列表
API	应用程序接口
APN	接入点名称
CERTS	计算机应急响应小组
CLP	GSMA 互联生活项目
DDoS	分布式拒绝服务
GSMA	GSM 协会
HSM	硬件安全模块
IoT	物联网
IP	互联网协议
SQL	结构化查询语言

术语	描述
TCB	可信计算基
VM	虚拟机
VPN	虚拟专用网络
WAF	网络应用程序防火墙

1.6 参考文献

参考文献	文件编号	标题
[1]	CLP.11	IoT Security Guidelines Overview Document
[2]	CLP.12	IoT Security Guidelines for IoT Service Ecosystem
[3]	CLP.13	IoT Security Guidelines for IoT Endpoint Ecosystem
[4]	CLP.14	IoT Security Guidelines for Network Operators
[5]	不适用	OWASP Secure Application Design Project https://www.owasp.org
[6]	不适用	TCG Trusted Platform Module http://www.trustedcomputinggroup.org
[7]	不适用	TCG Guidance for Securing IoT http://www.trustedcomputinggroup.org
[8]	不适用	OAuth 2.0 http://oauth.net/2/
[9]		OpenID Foundation http://openid.net/foundation/
[10]	不适用	GSMA Mobile Connect https://mobileconnect.io/
[11]	GPC_SPE_034	GlobalPlatform Card Specification www.globalplatform.org/specificationscard.asp
[12]	GPD_SPE_010	GlobalPlatform TEE Internal Core API Specification www.globalplatform.org/specificationsdevice.asp
[13]	CLP.17	GSMA 物联网安全评估检查清单 https://www.gsma.com/iot/iot-security-assessment/
[14]	不适用	ETSI TC SmartM2M specifications www.etsi.org
[15]	不适用	oneM2M Specifications www.onem2m.org
[16]	3GPP TS 33.220	Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA) www.3gpp.org

2 服务模型

现代物联网产品和服务需要一个服务生态系统以便为终端、合作伙伴和用户提供实际意义、功能和价值。根据物联网产品和服务所提供的应用程序的复杂性，基础设施可能非常庞大，由许多不同类型的服务和服务接入点组成。另外一方面，如果应用程序非常简单直接，基础设施可能会较为简化。

无论形式如何，服务生态系统都是整个物联网技术各核心面的功能和通信连结纽带。所有其他生态系统都依赖于服务生态系统进行分级认证、连接用户、实现可用性、管理和执行日常物联网运行所需的其他关键任务。为完成这些任务，服务生态系统由许多所需的层级组成，以实现基础实施目标。数据库集群、应用程序服务器、应用程序代理服务器以及其他类型的基础设施均为此类层级的范例，在许多给定的部署中均存在。如下图所示，网络和终端生态系统依赖于服务生态系统的核心功能。

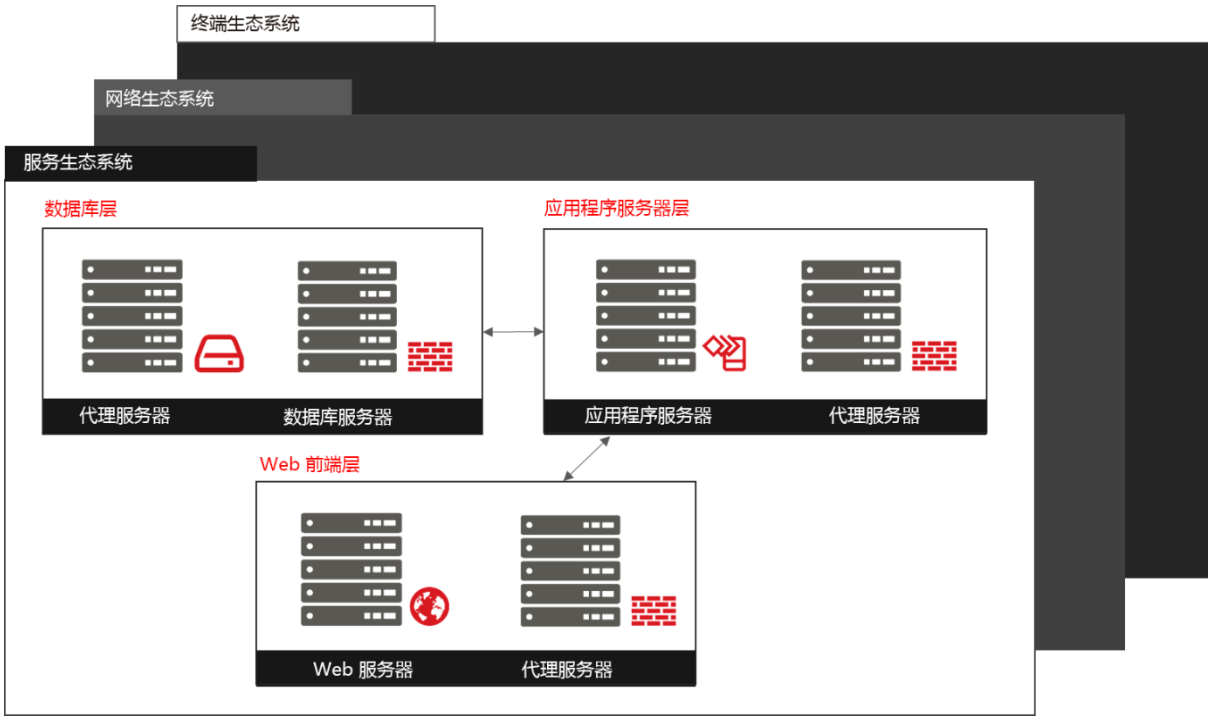

图 2 - 对服务生态系统的依赖性

现代服务生态系统的范例包括但不限于：

- 基于云基础设施的解决方案
- 基于容器的应用程序部署
- 传统数据中心服务器环境
- 数据库集群
- Web 应用程序框架服务集群

虽然每个示例环境可能在设计、拓扑结构和执行方面大相径庭，但就信息流入与流出应用程序的方式而言，其均基于同一理论。

所有现代计算系统均需要一个进入点（称为服务接入点）以进入应用程序基础设施。为此应用程序创建内容和环境的内部子系统必须能够处理安全可靠环境和网络中的数据。数据必须存储在某个地方，然后再返回服务层，该层将回应授权命令，或者将其发送到同一生态系统或其他生态系统及其关联网络中的各个组件。

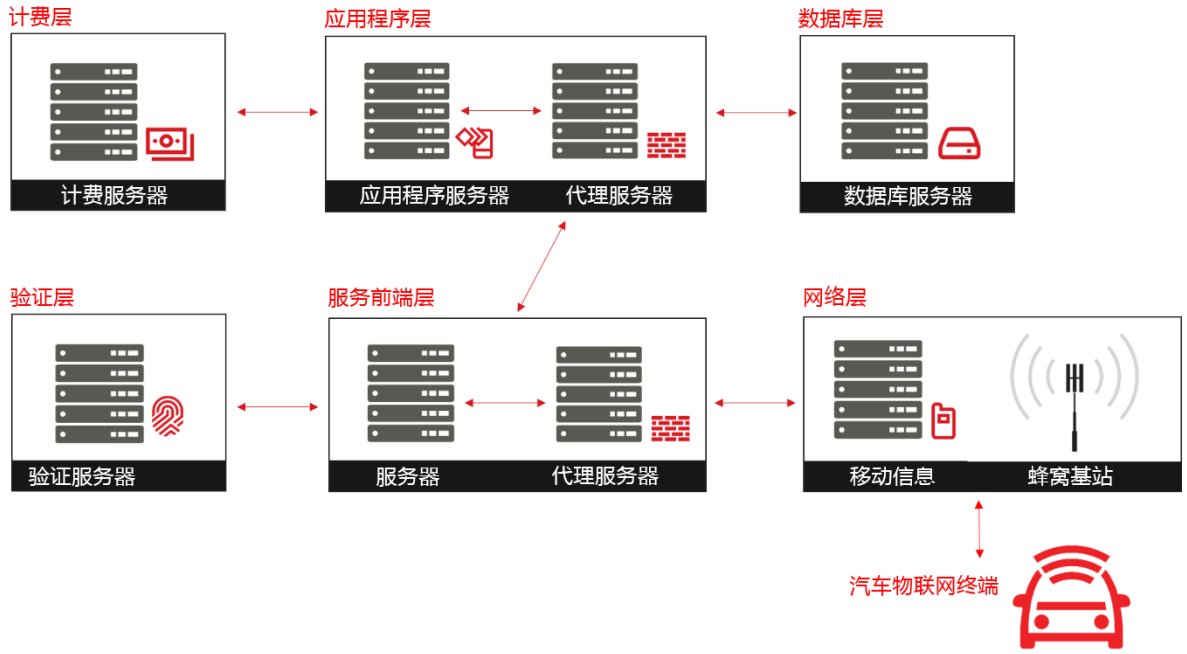

图 3 - 服务生态系统示例

无论利用现代技术还是传统技术实施这一标准框架，均应使用公认的协议与技术处理、提供和验证信息。虽然处理环境的拓扑结构和抽象方式已发生变化，以符合速度、计算能力和存储方面的现代要求，但实现这些创新所使用的核心技术仍然没变。例如，每层通常都包含一个代理或防火墙系统，对自/至特定类型的服务器组的连接进行管理。计费层将提供计费服务。应用程序服务器驻留在特定于应用程序的层级。数据库服务必须在数据库层进行管理。这些系统根据代理服务器使用的进出规则协同工作。

因此，服务生态系统的安全模型可轻松分成一系列组件。这些组件将在本文档中加以讨论。

3 安全模型

无论使用何种拓扑结构或创新来构建应用程序架构，均可使用通用的基础设施、策略和政策设计服务终端环境中的安全性。服务生态系统的每个方面都可分成各组件。这些组件必须进行单独保护，但可使用相似的方法。

例如，使用通用组件共建简单服务，这种服务可应对查询，并从/向终端、合作伙伴及用户发送回应。该模型应包含但不限于如下层级：

- Web 服务层
- 应用程序服务器层
- 数据库层
- 验证层
- 网络层
- 第三方应用程序层，例如计费层

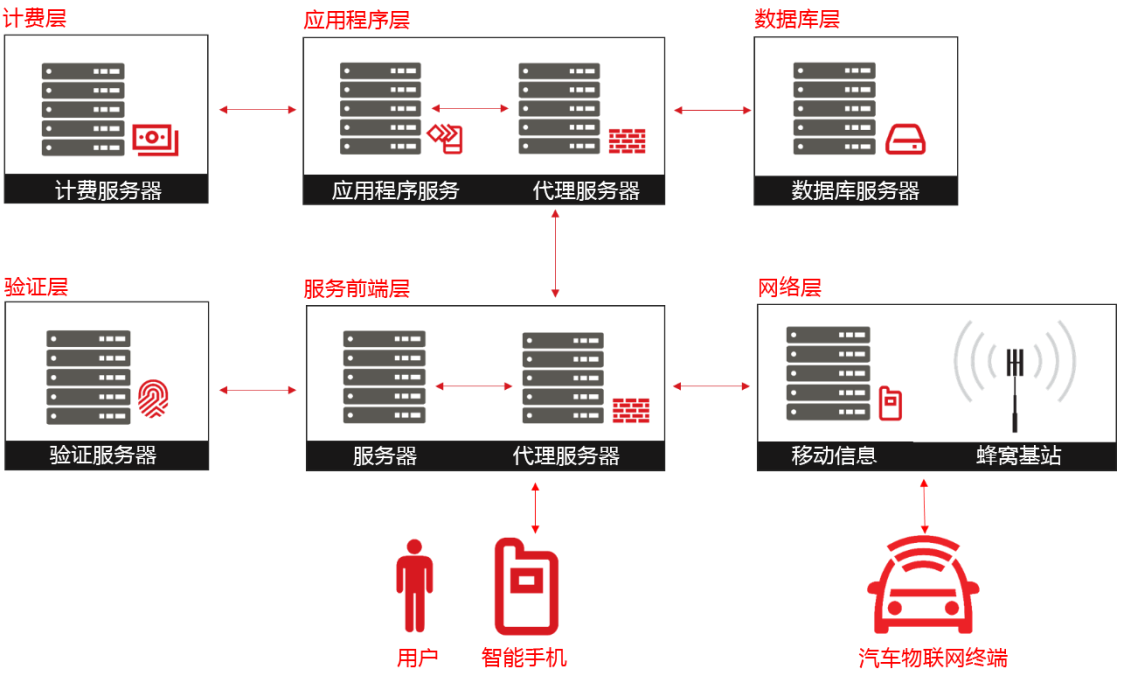

图 4 - 具有独立层级的服务生态系统示例。

即使每个层级仅有一台服务器，但从架构层面看，将每个逻辑概念分至其各自层级将更加有效。若出现问题，或系统需要扩展以满足更多需求，这将有助于将技术层与其他层分离开来。

若从*层级类型*角度考虑系统类型，则可更轻松地对其进行保护、按需扩展、停用和废止。唯一的要求是 API 功能要足够多样化，可在整个层级周期中进行扩展或调整。本文档不会讨论如何定义此 API，但将讨论有关组织选择或定义的 API 高层级安全属性的建议。

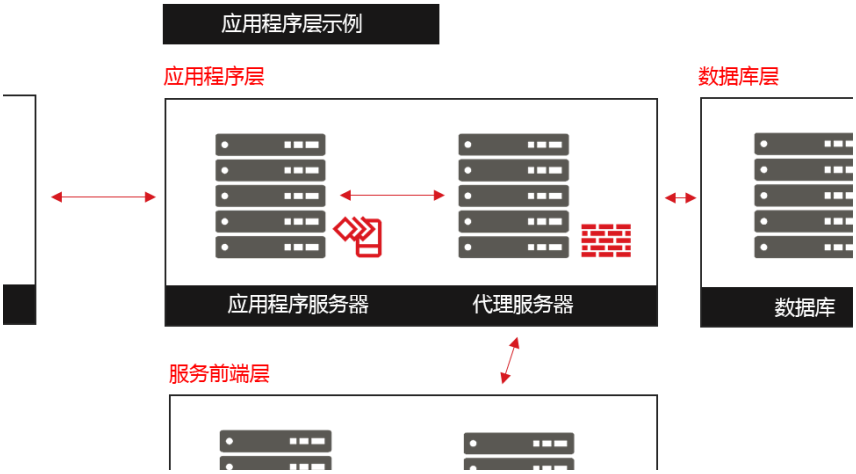

图 5 - 由防火墙技术防卫的应用程序层

上例对层级进行了略微更完整的描述。对层级的描述唯一需要扩展的地方在于代理服务器。该代理服务器只是一种描述符，代表在此层级中将使用的现实安全技术。不论实际控制是否为硬件防火墙、软件防火墙、安全组、访问控制列表 (ACL) 或其他技术，都将有一个组件代表层级管理进出控制。

选择或定义 API 时，组织应考虑可能解决工程团队疑虑的现有规范。组织尤其应考虑以下规范：

- ETSI SmartM2M TS 102 690、ETSI SmartM2M TS 102 921 [14]
- oneM2M TS-0001、oneM2M TS-0003 [15]
- 3GPP TS 33.220 [16]

对于可公开访问的组件来说，如服务前端层，模块所需的唯一扩展是用于以下方面的附加安全组件：

- 分布式拒绝服务 (DDoS) 保护
- 负载均衡
- 冗余
- 可选 Web 应用程序防火墙 (WAF) 功能

任何服务均应使用上述技术以实现正常运行，并确保即使在资源最为受限的环境中，仍能提供其保护的服务。本文档不会定义这些组件，但可参照以下实体进一步探究：

- 云安全联盟
- NIST 云计算标准
- 联邦风险和授权管理程序 (FedRAMP)
- 思科网络管理指南

层级安全运行所需的其他属性是定义服务器本身。其由管理员、应用程序以及控制工程团队所选的平台内部的操作系统控制进行定义。

平台环境内部部分问题列表如下：

- 登录集中式日志服务
- 管理验证和授权
- 通信安全实施
- 数据备份、恢复和复制
- 应用程序职责分离
- 系统监控和完整性

3.1 网络基础设施攻击

从网络的角度看，试图攻击服务终端的攻击者会认为实体通信的方式肯定存在弱点，而通过服务接入点提供的公开服务也存在漏洞。这些攻击会假定，如果在网络中处于高权限地位，则在通信通道中也会同样处于高权限地位。

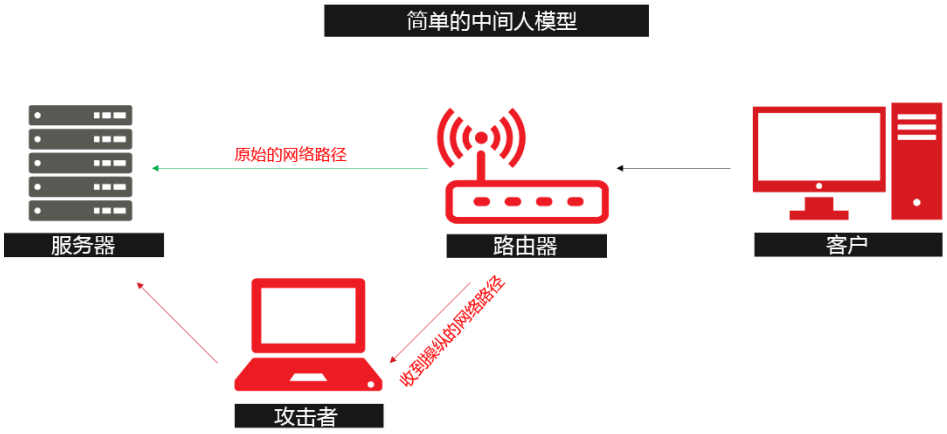

图 6 -“中间人”攻击模型示例

此模型中最常见的攻击方式是中间人 (MITM) 攻击。该攻击假定通信通道中不存在对等验证和单方对等验证，或者相互验证被破坏。攻击者的目标就是冒充对话的一方，强制对等方代表攻击者执行操作。通过执行相互验证可降低此类攻击的风险，而这需要明确定义的组织信任根、可信计算基 (TCB) 和通信模型。

其他攻击包括针对正向加密和加密通信分析的攻击以及旁道攻击等。必须使用合适的加密协议、算法和标准降低这些攻击风险。

此类攻击很难应对，其需要访问网络基础设施，要么进入组织内部，访问组织及其合作伙伴或终端生态系统间的核心互联网基础设施，要么访问终端附近的基础设施。最简单和最常见的攻击是试图操纵终端的网络基础设施，例如 Wi-Fi、以太网或蜂窝网络，以获取服务及其对等方的高权限地位。

针对单一端点基础设施的攻击仅限于此终端，或该物理位置上的终端组。对核心互联网基础设施的攻击通常涉及边界网关协议 (BGP) 劫持、攻击核心路由器或滥用域名服务 (DNS) 基础设施。这些攻击会提供与特定目标极为无关的高权限地位，使攻击者能够同时访问多个系统目标。针对内部网络基础设施的攻击需要访问内部网络，这意味着或者为内部攻击，或者在公司环境中具有高权限地位，也表明系统已受到深层攻击破坏。

无论是何种类型的攻击，只要利用相互验证、正向加密、适当的加密协议和算法，就可轻松降低该模型的攻击风险。这样可使攻击者无法滥用此基础设施，或大大增加此类型攻击的成本，使普通攻击者难以实施攻击。

3.2 云或容器基础设施攻击

这些攻击假定在云或容器基础设施环境中具有一个高权限地位。例如，如果攻击者能够攻破云服务网络，他们就可能进入正在运行访客虚拟机 (VM) 系统的主机。这样可让攻击者检查并修改正运行的 VM 系统。攻击者可能心中已有特定目标，或者可能已经侥幸攻破云服务供应商，只为访问多个不同类型系统获取重要数据。

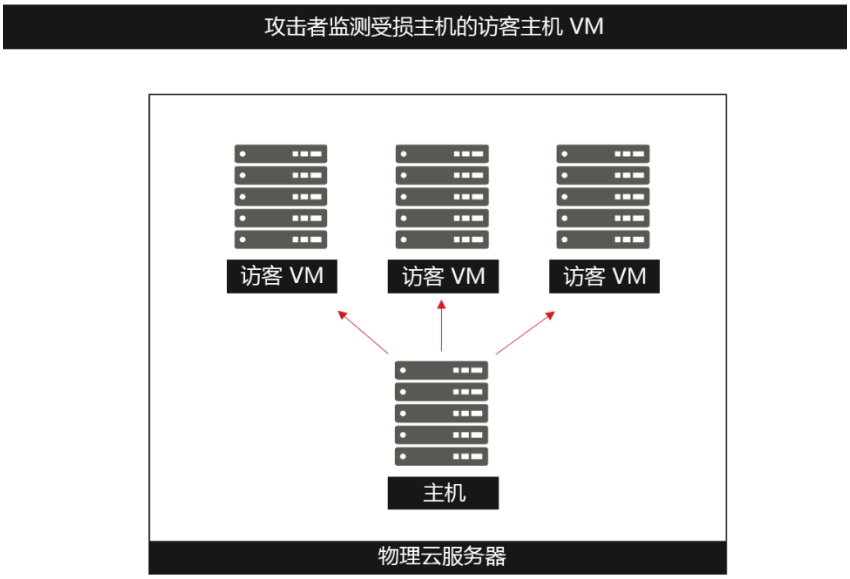

图 7 - VM 攻击模型示例

另一种云或容器基础设施攻击假定攻击者可控制与目标 VM 相同的物理服务器上的 VM。攻击者可能会使用多种方法攻破物理服务器上的其他 VM。他们可以：

- 利用 VM 基础设施的漏洞摆脱访客身份限制进入主机系统
- 利用旁道攻击推断另一访客 VM 的密钥
- 利用物理服务器上的大量资源，强制目标 VM 迁移至攻击者具有更多控制的物理服务器上

无论使用何种攻击模型，企业均无法采取措施防范此风险。相反，云服务供应商必须充分发挥作用，以降低攻击者破坏云或容器基础设施的可能性。

降低此风险的一种方式就是实施基于容器的架构和独特的加密身份，该架构能够将每个容器限定给特定用户。虽然这是一种资源高度密集型的活动，并且可能产生额外费用，但其能够削弱攻击者滥用 VM 基础设施同时访问多个用户或多项服务的能力。

虽然云或容器环境中的高权限地位对访客 VM 中应用程序的执行构成严重威胁，但访问该位置需具备强大的技能，投入大量的时间和资源。一旦获得访问权限，攻击者必须对其长期维护以识别哪些系统包含与其利益相关的 VM。此外，他们必须能够在不被云服务供应商的事件子系统检测到的情况下监测或更改该 VM。这可能会带来严峻挑战，应该会降低攻破的可能性。

但值得注意的是，访客 VM 以及正运行的应用程序大多不能检测到此类攻击。因此，通常能够收集揭示特定云 VM 或容器异常行为的指标，但要识别攻击是否真实发生可能极为困难。这是因为在 VM 基础设施主机层中拥有充分权限的任何攻击者都能够操纵访客 VM，使其难以检测到操纵行为。

访客对访客的攻击即使云服务供应商也极难检测到。但请务必注意，此类攻击大多只具有理论意义。虽然可能发生旁道攻击，但其是否能实际发生有待进一步考证，因为这些攻击需要底层执行平台保持一致性，而这在现实环境中并无法得到保证。此外，VM、容器或管理程序环境中访客对主机的升级攻击也很难发觉，甚至更难被利用。这就使漏洞所导致的利用大量访客或特定目标的行为变得不太可能。

因此，尽管这对攻击者而言是个重要的高权限地位，但攻击成功的可能性很低，因为困难性、成本和机遇因素让这种利用行为不大可能实际发生。

3.3 应用程序服务攻击

虽然讨论应用程序执行架构在很大程度上超出本文档的范围，但请务必注意，若该层级遭受攻击，则面临的风险最大。如果已按照本指南的建议正确配置服务生态系统，攻击者将从对网络基础设施的攻击转为对应用程序自身进行攻击。

应用程序代表着任何产品或服务中最复杂的层级，并且始终存在攻击者通过多个技术层提升其权限的可能。因此，尽管本文档旨在推动人们关注如何使网络基础设施免遭攻击，但其在很大程度上也推动将焦点放在攻击更有可能成功的*地方*。

若要降低攻击的可能性，请查阅大量记录应用程序安全的文本（例如 OWASP 安全应用程序设计项目 [5]），以便尽可能安全地实施应用程序执行架构。

3.4 隐私

虽然合作伙伴系统旨在使用数据/指标或其他以用户为中心的组件为整个系统提供增值功能，但有关合作伙伴所执行的安全级别从未有过保证。不要简单地将信息传递给第三方，必须对应递交的数据类型、有形回应类型以及应如何保护信息等方面进行评估。

虽然可通过合同和保险条款减弱法律责任，但由于第三方的失职仍可能造成客户流失。组织不应冒损失业务的风险，而是需评估第三方工程团队，以确定其基础设施、应用程序和 API 应用的安全级别。若安全级别不足，建议寻找替代合作伙伴。

3.5 恶意对象

第三方系统旨在向客户提供信息或多媒体。实现这一点的显著途经就是借助广告。各类型文件的结构很复杂，软件难以进行正确解析。广告网络是一种引人关注的恶意软件传播渠道。内容分发网络 (CDN) 也是传播恶意软件的潜在渠道。提供复杂多媒体类型或代码包（网络或可执行格式）以渲染动态信息为目标的任何系统都可能传播恶意软件。

因此，企业必须评估经特定渠道传递的不同类型的技术。企业必须决定哪些内容可以传递，哪些内容不能向其客户传递。例如，广告公司可能希望通过物联网公司为合作伙伴提供的代理服务应用程序向客户系统传递 Java 代码。企业需要决定在特定环境下运行的客户系统是否更易遭受 Java 技术的攻击。若发现确实易遭攻击，企业可能会禁止 Java 通过，但会允许其他技术通过，如超文本标记语言 (HTML)。

由于恶意软件形式多样，从多形态的文件类型到 Adobe Flash、Java 以及多媒体漏洞，因而没有一个统一的方法来确保终端用户的安全。一个简单的解决方案是工程团队严格执行相关政策，即在其通道中*应*使用哪种技术，以及其用户将*如何*受到影响。监测子系统和沙盒要落实到位，以确保客户系统上呈现的任何软件少被滥用。

3.6 验证和授权

合作伙伴通常提供仅特定于某些用户的服务，可能包括用户可选择订阅的有偿服务。这还可能代表着一种用户可以对系统进行验证的方式，但使用与独立知名技术共享的凭证，例如来自网络服务供应商、社交网络基础设施以及现有的 M2M 或物联网管理实体的现有验证 API。

虽然这些都是跨平台共享技术的绝佳方式，但工程师必须确保技术不会无意间使用凭证以滥用未明确授权给第三方服务的权限。例如，某些平台 API 允许将权限限定在用户接受或拒绝的类别中。这样可使用户根据其特定的隐私需求调整使用体验。若平台不能提供细化的安全权限，应列出其*确实*要访问的技术。

工程团队必须要求其合作伙伴提供可行的细化权限，以确保服务的取消不会无意间使得在订阅取消后仍继续提供用户数据访问。

3.7 误报和漏报

虽然检测和日志服务是扩充现有安全基础设施的绝佳方法，但必须对其慎重评估以防误报和漏报。因为这些系统仅解释源于物联网产品或服务内各生态系统的数据，并且这些系统并非由内部的工程团队研发，其只能对事件提供主观的看法，而且也不能正确辨别攻击行为是否真实发生。

因此，必须借助 IT 和工程团队以确定可疑事件是否实际上由恶意行为引发。这样，监控团队就不会禁止合法用户访问系统。若该过程自动发生且存在错误，许多用户可能会由于客户应用程序或基础设施异常所引起的误报而无法使用其合法服务。发生可疑的重大事件时，IT 和工程团队应查看数据以评估攻击是否的确发生。

此外，工程师还必须对通过模拟通道所获得的信息进行建模。特别是在数据必须被极速处理的生态系统中，若不能完全信任所获取的数据，而应用程序又无法正确评估最安全的行动措施，

误报和漏报可能会造成严重后果。值得注意的是，依托充足的时间、完备的技术和专业知识，所有模拟数据都能模拟出数字系统。

4 常见安全问题

本文档中，服务安全按优先性划分为若干建议。但是在实际应用中，从实际角度评估建议会更有帮助。工程师通常根据技术或商业影响目标开始制定一系列建议。本部分从终端的角度概述共同目标，以及与实现该目标相关的建议。

4.1 我们如何应对克隆？

要将物联网服务供应商制造的正版设备与复制或“剽窃”（克隆）的设备区分绝非易事。所有物联网服务供应商都不会愿意向未授权的终端提供服务，因为服务供应商必须为 CPU 时间、带宽、磁盘存储器及其他资源支付费用。无论设备是否由物联网服务供应商制造，组织都必须付费。

此外，组织必须能够辨别其终端构架是否被破坏。这样，组织就能对被*克隆*为同一设备多个实例的设备及时作出反应。毫无道德的制造商或要冒充特定用户的攻击者很可能会进行此种克隆。

请阅读下列建议以获取有关如何使用服务应对克隆的帮助：

- 定义组织信任根
- 使用网络验证服务
- 通过服务生态系统强制验证
- 定义应用程序层验证和授权

4.2 如何通过终端进行用户身份验证？

物联网最重要的概念之一是将终端验证与用户验证相分离。终端可由其可信计算基进行验证，但*用户*验证却是一个依赖于终端 TCB 的单独过程，本概念最重要的一点是评估通信通道对用户验证的可信赖程度如何。

譬如，若因没有终端 TCB 或使用执行较弱的终端 TCB 而导致终端的可信度较低，则依赖于终端软件/固件而运行的用户验证机制不可信赖。这意味着任何通过终端设备进行的用户验证均不能视作已验证。

换言之，若验证方案能轻易被绕过，则一个构架良好的终端 TCB 也无法有效验证终端用户。因此，服务生态系统必须依赖于终端可信度以及验证机制的执行，以确保服务生态系统能够保证只有正确的用户登入系统中。

请参考下列建议以获取有关如何处理此类复杂问题的帮助：

- 执行服务可信计算基
- 定义组织信任根
- 定义明确的授权模型

- 使用网络验证服务
- 通过服务生态系统强制验证
- 执行高强度密码政策
- 定义应用程序层验证和授权

4.3 服务如何识别异常终端行为？

管理分散式物联网网络终端的最大难点之一在于判断终端是否有异常行为。无论从安全角度，还是从可靠性角度而言，这一点都非常重要。异常行为通常表明固件或硬件出现问题，也可能表明组织需要修复意外问题。然而，若该行为发生在物联网服务供应商无法进行分析的网络部分，则这些指标均将丢失，使组织的优势大大减弱。

若要解决这一问题，则要求具备检测终端、网络层及服务生态系统行为的能力。然而，若未建立正确的基础设施、服务及合作伙伴以收集这些数据点，则组织将无法得到必要信息以判断是否存在问题或问题是否与安全或可靠性有关。

请从服务生态系统角度评估下列建议：

- 定义暴露于公共互联网的系统安全基础设施
- 定义系统日志和监控方法
- 定义通信模型
- 使用网络验证服务
- 执行输入验证
- 执行输出过滤
- 使用合作伙伴增强型监控服务
- 使用专用 APN 进行无线连接
- 定义假阴性/阳性评估模型

4.4 服务如何限制异常终端行为？

终端被确认为行为异常后，服务应确定对哪些资源进行限定或限制。这一问题关乎服务基础设施的每一层。

譬如，对于一个可使用无线网络的终端，若不时会重复错乱地接入和断开移动网络，则该终端应当被强制禁用，直至该无常行为得到解决。再譬如，一处攻破的终端被攻击者用于攻击后端服务。这种情况下，后端服务应当彻底禁止被滥用的终端访问服务。

如何处理各情况取决于物联网服务供应商及其业务目标和事件处理规定。为帮助制定这些指南，请参考下列建议：

- 定义组织信任根
- 定义暴露于公共互联网的系统安全基础设施
- 定义事件响应模型
- 定义恢复模型
- 定义废止模型

- 定义通信模型
- 定义泄露数据的违规政策
- 通过服务生态系统强制验证
- 使用专用 APN 进行无线连接
- 定义假阴性/阳性评估模型

4.5 我如何能够判断服务器或服务已被攻击？

尽管终端的异常现象更加难以发觉，且多数攻击需要大量的行为分析来捕获，但服务生态系统却非常简单直接。服务及服务器部署所在的环境由管理云端或服务器基础设施物联网服务供应商或其合作伙伴严格控制。因此，组织及其合作伙伴可以使用现成的监测和诊断系统来识别并控制潜在问题。

请参考下列建议以获取帮助：

- 定义管理模型
- 定义系统日志和监控方法
- 定义事件响应模型
- 执行输入验证
- 执行输出过滤

4.6 服务器若被攻击，我能够采取哪些措施？

若服务器已被确定为受到攻击，则管理团队需尽可能快和高效地解决该问题。解决问题的复杂性通常在于判断哪些资源、信息和账号处于危险状态。在架构较差的环境中，攻击产生的影响通常无法量化。因此，组织*必须*实施计划以解决安全漏洞，*并须*同时保护现场处于风险之中的资产。生态系统及漏洞得到保护后，组织随即可以实行计划以重建受影响的技术。

请参考下列建议以获取更多信息：

- 定义事件响应模型
- 定义恢复模型
- 定义废止模型
- 定义安全密级
- 定义数据类型集分类

4.7 管理员应如何与服务器和服务交互？

开发一款能够保证服务生态系统安全的管理模型，是物联网服务架构的重要组成部分。管理层数较多，每层都应由工程师及安全团队仔细核查。譬如，管理服务器（无论使用的是虚拟、微服务或是 Unikernel 架构）的管理员必须能够通过安全可靠的通信通道与活动服务器交互。管理网络应用程序的管理员通常在同一网络通信层与应用程序交互，但使用的是代码中嵌入的特殊应用程序。

无论管理是否需要，界面访问均应受限，以此来限制攻击者与技术交互或滥用技术的能力。请参考以下资源：

- 定义暴露于公共互联网的系统安全基础设施
- 定义管理模型
- 定义明确的授权模型
- 定义通信模型
- 使用专用 APN 进行无线连接

4.8 服务架构如何限制攻击影响？

物联网网络的一项卓越属性是其能够将服务与特定消费者进行匹配的独特能力。在网络服务中，每位用户都必须能够从任何类型设备甚至任何地点与服务交互。物联网技术并非如此。物联网技术通常要求特定的终端设备与物联网服务交易。因为这种差异，服务器生态系统架构者能够利用终端与消费者之间的一对一关系，将终端的访问限制在后端数据。

设想这样一个场景，终端正在将传感器指标传回后端服务。微服务架构中，服务生态系统针对特定消费者，可能会配置特定的微服务或 Unikernel。利用该架构，工程师能够确保微服务*仅*提供传递*特定个体消费者*数据及服务所必需的资源和接入能力。

这意味着若服务被攻击，且该终端是能够与此特定服务进行通讯的唯一技术，则攻击该服务将毫无利益可言，因为攻击所获得的访问权限将仅限于终端*已经*能够使用的资源。从根本上讲，该攻击的收益为零。

请参考下列建议以获取帮助：

- 执行服务可信计算基
- 定义引导方法
- 定义暴露于公共互联网的系统安全基础设施
- 定义永久存储模型
- 定义管理模型
- 定义废止模型
- 定义明确的授权模型
- 在可能时提供服务器
- 定义应用程序执行环境
- 虚拟机受到攻击

4.9 服务架构如何能够减少攻击发生时的数据丢失？

物联网架构的另一有趣属性是可以减少数据丢失。这一点类似于将服务限定于特定用户的方式。用户通过验证后，数据也能限定于特定用户。然而，由于数据库及存储基础设施开销的原因，数据无法按用户分开进行存储。

因此，服务会配有单独的令牌，使其能够在存储基础设施范围内代表特定用户进行操作。这样，能够访问数据存储环境的攻击者也许能够接入服务，但除被攻击的用户外，攻击者将无法与其他用户的数据交互或者对其进行检索或修改。

从网络层角度而言，同时也要求减少服务器生态系统发往互联网的流量。出口控制会迫使攻击者通过特殊通道传递知识产权或客户数据。这可能会导致传递大规模数据的难度增加，或迫使其通过通信层进行，而该层可在事件发生期间检测并切断通讯。

请参考下列建议以获取更多信息：

- 定义引导方法
- 定义暴露于公共互联网的系统安全基础设施
- 定义永久存储模型
- 定义安全密级
- 定义数据类型集分类
- 在可能时提供服务器
- 定义应用程序执行环境
- 默认开启或故障时开启防火墙规则

4.10 服务架构如何能够限制未授权用户的连接？

利用通用物联网架构的一个好处就是可以限制未授权互联网用户直接接入后端服务的能力。多数 Web 应用程序不具备这一特性，而必须向公众开放。但在物联网中，由于终端是必须接入特定服务的实体，因此可以使用虚拟专用网络 (VPN) 来限制后端服务的访问者。可以依照标准互联网协议或使用移动业务（如专用 APN）执行此步骤。请参考下列建议以获取更多信息：

- 定义暴露于公共互联网的系统安全基础设施
- 使用专用 APN 进行无线连接

4.11 如何降低远程漏洞攻击的可能性？

一直以来，Web 应用和服务的远程漏洞攻击都是基础设施管理员所关心的问题。管理员们每天都要防范攻击者，避免其侵入内部网络，或是获取有价值的资源。减少攻击者对服务生态系统攻击的唯一途径，就是减少易于维护的可管理服务组中可能的目标数。对于架构而言，第二重要的扩展是底层架构设计：执行架构、操作系统配置、部署工具链、编程语言安全以及其他定义应用程序运行安全性的选项。这些选项能区分应用程序崩溃和基础设施受到攻击之间的不同。

有关降低远程漏洞攻击可能性的详情，请参见：

- 定义暴露于公共互联网的系统安全基础设施
- 定义更新模型
- 执行输入验证
- 执行输出过滤

- 默认开启或故障时开启防火墙规则
- 定义应用程序执行环境
- Rowhammer 漏洞与类似攻击
- 虚拟机受到攻击

4.12 服务如何管理用户隐私？

在物联网服务供应商的发展过程中，一定会和使用消费者数据的组织进行合作，并且这些组织的使用方法也在不断的创新。然而，使用数据的代价是牺牲消费者的隐私。消费者应当有权决定可以与合作伙伴分享数据的类型和使用范围。此外，还应对合作伙伴使用数据的方式做出特定的要求。使用授权模型能够实现这一点，但是这意味着需要讨论的范围扩大，包括隐私、法律后果、商业保险等方面。

组织内部开始讨论之前，请查看以下建议：

- 定义安全密级
- 定义数据类型集分类
- 定义明确的授权模型
- 定义泄露数据的违规政策
- 评估通信隐私模型
- 定义第三方数据发布政策
- 创建第三方数据过滤器
- 创建使用者 API 以控制隐私属性

4.13 服务如何提高其可用性？

在现代互联网中，拒绝服务 (DoS) 攻击或分布式拒绝服务 (DDoS) 攻击很常见，每家公司都应对此类攻击有所防备，即使是遭受长时间攻击也依然能够保证在线。由于实行此类攻击无需太多技巧，并且实现的工具可以在网上随时获得，因而非常普遍。实际上，不怀好意的人士可以使用在线服务，雇用攻击者向特定的目标发起分布式拒绝服务攻击。

因此，针对服务可用性建立新模型以应对这种威胁。在创建服务生态系统时，请考虑以下建议：

- 定义暴露于公共互联网的系统安全基础设施
- 定义系统日志和监控方法
- 定义事件响应模型
- 定义恢复模型
- 定义通信模型
- 默认开启或故障时开启防火墙规则

5 重要建议

在开发安全终端时，应始终遵照以下建议。以下重要建议定义了安全终端架构。如果不遵循这些建议，终端安全配置将不完善，很容易被攻击者滥用。

5.1 执行服务可信计算基

可信计算基 (TCB) 由一系列硬件、软件、协议和政策组成。TCB 是所有给定计算平台的基础，并且必须定义应用程序能够可靠、安全并且高质量运行的环境。

在任何指定的系统类别上都可创建并部署 TCB，例如移动设备（智能手机）、物联网终端，甚至服务生态系统中的服务器。TCB 由相类似的技术组成。然而，根据系统类别的不同，这些技术可能会呈现不同的特点。例如，在云服务器中引导 TCB 与引导终端就有很大不同。

在服务生态系统中创建 TCB 意味着定义推出应用程序形象的方式。在此环境下，形象代表原始二进制数据，包括应用程序可执行文件、配置文件以及元数据。通常，这些事物共同组成了应用程序形象，或简称形象。在大多数现代服务生态系统中，系统可以根据需求进行复制、启动或挂起，以适应计算环境的变化。这意味着 TCB 必须定义一种方法，使得系统在维持持久安全模型的同时，还可有效缩放。

要正确做到这一点，团队必须：

- 实现计算平台的标准化：
  - 选择一组物理服务器模型
  - 选择一组云平台或虚拟机 (VM) 形象
- 定义在计算平台上运行的应用程序、库和配置文件组：
  - 定义容器环境（如果适用）
- 生成由以上定义的集合所组成的应用程序形象
- 使用层级 TCB 签名密钥，为形象档案的签名加密
- 安全存储归档和签名

执行此任务组将生成可在特定层部署的已批准应用程序形象。每个层都有最适合该层的不同硬件和应用程序模型。例如，数据库硬件与应用程序层对于性能和存储的要求就有很大不同。存储层与数据库层组硬件存储方面的需求相似，但在性能要求上仍然不尽相同。将每个层的定义都标准化后，将生成可在各个硬件平台上部署和验证的形象。

部署 TCB 的困难源自：

- 建立组织信任根以管理形象的加密签名
- 建立各个形象的签名程序
- 建立各个形象的验证程序
- 建立自动推出形象但要进行验证的程序

请考虑使用以下组织提供的材料，以帮助实施此建议：

- GlobalPlatform Card Specification [11]

- Trusted Computing Group’s TPM Specification [6]
- GlobalPlatform TEE Internal Core API Specification [12]

5.1.1 风险

如果没有明确定义的可信计算基，计算平台将无法验证其目前是否在工程团队批准的配置下运行。由于应用程序子系统必须能够判定其是否遭到攻击者的攻击，因而这一点至关重要。TCB 可用于修复此风险，并为所有的网络通信提供安全层。

5.2 定义组织信任根

组织信任根是一个基于证书或公钥的系统，用于验证组织中的计算平台实体。服务生态系统中的每个计算平台必须在网络通信时进行加密验证。这就减少了内部或拥有高权限网络地位的攻击者假冒或滥用特权系统信任的可能性。

要创建组织信任根，只需要执行以下操作：

- 构建或获取硬件安全模块 (HSM) 以存储组织根机密
- 生成根机密和/或证书
- 确保机密的私有部分安全储存
- 产生一个或多个签名密钥，作为层 TCB 签名密钥
- 使用组织根签署签名密钥的公共部分
- 确保在未经业务和工程领导的验证及授权时，无法使用这些密钥

每次定义一种新的层系统，就可使用签名密钥签署其独有的密码密钥或证书。如果其他系统与这个新系统连接，则可通过验证由组织根定义的信任链来验证该系统身份。

这将会加密验证信息是否由代表系统的公共密钥签名。然后，将会验证签名密钥生成的该系统独有公共密钥的签名。之后，客户应当验证该签名密钥确实是由组织根验证的密钥。

在组织中，由于每套证书或机密知道的人越少越好，并且定义的政策和程序也应限制使用者和使用时间的范围；客户越接近根链，信任度应当越高。

必须明确定义服务，以向服务生态系统中授权的对等方展示身份验证功能。例如，使用证书或机密链的验证方法不能单独使用以保证安全性。必须启用相应服务，以验证证书当前是否已经失效。根据底层基础架构要求的不同，可能还需要使用另一服务，以验证服务器或短期服务的身份。

在定义信任根时，请考虑：

- 每个机密都要进行保护，以防止滥用
- 每个机密的内部使用必须进行可验证地跟踪和监控
- 每个获得机密使用批准的个人在访问机密时，必须进行多重因素验证
- 定义一系列政策和程序以确保一致和安全的使用，这一点具有挑战性
- 创建废止或撤销证书的流程具有挑战性
- 识别密钥是否遭到滥用具有挑战性

- 选择一套正确的加密算法可能不太容易

有关信任根概念的更多内容，请考虑以下信息来源：

- 可信计算组
  - TPM 规范 [6]
  - TCG 保护物联网安全指导 [7]
  - ISO 11889
- PKI 规范
  - RFC 2510
  - RFC 3647

5.2.1 风险

不使用组织信任根的风险是单个密钥遭到任何攻击都可能导致整个生态系统被攻陷。将组织分为层次结构，再为层次结构部署不同的密钥，就可以根据密钥关联的应用程序或子组织优先级，定期循环使用密钥。

5.3 定义引导方法

为了能让应用程序正常运行，其必须在可靠、优质和安全的平台上以一致的方法加载并执行。TCB 定义建构此平台的方式，但引导模型定义应用程序在其上运行的方法。

为了有效定义引导模型，需要考虑以下方面：

- 定义能够使应用程序通过加密方式向对等方表明自身身份的 API
  - 考虑使用由值得信赖的行业领导者定义的现有 API
- 定义应用程序验证终端、服务同行以及合作伙伴的方法
- 定义应用程序的配置方式
- 每个不同的应用程序都应有独特的身份，尤其是在不同层运行的应用程序

尽管应用程序通过加密方式向对等方表明自身身份的方式看似直观，但 API 却无需如此，其流程不太直观。这是因为在引导模型中，必须考虑*对应用程序*配置加密身份的*方法*。应用程序如何获得其身份？身份获得是否安全？在需要更新或更改机密的情况下，撤销身份所用机密的过程是什么？

在运行时，应用程序需要特定资源以便有效执行。应用程序必须能够与所有外部服务、终端以及此流程中涉及的所有合作伙伴进行通信和相互验证。

应用程序的配置往往决定了流程的安全程度。应用程序应当执行配置，并且不能修改。应用程序或滥用应用程序基础设施的人员应当无法轻易地更改应用程序的配置。

使用组织信任根为整个生态系统中部署的每层定义信任模型。如此，就能让各个独立的应用程序拥有唯一的加密身份。这样可以帮助对等方区分数据库服务和应用程序服务。

5.3.1 风险

如果没有明确定义的引导模型，系统将无法验证运行所需的各个层级。从根本上而言，整体技术的各个方面没有信任分层。缺乏信任层将增加复杂度，导致出现漏洞而被攻击者滥用。

5.4 定义暴露于公共互联网的系统安全基础设施

对于可公开访问的服务，需要几项安全和可靠性技术以保持服务的可用性、机密性和完整性：

- 防 DDoS 基础设施
- 负载均衡基础设施
- 冗余系统
- Web 应用程序防火墙（可选）
- 传统防火墙

这些附加技术应置于应用程序层之前，以确保其不会被公开攻击者所操纵。通信安全模型会禁止匿名第三方访问系统或降低这种可能性，但这些技术也会将降低攻击者使系统瘫痪的能力。

前端安全应用于服务执行的*所有*协议。例如，如果在 IPv4 和 IPv6 上提供服务，则这两个协议上的服务应该使用相同的安全限制。如果可以通过 TCP 和流控制传输协议 (SCTP) 使用服务，则这两个协也应使用相同的安全限制。如果端口不提供连接至物联网产品或服务的公共服务，则应该不能访问。

确保在任何可能的情况下，控制流入*和*流出过滤。虽然流入过滤可以阻止一系列攻击，但是对于可公开访问服务的任何攻击还是会导致服务生态系统受损。此时必须执行流出过滤，以确保攻击者无法使用服务生态系统的受损组件在生态系统中横向移动。另外，借助流出过滤，攻击者将生态系统的重要数据转移至其所控制服务器的难度增加，这样管理员就有更多时间发现并隔离攻击者。

多个组织在简单 API 模型中提供这些服务，而该模型可植入指定技术。这样就可以轻易使用技术。在服务供应商系统中注册并配置应用程序无需太多的工程工作。请咨询您的服务供应商，以确定在您的环境中执行其安全技术的最佳方式。

请考虑使用以下组织提供的材料，以帮助实施此建议：

- Amazon Best Practices for DDoS Resiliency：
  - https://d0.awsstatic.com/whitepapers/DDoS_White_Paper_June2015.pdf
- Arbor Networks DDoS Mitigation Best Practices：
  - https://www.arbornetworks.com/images/documents/Arbor%20Insights/AI_DDoSMitigation_EN2013.pdf
- Cisco DDoS Defence Guide：
  - http://www.cisco.com/web/about/security/intelligence/guide_ddos_defense.html

5.4.1 风险

考虑到互联网的不稳定性，公用服务和应用程序都必须有安全基础设施。随机 DDoS 攻击经常发生，且原因不明。只需数百美元就可以在“地下市场”买到 DDoS 服务。因此，企业或企业客户的攻击者不是此类攻击的唯一作恶者。随机攻击有时只是为了看看是否可以成功攻破系统。最好时刻准备应对此类攻击，以确保重要的物联网服务不会被意外攻破。可用性是物联网产品或服务的重要指标。

5.5 定义永久存储模型

现代计算中的应用程序环境通常周期较短，如基于容器的系统或云环境。因此，分配至这些系统的存储容量不会太大，也未设计为供长期使用，应用程序并不能将这些技术作为永久存储。另外，这些系统可能被定义为按需实体，可能和集中化不同。也就是说，其他系统无法定义*哪个系统*拥有足够存储空间供永久使用。

因此才需要中央存储系统，并严格保护其安全。由于此类环境的任何指定临时系统都必须能够访问存储系统，任何受攻击的短期服务器或服务将可以访问其他许多服务器或服务使用的永久存储实体（或层）。攻击者可以通过这种方式有效地横向（或者也有可能垂直）攻击任何指定网络。

为限制此类行为，每个服务器或服务都应该可以访问永久存储，但应基于其代表的应用程序，以及更重要的应用程序所代表的*唯一终端*、*合作伙伴或用户*而存储信息。最后一部分是最重要的一点，因为代表指定*身份*强制永久存储访问将限制短期服务器或服务对数据的访问。

也就是说，攻击*短期系统*的攻击者只能影响代表连接至*同一短期系统*的身份而存储的数据。如果该系统只能访问一个身份的数据，攻击者将无法使用该系统的受损而横向移动至其他账户。它们只能访问该单个身份的信息。这可以极大地限制攻击者利用一个漏洞而攻击整个重要系统的能力。

5.5.1 风险

如果未定义安全的永久存储模型，就不会有架构可以执行用户唯一的属性以安全地与其他资产分离。这种情况下，如果令牌被攻破，攻击者就可以访问存储设备，导致多个用户的数据受到泄露。但是，永久存储模型可以将入侵隔离至单个用户或带有加密数据的单个存储技术。在任一情况中，入侵的范围都将大幅减少，让组织有更多时间及时应对并解决给用户和企业带来的威胁。

5.6 定义管理模型

管理人员必须可以访问每个系统，以寻找故障并诊断应用程序错误。如果未充分设计管理模型，则在短期服务或服务器的环境中，这一点将会非常有挑战性。

要实现此功能，请确认管理团队与各层各个系统交互的方式。应该设置验证边界，如 VPN，以便将系统彼此分开。确保管理团队验证各个层级。

还要确认管理员与系统交互的方式。是否可以像 VM 一样对系统进行快照？是否使用终端？是否使用远程安全外壳 (SSH) 与系统交互？是否有 API 监控并分析系统指标，如 CPU 使用率、磁盘使用情况和网络使用情况？这些是否可以用于寻找故障或发现异常情况？

除模型外，还*必须*定义以下事项：

- 管理员如何验证环境
- 如何将管理员验证用于确定物理身份：
  - 利用双因素验证 (2FA)
- 如何对系统进行快照
- 如何进行更改并对其进行跟踪

5.6.1 风险

如果环境中没有构架良好的管理访问路径，则最终通常会使用特别方式访问生产中的系统。这经常指向开放给公共连接的管理端口或提供诊断的服务，但不限于被第三方使用。清晰的管理模型可以减少攻击者可能用于获取对重要物联网资源的特权访问的潜在路径。

5.7 定义系统日志和监控方法

必须对每个系统进行监控，以便管理员和信息技术 (IT) 人员能够检测并诊断异常情况。必须从多个维度进行监控。例如，基础设施级别的网络监控有助于诊断网络组件受到的应用程序攻击或 DDoS。层级监控可以确认特定应用程序或基础设施部分是否受到攻击。系统级别的监控可以定义单个应用程序或应用程序平台是否正在遭到攻击或已经被攻破。

很明显，这需要多个级别的监控，并应将信息合并到可传输至监控团队的资源中。多种专业应用程序都提供这种技术，并可将指标转换至可视化系统，供 IT 专业人员和系统工程师使用。

意味着存在攻击行为的异常可能包括但不限于：

- 网络流量增加
- 在*奇怪*的方向（尤其是流出）上网络流量增加
- 从不需要流出的资源中流出网络流量
- CPU 使用率异常
- 系统 GPU 使用没有可视化界面，但 GPU 是 CPU 的一部分
- 磁盘或网络存储使用情况
- 特定主机的系统时间出现异常变化

用于获取异常的监控系统已经就绪，但其使用方式可能特定于组织使用的应用程序或基础设施。请咨询提供监控系统的企业，以确定如何以对具体实施中最有效的方式获取并解释相应指标。

不同的层级在表示存在攻击或受损的异常方面可能存在差异。评估每层的具体指标。

请考虑使用以下组织提供的材料，以帮助实施此建议

- Amazon EC2 Monitoring Documentation
  - http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/monitoring_ec2.html
- Google Cloud Monitoring
  - https://cloud.google.com/monitoring/
- Microsoft Azure Monitoring
  - https://azure.microsoft.com/en-us/documentation/articles/best-practices-monitoring/
- DigitalOcean Monitoring Tutorials (General)
  - https://www.digitalocean.com/community/tags/monitoring?type=tutorials

5.7.1 风险

系统监控技术是物联网安全模型的重要属性。如果没有监控，就无法确定在重要服务组件中是否发现漏洞。监控可以让管理员快速诊断服务和基础设施中的痛点，帮助区分安全事故和软件故障。

5.8 定义事件响应模型

只检测潜在入侵或持续攻击远远不够。组织必须能够及时对攻击作出反应和应对。如果系统受损，清理或切断系统还不够。组织应该诊断攻击源、为系统打补丁，并在所有现存基础设施中部署补丁。

如果使用的是基于容器的环境，其中运行的克隆应用程序使用的配置易受攻击，则会比较难以执行。应用程序系统必须能够检测出“重启”或“更新”事件，此时应用程序连接会转交至云端另一系统，或用户被迫退出登录，以允许更新。

但是无论执行模型如何，工程团队都必须能够以一种可以取证分析的方式捕获到指标。这些政策和程序必须保持不变，并获得法律团队（可能还有保险团队）的批准，以验证包含的信息是否适合执法人员 (LEO) 使用。合规有助于确保企业不仅遵守当地和联邦法律，还提供可在法庭中使用的受攻击实例。

捕获到实例后，应评估整个系统各个方面的日志、指标及其他可证实目标事件的数据。应捕获所有数据并存储于安全系统，以供法律审查。

请考虑使用以下组织提供的材料，以帮助实施此建议：

- CERT Recommendations for Creating a CSIRT
  - http://www.cert.org/incident-management/products-services/creating-a-csirt.cfmhttp://www.cert.org/incident-management/products-services/creating-a-csirt.cfm

5.8.1 风险

缺乏事故响应模型的组织将花费更多时间组织资源、确认受损系统、隔离系统，并查看系统了解信息。这也会大幅度减缓为打补丁并恢复指定系统应做的工作。这种准备不足会让攻击者有

机可乘，将攻击在指定环境中横向或垂直移动。响应时间增加会导致攻击入侵更加严重。组织应时刻准备立即应对事故，以缩减攻击者控制服务关键部分的时间。

5.9 定义恢复模型

无论用户或应用程序因为安全入侵还是硬件故障而受到影响，都必须进行恢复。应制定恢复应用程序层的信息和功能的程序。程序必须适用每个应用程序和每层的情况。

例如，如果应用程序从终端收集有关某项操作输出的信息，而存储故障不允许应用程序固化永久存储器中数据的输出，应用程序可以：

- 进行多次存储尝试，直到成功（可能需要一直尝试）
- 进行有限次数的存储尝试，直到成功或达到失败次数上限
- 立即失败，可能丢失指标
- 再次向终端请求相同的数据（可能永远无法使用）

必须选择最适合应用程序和业务要求的方法。这还是要取决于应用程序的具体情况，并且在指定系统外不易建模。

让工程和业务领导者参与决定如何恢复失败或受损的应用程序，尤其是在涉及用户活动的情况下。

对于已经证实被攻击者入侵的系统，则必须设定模型，以验证在恢复前已对应用程序或系统充分打补丁。如果不制定该政策和程序组，易受攻击的系统可能会被再次部署至服务生态系统，从而引发后续攻击行为。

5.9.1 风险

恢复模型可以确保正确修复信息、应用程序及配置。如果没有恢复模型，团队可能无意中将易受攻击的子系统再次部署至服务器或基础设施中。另外，数据库或存储环境中可能已被攻击者操纵的受污染数据，可以在多个系统中复制，从而无意间传播恶意软件或更改的数据。攻击者可以滥用事故恢复中的薄弱环节，令原本就需付出很多代价的事故雪上加霜，而恢复流程将降低攻击者这方面的能力。

5.10 定义废止模型

组织部署的每个系统和使用的各层都有生命周期。即使组织几十年来一直利用同一种产品或服务，用于驱动该产品或服务的技术也会改变。因此，不仅要制定计划以设计并执行产品或服务，还要有计划*废止*该产品或服务。

此流程可以保证所有技术的废除和废用，都可让攻击者无法利用该技术的身份或使用其设施。例如，一个简单的实例就是公司被母公司收购后特定产品的域名。如果产品重命名，并且域名迁至母公司域名，则攻击者可能获得当前失效域名的所有权。如果攻击者对该域名发布密码证书，并依然使用旧域名下部署的技术进行交互，则由于缺少废止该产品或服务的程序，将会产生巨大的安全漏洞。

指定产品或服务的架构、执行和管理过程中使用的每项技术，都必须进行分类并根据其可用性进行评估。一旦技术不再可用，可根据其模型进行废止。这样，工程师和业务领导者就可以将该技术迁移至更合适的创新集，而底层平台中不会存在漏洞。另外，还可以确保不再向合作伙伴和用户提供的产品将终止其生命周期，使得攻击者无法在业务关闭后利用其进行攻击。

5.10.1 风险

缺乏废止流程可导致终端和服务受到竞争者或攻击者的入侵。这可能是合法行为，因为如果组织释放对某些对象的访问，如域名、电话号码或其他可更新服务，攻击者或竞争者将有权获取这些对象，即使这看上去并不道德。这可能使设备或服务受到不择手段的滥用甚至恶意行为。

5.11 定义安全密级

为了恰当有效地管理与合作伙伴组织的交互，必须定义安全密级。这不仅将为组织内部政策在数据安全方面奠定基调，而且可帮助定义合作伙伴组织用于业务数据、自身数据及客户数据的安全等级。

虽然应对该流程进行调查，并针对组织进行定制，但大多数数据安全密级政策应从以下密级开始：

- 公开 - 任何实体都有访问权限
- 机密 - 用户必须授权发布
- 秘密 - 用户特定的数据
- 绝密 - 组织特定的数据，永远不能发布

定义基本密级后，组织必须评估如何为数据类别设定安全密级。即评估密级如何应用于实践，而不仅停留于理论。从业务*和*工程角度出发，确定应制定的政策和程序。

这样组织不仅可以制定技术政策，还可以构建支持技术要求的业务政策。工程团队可更加容易地将这些要求传递至试图有意或无意违反政策的合作伙伴和内部组织。

安全密级标准化后，务必要评估安全密级模型如何受到企业及其用户隐私要求的影响。组织必须抽时间将隐私模型应用于安全密级，以便设定用户数据的保密性，并在合作伙伴试图访问可能泄露用户的特定资源时，保护用户隐私。将隐私融入安全密级中之后，如果合作伙伴希望获取某类隐私数据，将需要获得业务领导者*和*用户的批准。用户*必须*可以选择保护其隐私数据，而且必须能够限制其数据泄露给第三方。

5.11.1 风险

为构建有效使用安全的解决方案，必须设定安全分类模型。为保护信息，这些信息必须量化，从而根据相应政策和程序制定出相应的控制措施。如果没有这些模型，工程师可能会根据其对所涉风险的理解，过于严格执行安全措施，或者根本不执行。包括工程和业务领导者在内的整个团队应确定数据对业务的意义，以及如何通过一系列成本效益高的合理控制措施保证数据安全。

5.12 定义数据类型集分类

确定安全密级后，组织应定义整体物联网产品或服务使用的数据类型。这样组织可以清晰定义获取、生成并向物联网系统对等方传播的信息类型，以及组织应如何处理这些数据类型。该数据将向整个物联网环境中使用的整体组件提供相关状况和价值。

本文档并非旨在为所有与特定组织相关的数据类型建模，但仍有某些类型如下所述：

- 用户
- 操作
- 图片
- 可编辑文档
- 个人识别信息
- 受保护的健康信息

一条信息可能有一个或多个*类型*，但数据本身只有一个*安全密级*。*类型*可以确认数据代表的含义以及应该如何处理，而*安全密级*则代表着使用信息的*方式*、*地点和时间*，以及可能分享的*对象*。

定义多种数据类型并确定其密级是一个较长的过程。这样可以为业务设定组织标准，让工程团队围绕数据及密级执行技术控制措施。工程和业务领导团队日后与合作伙伴就如何分享和处理数据进行协商时，这会起到很大的帮助。

5.12.1 风险

和安全密级一样，如果不量化数据及其与业务的关系，就无法围绕数据实施控制措施。这些密级定义信息在系统中应如何使用、应对数据进行哪些保护，以维持恰当的安全状况。如果没有这些密级，工程师就有可能采取过于严苛或过于宽松的安全措施。安全措施应获得工程团队和业务领导者的同意，以平衡控制，保持数据对业务的重要性。

6 高优先级建议

高优先级建议是指只有终端架构需要时才执行的一系列建议。例如，并非所有终端架构都要求防篡改产品保护。应当对这些建议进行评估，以确定业务案例是否需要。

6.1 定义明确的授权模型

隐私模型处理向合作伙伴提供用户信息的方式，而授权模型则定义企业或合作伙伴如何代表用户行动。例如，这在家庭自动化系统中非常有用，合作伙伴指标可以优化特定家庭对加热或冷却的使用。通过授权模型，合作伙伴如果检测到某些指标，就可以更改该用户家庭的加热或冷却控制。

要实现这一点，需要有描述具体授权功能以及如何分配至合作伙伴的类似 GUI。允许用户同意对要求的某些功能进行访问或撤回访问。确保撤销功能可立即生效，以降低滥用的可能性。

必须严格监控系统，以确保合作伙伴不会执行其未获得允许的行动。授权模型的具体控制应允许用户配置合作伙伴何时访问某些功能及其频率。此类属性将提升用户是否可以在遇到潜在滥用或受损（遭黑客攻击）的合作伙伴时控制其系统。

6.1.1 风险

如果没有授权模型，第三方对于用户功能的访问将不受限制。这可能让缺乏控制或受损的第三方获得对用户技术或数据的完全访问。通过创建授权模型，访问仅限于用户允许的属性。这样，用户可以更好地控制对第三方开放的功能和数据，并通过减少大范围攻击的几率，降低物联网服务供应商的风险。

6.2 管理密码体系架构

物联网环境中配置的所有技术，无论是初级低功率终端，还是功能强大的云服务，都必须使用密码体系。要在物联网产品或服务中正确执行安全措施，所用的密码体系必须得到良好架构、管理及调整，以满足不断变化的规范要求。

工程团队必须能够识别是否：

- 其密码算法已被弃用
- 正在使用的密钥具有足够长的位数
- 哈希算法受到碰撞攻击
- 使用随机性较强的数字发生器
- 信息被随机数据充分填补
- 密码协议（如 TLS）紧贴最佳实践
- 使用以隐私为中心的概念（如正向加密）
- 明文密码或 Pin 码通过网络传送
- 使用惯用的密码算法

诸如上述的各条，对维护物联网产品或服务的高质量密码体系架构而言都至关重要。密码解决方案的成功部署与工程团队密不可分，其必须有能力利用最具弹性的密码解决方案，对使用弹性较差解决方案的技术进行弥补。

譬如，最近发现 RC4 算法有重大安全漏洞。若能向配置使用 RC4 的客户安全分发一款补丁，将 RC4 替换为 AES-256，则对 RC4 的风险担忧就会减少。若使用更具弹性的技术（如瞬时 Diffie Hellman 密钥交换和非对称密钥，或 UICC 安全令牌）进行相互验证，则无需使用易受攻击的密码算法即可验证补丁。

用户或终端使用的密码及 Pin 不可在网络中以明文形式传递，即使通信通道已被加密。而应当对密码或 Pin 使用密码散列，以确保密码通道中的任何错误配置均不会暴露密码。该散列应当由密码和至少一个唯一的一次性令牌生成。尽管该令牌通常可以从网络会话中获取，但从存储在终端及服务基础设施内的滚动码中获取该值将会更加安全。这样，对于拥有网络特权的攻击者来说，散列就不具有效益价值，否则可能会导致强制签名攻击。

切不可使用惯用密码算法（内部设计的算法）。始终使用由密码员研发、由专业从事密码安全的监督组织推荐的算法。始终避免使用设计拙劣、弃用或压缩、二进制到文本或其他被误认为密码算法的算法，如 LZO、base64、ROT13 及 XOR。

请参阅下列指南及参考资料以获取更多有关此主题的信息：

- ISO 18033-1:2015 – 加密算法
- ISO 18033-2:2015 – 非对称密码
- ISO 18033-3:2015 – 分组密码
- www.owasp.org/index.php/Guide_to_Cryptography
- csrc.nist.gov/publications/nistpubs/800-57/sp800-57_part1_rev3_general.pdf
- csrc.nist.gov/groups/ST/toolkit/key_management.html

6.2.1 风险

正确部署带有密码体系架构的解决方案可以确保所用的算法、协议和机密均符合当前建议。此外，建议是因时而变的。若没有密码体系架构，要想识别所有弃用的技术将愈加困难，从而形成安全漏洞。

6.3 定义通信模型

服务生态系统中的各系统必须能够相互验证。匿名公共用户应当无法接入该生态系统中的计算平台。各终端、合作伙伴、或用户将借助需相互验证的技术，与服务生态系统进行通信。由于构成用户界面的服务通常是在独立环境中进行部署和管理，因此可公开访问的界面必须限制在该区域范围内。然而，服务生态系统包括用于向所有已验证资源部署服务的整套系统。

这包括尚未由此系统配置的终端，这是因为硬件制造及个性化过程*应当*能够充分配置硬件，使其能够作为企业部署的资源而*验证*。

因此，通信模型*必须*提供：

- 相互验证
- 机密性
- 完整性

为有效实现该目标，通信模型还必须提供：

- 集中式信任根或分散式信任根
- 身份配置及撤销
- 完好的正向加密

信任根必须用于确保通信模型中的各个实体由对等的相同组织授权。这有助于确保所有实体由同一中央组织进行配置和授权。用于确保此信任根的技术可以是集中式（与 TLS 证书相似），也可以是分散式（与基于比特币区块链的物联网模型相似，如 IBM/Samsung 的 ADEPT 项目、Tilepay 等）。无论如何，核心业务必须成为该模型的*所有者*，并且保护配置系统。

配置及撤销必须成为通信模型的一部分，以帮助保证所有被入侵的机密或身份能够以最小努力从系统中清除。在线证书安全协议 (OCSP) 等技术可以帮助实现这一过程。

通信协议*必须*使用一种技术，能够降低从*过往*内容中攻击通信的可能。创建用于交换通信机密的瞬时非对称密钥可以实现这一点。若证书被攻击，瞬时机密将保持完好。这可以确保若证书专用机密被攻击或暴露，长时间存储的加密讯息也不会被攻击者解码。

通信安全的挑战在于技术的执行和寿命。加密算法可由权威机构在高度机密的条件下选取，以减少失败的可能性。

*必须*使用由工程部门设计或认可的函数库及算法。*切勿*使用惯用算法。这样不仅可以减少工程团队的工作量，而且降低了算法密码被设计拙劣或错误执行的系统削弱的可能。

请考虑使用以下组织提供的材料，以帮助实施此建议：

- CafeSoft Apache 相互验证实施指南：
  - http://www.cafesoft.com/products/cams/ps/docs32/admin/ConfiguringApache2ForSSLTLSMutualAuthentication.html

6.3.1 风险

通信安全是物联网的基石。若没有通信安全，就无法保证嵌入式设备与正确的后端服务进行通信。对向车载资讯系统、医疗设备及工业控制系统等设备进行指导、配置和发送指令的关键服务而言，这一点势在必行。若没有通信安全，就无法保证将指令发送至正确的终端。强制实施通信安全，以确保信息发送到预期的对等方，并由其接收。

6.4 使用网络验证服务

网络运营商作为合作伙伴时，允许用户使用网络运营商特定的令牌进行验证。尽管这些存在于网络运营商 UICC 中的令牌可使用户通过验证进入网络层，它们却无法使用户通过验证进入应用程序层。以下技术的使用可以使网络验证更加便利：

- 通用引导架构 (3GPP TS 33.220)
- M2M SM (ETSI TS 102 921)

出于验证目的，评估验证技术是否在应用程序层有实际意义。若该令牌能够用作安全存储，再判断物理终端能否使用该设备作为验证层以使用令牌建立 TCB。

尽管诸多网络运营商执行的是基于网络的验证，允许接入此 API 以验证用户或终端仍是一项最新的技术。评估您使用的网络运营商能否在该区域内提供有意义的体验。若能，可考虑不仅将该技术作为网络层验证令牌，因为使用一项安全存储技术要比使用多项技术更加简便。

6.4.1 风险

当网络验证服务与信任锚（如 UICC）整合后，若*不*利用这些服务保护应用程序层，就会限制应用程序验证用户的可靠性，并会增加底层终端平台的费用。这将增加部署成本，也会减少网络运营商向组织提供的信息。

6.5 在可能时提供服务器

服务器配置包括在生产环境中定义、配置、个性化及部署服务器。从服务角度而言，配置过程可以强化服务器的安全，且准备好在可能存在风险的环境中进行部署。

无论服务器部署在云基础设施、专业托管供应商处还是公司的单独机架空间内，服务器均易受到内部和外部的威胁。因此，在服务基础设施中部署服务器前，必须对其加强防护以免受攻击。

为实现这一目标，需确定周围环境可以访问的服务。定义服务器驻留的环境是否为公共或私有，以及其对服务器安全的影响。确定服务器内运行的各服务是否应向公众开放，或仅限已验证的客户接入服务。

评估服务器内运行的操作系统的生命周期。确定如何正确管理软件更新，以确保安全补丁能够迅速部署并投入生产中的服务器。评估回滚模型，以防更新失败或引发生产服务的意外状况，因为某些函数库或应用程序更新可能会导致意外的副作用。

最后，评估已配置服务器的废止模型，以确定从系统中移除资产的最安全方式。这包括评估异常服务或客户行为时所需的系统日志。

此建议意味着组织应执行补丁管理流程，以识别易受攻击的服务、部署补丁并监控执行这些补丁的成功与否。

请参考下列有关补丁管理的材料：

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

6.5.1 风险

服务器配置是物联网环境整体安全必不可少的一部分。若缺少此环节，组织对服务器架构的控制将大幅削弱。这可能会因缺乏架构技术规范而导致安全漏洞。若没有技术规范，组织将无法审查部署的技术是否符合现代最佳实践。此外，若要提高这些技术，需要调查各个部署的系统，以评估所部署资产间的差异。若需要部署的是关键安全更新，则这还远远不够并将引起高度关注。若没有一致性和架构来定义服务，则无法轻易追踪到哪些系统需要立即关注，除非手动依次检查。

6.6 定义更新模型

更新执行环境、应用程序形象或 TCB 是一个极具挑战性的过程。请参考下列可以简化整体流程的示例模型：

- 为执行平台的各层定义网络资源，如新应用程序形象的唯一 URL
- 为各特定层生成签名密钥
- 为各层所有新授权版本生成该层形象
- 各层形象中包括描述形象（版本、时间标记、身份等）的元数据
- 使用签名密钥签署层形象
- 通过唯一的网络资源或更新服务，提供形象、签名及公共密钥

新系统部署后，应当：

- 对于各层：
  - 检索要部署的版本
  - 使用密码验证形象
  - 在系统内部署形象层

任何应用程序层内未存储私有机密。机密必须在部署各个系统时进行动态配置，以个性化定制每个系统。当系统弃用后，这些身份应当被撤销，无论该系统的生命周期为多长。

本建议意味着应使用补丁管理流程以维护基础设施内的服务及技术。

请参考下列文档以获取更多信息：

- http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-40r3.pdf

6.6.1 风险

若没有明确定义的更新模型，服务和应用程序会因更新过程的滥用而存在被攻击的风险。攻击者可能会将惯用应用程序植入更新过程中，并将其自己的软件部署到云系统及其他服务器中。若通信安全基础设施未得到切实保护，通过操控域名服务 (DNS) 等网络服务就能轻易实现此类攻击。过去已发生多起针对路由的高级攻击，如边界网关协议 (BGP) 攻击，目的就是攻击未受防护的服务。

6.7 定义泄露数据的违规政策

仅确定数据密级的政策和程序远远不够，还必须具备一个模型，以检测数据是否被合作伙伴泄露。组织必须制定一个计划，以评估合作伙伴是否涉及违反保护用户数据和隐私的技术控制措施或政策的业务活动。

为实现这一目标，工程团队必须定义监控和日志技术，其要适用于*安全密级*，而不仅仅是用户数据。这样可让审计跟踪不仅适用于信息，还适用于该信息的*密级*。若用户信息被泄露，这将有助于组织进行自我保护。组织将能表明其安全密级以及技术控制措施实施到位，并根据政策管理、存储和传播数据。

当合作伙伴违反安全密级规定，这可帮助组织利用监控和日志技术进行证明。彼时，领导者应决定是否应对合作伙伴进行罚款、解约或施加其他处罚。

6.7.1 风险

若没有违规政策，则保护组织对第三方所泄露数据免除责任的法律防范会较少。若企业是所泄露数据的来源，第三方可能会丢失数据，但企业需对其提供给合作伙伴的数据负责。

违规政策可确保合作伙伴必须具备足够的安全等级，以保护提供给其的数据。若违反安全规定，只要物联网供应商遵守其自身的安全要求，就可以免于承担责任。然后，就要看合作伙伴是否遵守政策。

这些政策应当由法律及保险团队进行审核，以确保在遵守严格的安全政策及程序的前提下，该模型确实能够减少组织的责任。某些企业由于其所提供产品或服务的性质，根据法律法规或其他问题可能无法被免除责任。

6.8 通过服务生态系统强制验证

用户界面*绝对不能*直接验证用户。系统必须始终能够使用集中提供的服务来验证用户。移动设备上运行的应用程序由本地密码进行保护，这种情况是本规定的唯一例外。该密码可以用于访问本地应用程序。然而，对远程服务及资源的访问应当由单独的验证令牌进行验证。

但是出于可用性考虑，若用户充分了解使用相应验证方法的风险，工程团队可以选择将这两种验证方案合二为一。这样，已验证用户就可利用本地应用程序密码来解码包含远程服务所需验证令牌的本地数据库。这种多步骤验证模型对多数用户来说已足够。

无论如何，集中式验证服务必须首先使用户通过验证接入本地应用程序，然后再执行确定该验证令牌如何使用以及何时使用的相关政策和程序。另外还应收集相应指标，以判断用户是否已迁至其他计算平台，但仍在使用相同令牌。或者用户是否已在短时内迁至其他位置，但仍在使用相同令牌。根据移动的类型及速度，这些指标可能表明该令牌存在潜在受攻击危险。此时，该令牌应失效，且用户应被强制重新登录，适用时可以使用多因素验证。

6.8.1 风险

由于终端系统中可能存在滥用现象，因此无论架构如何安全，若没有后端系统的确认，用户验证始终不可靠。这样做的前提是假定用户未更新其凭证，或能跨多种设备类型拆分凭证。如果受攻击设备使用旧版用户凭证，这样做并不充分，并且可能会形成漏洞。

6.9 执行输入验证

所有从终端、用户或伪装用户处获得的数据必须进行分析以识别任何异常行为。对攻击者来说，最屡试不爽的攻击路线始终是在组成用户界面的服务中滥用 Web 应用程序输入信息。因为该技术必须根据各用户之间位置、编码及其他参数的变化，进行信息的动态转换。专业的用户可以操控编码的某些属性而引起意外的副作用，从而在处理子系统的不同层帮助攻击者。

譬如，一次有效的攻击会将空字节编码为更高级语言可作为字符串处理的消息。一些高级语言会将空字节视作二进制字符串的一部分，而非分隔符。当该二进制字符串被传递至低级函数库中时，嵌入的空字节会被译为字符串分隔符，这样字符串就会被截断，且其所表达的含义也与应用程序所解释的字符串含义截然不同。在过去，这是访问文件系统资源的聪明之选，否则特定用户将无法获取这些资源。

虽然恶意输入可发生无数变化，但工程师无需测试每一种可能的情况。相反，这个过程其实相当简单：

- 确定数据应在内部如何使用
- 根据内部使用模型，围绕应使用的编码和字符制定相应政策
- 设计一款 API，根据该政策分析数据
- 当数据被确认违反模型时，提出一个例外
- 使用有关会话的元数据在内部记录该事件，以帮助检测攻击者行为

系统内储存的所有数据都应首先处理并合成为一个静态模型。要有效达成这一目的，仅需将所有数据使用 base64 算法进行编码，然后放入数据库中。这可以确保数据绝对无法操控数据库。

6.9.1 风险

未采用输入验证的系统易受诸多可能的攻击，包括 OWASP 前 10 大攻击中提及的问题，如 SQL 注入攻击 (SQLi)，甚至远程代码执行攻击。潜在滥用的范围非常宽广，其风险无法被完全量化。输入验证是所有安全应用程序的重要属性，无论是云服务还是终端上运行的应用程序。

6.10 执行输出过滤

输出过滤是对输入验证的补充。该流程不仅可以保护表示层不受攻击者操纵，还可以禁止系统向应享有特权的用户提供信息。

对于前者，表示层提供的所有数据必须经过评估之后才能离开服务层。这可以确保编码后存入表示层的数据（如 JSON 信息或编码后的 JavaScript）不含有可能破坏数据表示或使其失效的格式。这意味着，储存在系统内的所有若转换就会损坏表示模型的字符，必须被过滤掉，或以一种不会意外更改表示的方式进行编码。

修复该问题的方法可以是将受限字符过滤掉，或对所有字符进行编码以确保字符的表示不会更改 GUI（字符不会被转译引擎译为控制代码），也可以是简单地不显示信息。这些方法均行之有效，但在特定应用程序中，某些方法更为适用。回顾信息论坛示例，若攻击者能够运行一种脚本，而其他人会在全然未觉的情况下复制并执行该脚本，则会出现同样坏的结果。因此，不能简单地用一种不会将 HTML 或其他脚本注入到表示层的方式转换信息，而是应对信息进行净化，以确保其他用户不受影响。

如果数据不应被传回给用户，这与攻击者所存储和转换的信息无关，而是因为数据显示不适合于公共用户，其应当被储存以供管理者和工程师使用。譬如，若在处理信息过程中产生了一个内部错误，则该错误不应带着全部调试数据被传回给用户。这可能会使想要攻击应用程序弱点的用户发现并利用错误所在。该信息应当在内部记录，通用错误可以提交给用户，这样用户就没有足够信息滥用程序错误。即使用户能够复制程序错误，也应该无法评估应用程序输出的差别，因此不能对攻击方法进行改进。

6.10.1 风险

输出验证是物联网安全的重要属性。如果系统不执行输出验证风险，会面临泄露关键用户数据、隐私相关数据、诊断数据、详细错误消息等风险。这些消息可能用于泄露用户信息或对已联网服务进行有效攻击。

6.11 执行高强度密码政策

如果用户验证需要密码，则所有验证系统都必须执行高强度密码。密码复杂度一直是信息安全研究者、工程师和业务领导者之间的持久战。业务领导者通常希望用户轻松记住密码。工程师需要降低界面复杂度，尤其是要为表示层的设计师降低难度。信息安全研究者经常高估攻击者的技能，为指定技术强加上不必要的复杂度。

但正确答案介于三者的要求之间。密码在长度上一定要长，但不应该复杂。虽然八个字符密码曾经是标准要求，在编写本文档时部分系统甚至允许六个字符，但密码长度应该由最新版最佳实践标准确定，可能远远超出八个字符。通过执行更长的密码，复杂度要求可以有所降低。用户不再需要设置一串奇怪的字符集，所以很容易记住密码。用户可以选择使用空格、大写、数字和标点符号，因此攻击者强行破解的难度自然会增加。

切勿忘记，攻击者获取密码通常有四种方式：

- 偷窃密码数据库和破解个人密码
- 暴力攻击应用程序验证服务
- 安装恶意软件
- 使用硬编码或默认密码

使用长密码有助于降低第一种风险。但是，确保服务生态系统层的安全会更加有益。第一种情况下攻击者应无法检索密码数据库，所以让我们看看第二种情况。

暴力攻击应用程序密码是攻击者能够滥用密码的最有效方式。恰当设计验证服务可显著降低这种可能性。如果猜错一次密码，系统应自动开始增加猜测之间需要的延迟。然后必须限定阈

值，限制尝试密码的总次数。若攻击者尝试次数达到阈值，账户应被锁定，用户应使用双因素验证或其他模型解锁并验证其账户。此安全类型能显著降低基于网络的攻击成功率，所以让我们看看最后一种情况。

客户系统中的恶意软件必须借助计算平台或已安装恰当应对技术的用户进行处理。应用程序本身通常不能对其加以保护。除强制执行 2FA 外，在对抗这种风险方面应用程序几乎无能为力。若攻击验证系统是攻击者*唯一可行的方法*，应用程序工程师将显著降低密码遭受威胁的风险。

但必须要注意，采取此建议所获得的*效果*并*不十分理想*。这是因为无论使用何种技术来降低密码验证遭受攻击的可能性，本质上而言，密码都是一种无形资源。它们并非是只能由单一个体获取的实体令牌，而是一种抽象对象，能够通过目视观察跨计算机系统中复制无限次数。因此，密码是一种极其薄弱的验证源，在任何情况下均无法充分表明特定用户的身份。密码本身安全系数低，因此任何使用密码的技术都易遭受其固有属性带来的风险。

密码在系统中不应被硬编码。终端应生成独特的密钥。请参阅终端文档，以了解更多有关终端配置的信息。对服务和用户界面而言，用户在注册时应设定密码。此时，密码必须符合强密码安全要求。切勿允许用户使用默认密码、弱密码或简单设定的密码。

确保用户始终能随时更改其密码。执行严格的验证要求和通信安全，以便用户更改其密码。尽可能实行双因素验证 (2FA)，以在准许更改密码之前核实用户身份。若用户向系统提交新密码，应始终强制其重新输入原始密码。这样做可确保其他用户不能利用未锁定的笔记本电脑侵入开放的 Web 应用程序，或偷窃 Web 应用程序会话令牌。

6.11.1 风险

未实施足够密码控制措施的系统会存在攻击者轻易猜中用户系统密码的风险。

6.12 定义应用程序层验证和授权

虽然组织信任根及其服务会定义保障网络通信层的验证技术，但用户、管理和合作伙伴授权技术必须单独配置。组织信任根能够保护这些实体的通信通道，但必须使用独立系统对其*行为*和*身份*进行验证。

通常，同一服务可促进该应用程序层验证，但要从独立资源中收集信息。例如，最好将用户和管理验证数据分开放置于单独数据库中。若攻击者能够通过应用程序层操纵数据库（如使用 SQL 注入技术），上述方法可确保其只能横向移动通过用户数据库。攻击者不可能在不攻击数据库的情况下垂直移动，将其权限提升为管理员。这将极大提升组织的安全。

若可能，请为以下身份定义独立的存储：

- 终端身份
- 用户
- 管理员凭证
- 合作伙伴

这将为应用程序和基础设施确立符合逻辑的职责分离，但要在受组织信任根服务管理的同一验证 API 中进行。

请考虑使用以下组织提供的材料，以帮助实施此建议：

- OAuth 2.0 [8]
- OpenID Foundation [9]
- GSMA Mobile Connect [10]

6.12.1 风险

如果没有强制执行应用程序层验证和授权的方法，系统将无法确认声称来自用户是行为实际是否获得该用户的授权。执行此建议可确保每个行为都可追溯到已认证的用户和授权。如果怀疑发生攻击，可指标存储供以后审核。若不采取这些措施，则无法保证将滥用风险减少到最小。

6.13 默认开启或故障时开启防火墙规则和系统加固

在某些服务基础设施环境中，默认情况下并未配置进出保护机制。这意味着工程师必须使用防火墙或网络流量规则集。向公众部署任何服务前，必须在基础设施中设置这些规则。

但有时，依靠这些技术来保护服务基础设施还不够充足。有时，防火墙和其他网络流量保护系统可能会发生故障。一旦这些系统发生故障，通常就会无法开启。这是因为，若系统发生故障，流量必须仍能正常运行，因为其他计算环境中的流量要与物联网供应商的流量一起通过基础设施。因此，流量不能突然终止。故系统通常会无法开启，以便使尽可能多的服务继续工作。

工程团队应使用操作系统强化功能，以确保基础设施故障造成的影响不会导致重大安全事故，而是仅仅意味现有服务基础设施可建立更多的连接。

例如，隐藏服务不应被置于防火墙等技术之后。相反，可使用虚拟专网 (VPN) 或其他高安全性保护措施，保护服务免受攻击。

请注意，软件防火墙具有额外的风险，因为其可能被狡猾的攻击者操纵。若使用软件防火墙，任何未正确强化的服务器基础设施都可能被攻击者操纵。换言之，若服务器上正在运行的公共服务具有某些不必要的特权（例如超级用户特权），在被攻破后，攻击者很可能会使软件防火墙禁用。因此，工程团队必须评估软件防护墙对已选架构而言是否风险过高。

6.13.1 风险

若未使用相关策略以应对网络流量安全系统的故障，该环境将遭受不必要的攻击，而若使用标准服务强化策略，则可轻松防止此类攻击。

6.14 评估通信隐私模型

与应用程序隐私（同上所述）或通信信息安全相比，通信隐私略有不同。虽然主要从第三方*有效读取*或*解释*数据能力方面评估隐私，但机密性和完整性并不代表通信隐私的全部。

影响通信隐私的其他问题包括：

- 每条信息的加密独特性
- 传输方式
- 明文元数据
- 硬件地址或相应的序列号

虽然应对每条信息加以保密并验证其完整性，但也必须对其设置独立密码。若作为攻击者可预测事件的回应而发送某些信息，则任何未设置独立密码的回应都可能被攻击者重放。每条信息都应独一无二，以禁止攻击者获取和重放有用的信息。

传输方式可使攻击者识别特定用户，或将行为与某个具有特定属性的行动相对应。例如，对于用户进入特定物理区域时将发出信息的技术，其可能会被能够在这些信息传输时将其接收的“嗅探器”所截获。尽管这可能不够直接，但若攻击者能够识别物理区域中的人员及其所在的位置，则就可能会引发问题。应评估网络模式，以确定是否存在一种简单的方法可让攻击者将传输方式转变成可操作的数据。

情报服务长期以来一直使用元数据，在未获得授权或合法访问加密数据的情况下评估信息系统的状况。通常情况下，组织利用元数据足以创建行动情报。然而，现在一些业余黑客、犯罪组织和好奇的用户能够利用元数据进行跟踪，或用于其他可能的不良企图。因此，减少向第三放开放的元数据量比以往更加重要。若可能，将元数据量限定在通信对等方足以评估信息是否为其所需的范围中。

顺沿这一想法，若可能的话，通信模块的硬件地址以及任何唯一序列号都应受保护或随机化处理。例如，苹果公司更改了 iOS 模型以探测 Wi-Fi 接入点。其并未使用静态的硬件地址，而是改变技术，使用随机性的硬件地址，这样可降低他人基于 Wi-Fi 主动扫描来追踪用户位置的可能性。物联网技术运行原理与之相似，但受该问题影响的通信技术更庞大。有些技术不能随机生成硬件地址，例如蜂窝技术。但其他技术，例如 802.15.4、Wi-Fi 及蓝牙技术，能够根据固件功能生成硬件地址。

6.14.1 风险

毋庸置疑，通信安全是必需的，但它*之所以*必需的原因有时会令人困惑。通信安全不仅能保证攻击者无法读取数据。它还能保证：

- 无法冒充终端
- 无法冒充关键服务
- 可以检测到滥用消息
- 软件或安全配置的变更可以安全进行

如果无法保证通信安全，就无法保证物联网产品或服务的质量、可靠性和隐私。

7 中优先级建议

中优先级建议集包括根据终端技术设计选择而定的一系列建议。例如，只有终端上运行操作系统时，提升操作系统级安全性才有效。如果终端包括单内核应用程序或配置一个嵌入式应用程序的嵌入式实时操作系统 (RTOS)，则此建议不适用。如果建议*确实*适用于终端设计，应予以实施。

7.1 定义应用程序执行环境

对于应用程序执行环境必须牢记以下几点：

- 使用的编程语言可能与安全有直接关系：
  - PHP 和 Ruby 等语言可能产生安全问题
  - GoLang 和 Erlang 等语言可能减少风险
- 必须对第三方库进行监控、管理和审计以识别风险：
  - 一些库没有很好维护
  - 一些库从未进行过安全漏洞方面的审计
  - 一些库需要过期的依赖项，但其中存在已知的安全漏洞
- 始终以无特权用户身份运行应用程序：
  - 如果应用程序要求特权资源，请使用包装器提供该资源，然后再放弃特权并执行完整的应用程序
- 使用定义明确的 TCB 和引导模型：
  - 具有定义明确的环境的应用程序会更*可靠*并且更加*安全*

请考虑使用以下组织提供的材料，以帮助实施此建议：

- OWASP [5]

7.1.1 风险

部署有安全架构的应用程序可能受到攻击，无法轻易追踪至具体来源。过去十年中，攻击服务和应用程序的工具与技术已得到很大提高。Metasploit 等开源技术可以开发自定义攻击并集成至攻击平台，后者提供相关技术以提高攻击的隐秘性。

通过确保应用程序运行方式、彼此交互以及运行所用技术的安全，安全的应用程序执行环境可以应对这种风险。这些属性不仅可以降低受到攻击的可能性，还可以提升跟踪能力和重要的日志功能，以跟踪并诊断被滥用的漏洞。

7.2 使用合作伙伴增强型监控服务

如果使用的合作伙伴是移动网络运营商，请确认其是否能够提供监控服务。一些网络运营商可以分析通过其网络传送的终端行为。具备这种能力的运营商在评估哪些指标意味着发生异常和攻击行为方面经验丰富。

这样，物联网企业可以更快地确认某个用户或终端是威胁，还是受到攻击者的攻击。这样，企业可以更有效地应对针对企业其他基础设施领域进行的预先攻击。

该服务的复杂之处在于网络运营商可以用有意义的时间轴提供情报。如果网络运营商只能在攻击者攻击物联网企业后提供情报，则物联网企业基础设施中的监控和日志系统应该可以检测到这些行为。但是，如果网络运营商能够在网络层通知企业有关的攻击行为，并且可以确认哪位订阅者在发出异常网络流量，则企业可以通过封锁该用户的流量，降低物联网生态系统的风险。

7.2.1 风险

物联网服务供应商依靠的某些技术可能无法被物联网服务供应商监控。其中之一就是将终端连接至服务和网络生态系统的通信网络。如果没有监控服务，物联网服务供应商将无法独自了解网络内发生的事件。因此，如果应用程序级别身份 A 试图攻击某一服务，组织将无法识别终端 B 才是连接至通信网络的设备。这种信息漏洞很严重，因为组织可能认为攻击来自身份 A，而非受损的终端 B。

7.3 使用专用 APN 进行蜂窝连接

接入点名称（APN）是一个蜂窝通讯组件，将无线网络连接至互联网。该接入点本质上是作为蜂窝终端设备与其必须交互的服务基础设施间的虚拟专用网络 (VPN)。专用 APN（有时称作安全 APN）是 APN 的一种，其安全性得到强化以实现多个所需的控制：

- 仅限于已验证客户的有限访问
- 防火墙
- 终端至终端通讯强制禁用
- 异常检测监测服务
- 可选安全或监测服务

通过限制对 APN 的访问，组织可确保只允许已验证的终端连接至服务基础设施，该连接通过 APN 实现。这减少了恶意或随机的无线客户端连接到 APN 和访问受限服务的可能性。此外，它可以让组织识别行为异常的特定客户端，以便让组织能够将此负面行为与特定硬件或用户相匹配。

防火墙确保客户端（终端生态系统）和服务端（服务生态系统）附着于 APN 的实体无法使用未经批准的信道进行通信，还使终端无法将 APN 滥用为通向开放式互联网的通道，同时封锁至已批准的特定服务组的流量。

终端通信限制可确保恶意终端无法利用 APN 作为广域网络攻击其他终端，所有通信都必须围绕组织批准的服务进行。若需要，组织可完全禁止终端至终端得通信。

监测服务将提升安全性，组织可通过监测现有云或服务基础设施做到这一点。通过 APN 匹配这些现有监测服务以及由网络运营商提供的网络监测技术，组织可以更容易地跟踪异常行为的来源。这使得组织可以更深入地检查终端或服务基础设施出现的问题。例如，如果应用程序层

显示用户 A 可能遭到攻击，而用户 B 的设备通过验证连接至 APN，组织便能应用 APN 监测服务确定用户 B 是否攻击用户 A，或攻击者是否同时攻击用户 A 和用户 B。

网络运营商具有可在上述服务之上进行分层的附加服务。这些服务有助于将网络中的不法分子列入黑名单、监测特定用户或用户组，并能改变显示异常的某些类型流量的路线。另外还可能提供其他选项。请与网络运营商共同确定适合您组织的服务。

虽然协调运用这些服务可能会具有挑战性，但与网络运营商合作可简化这一过程，将这些服务整合到企业现有的基础设施中也会变得更加简单。想要有效利用数据并不简单，需要有一个工程团队合理处理和管理数据。有些服务可能会产生额外成本。请确定最适合您组织的定价模型和服务。

7.3.1 风险

如果没有专用 APN，终端设备可以连接至几乎所有服务或技术，包括直接连接到 APN 上的其他终端或互联网上的任意服务。这会让一个遭入侵的终端可以与互联网上几乎任何服务进行交互，并将该终端变为攻击更安全网络或服务的代理，故本建议应强制执行，以限制终端进行任意未经授权的连接。强制要求终端只能连接至经批准的服务，对企业和整个物联网生态系统的安全性具有重要意义。

7.4 定义第三方数据发布政策

既然安全密级已定义，数据类型已归入有效的密级，并且违规政策也已制定，下一步应制定数据发布政策。数据发布政策描述如何通过技术控制措施来处理信息，并将信息传递至已授权访问数据的服务应用程序。权限模型是数据发布政策的一部分，并与用户创建细致数据权限的能力相匹配。

数据发布政策可能非常宏观，但需包含几个关键要素才能定义成功的政策：

- 需要哪个级别的相互验证才能传输数据
- 数据需要何种保密性和完整性
- 企业具有何种能力留存数据
- 合作伙伴具有何种能力留存数据
- 若允许留存，数据可以保留多长时间
- 数据必须适用于何种存储安全级别
- 数据必须适用于何种访问安全密级

7.4.1 风险

对于可能未遵守与物联网服务供应商相同内部安全级别的合作伙伴，数据发布政策会对其强制执行安全要求。由于物联网服务供应商无法控制合作伙伴在内部服务和网络中实施的安全措施，其只能强制发布给合作伙伴的数据以安全的方式传输。如果没有这个定义，合作伙伴可能会执行不安全的配置，从而会将用户数据暴露给攻击者，而该数据仍然在物联网服务供应商的控制下。通过对通信通道执行严格的安全控制，物联网服务供应商正尽一切努力在数据超出其控制之前确保安全。

7.5 创建第三方数据过滤器

接受来自合作伙伴的动态生成的数据（如广告等），需要对数据质量和安全具有一定程度的推测。工程团队必须采取措施，以确保从服务应用程序分发到合作伙伴的数据或来自合作伙伴的数据结构良好且不包含潜在的恶意内容，而不是向表现层做出假设和应用数据。

为此，工程团队应考虑以下模型：

- 数据是否符合合作伙伴为数据模型制定的格式
- 数据是否结构良好
- 数据是否表示可能被客户端误转译的多形态对象
- 数据是否会影响客户端呈现表现层的方式
- 数据是否会影响客户端*转译*表现层的方式
- 数据是否诱使或要求用户执行削弱安全性的行为
- 数据是否欺骗或冒充客户端 GUI 的组件（密码输入字段）

拒绝任何不符合已批准模型的数据。立即通知管理人员检测这些数据，包括尽可能多的有关数据来源和格式方面的指标。如若可能，在安全数据库中记录一个样本。

7.5.1 风险

来自第三方的动态生成的数据可能包含恶意软件、不适当的内容或其他不受欢迎的数据，无论是有意还是无意。如果没有针对第三方服务定义的入口过滤器，组织要承担无意中允许恶意软件或其他恶意内容到达最终用户的风险。由于这些数据的副作用，可能会导致系统被入侵，或是失去客户。

8 低优先级建议

低优先级建议是一系列适用于应对成本极高或不太可能影响终端设计的风险的建议。尽管这些建议很有价值，且建议内详述的信息非常重要，但所讨论的缓解或修补策略可能超出了特定企业的范围。请评估每条建议，确定所描述风险是否与企业及其客户相关或有重要关系。如果客户要求解决这些风险，请应用这些建议。

8.1 Rowhammer 漏洞与类似攻击

一些现代 RAM 技术（如动态随机存取存储器 (DRAM) 及静态随机存取存储器 (SRAM)）的实现，经证实易于因某些存储器存取序列而出现错误。滥用此类型错误会导致存储器可预测区域的某个或多个位改变。成功利用此漏洞可以改变存储器中代表软件所赋予的权限种类。

换而言之，如若正确利用，攻击者可通过操纵 DRAM 或 SRAM 现代实施中的硬件漏洞将权限从一个用户提升至另一用户。许多 DRAM 和 SRAM 的现代实施已证实可通过其漏洞被攻击。不过这要求能够在本地系统上执行代码，以创建触发该漏洞的存储器存取序列。

但通过运行时语言（如 sandboxed GoLang、Python、Erlang 等）可以远程触发这种行为。不过，这些类型攻击的准确性尚无记录，而且达成有效攻击的可能性非常小。

这种攻击必须在硬件级别加以解决。但工程师可通过禁止客户端在给定服务上通过虚拟机或运行时执行代码，从而降低滥用的风险。通过限制这种能力，工程师能阻止攻击者创建攻击所需的存储器存取序列。

8.1.1 风险

如果没有足够的措施来防御这种攻击，攻击者可能会对目标主机远程提升权限或执行任意代码。但应该注意的是，成功的攻击需要对硬件、操作系统、攻击向量和其他因素有极其深刻的了解，因而这种攻击实现的可能性非常小。

8.2 虚拟机受到攻击

现代服务基础设施经常利用虚拟机因需部署服务。虽然此模型经证实非常便利且易于部署，但该方法的问题是整个基础设施的安全性。即便工程团队可以成功部署一个深思熟虑的架构，但管理和部署虚拟基础设施的组织可能没有那么成功。

在虚拟服务器环境中进行部署的主要关注点是主机耐攻击的能力，或服务器（虚拟客户机）拦截同一基础设施上运行的其他客户数据的能力。

虽然这些攻击确实可能存在，并应该由物联网服务供应商进行评估，但其往往需要高深的技能和大量的时间才能进行。因此，攻击可能会发生，但比较罕见。然而，如果服务基础设施没有得到很好的保护，攻击者很可能会侵入虚拟机的管理访问。这种破坏可能无需高深技能就能成功。

解决该问题的方法之一是使用服务器配置。此过程将确保每个服务器都使用一组唯一的加密密钥进行编码。如果遵循此流程，所有攻击都会限制在单个服务器上。

8.2.1 风险

未能解决此种类型的攻击可能会导致服务基础设施易于遭受多种类型的攻击。也可能会使用从服务基础设施、数据泄露、隐私入侵获得的密钥进行服务器模拟和用户模拟。

8.3 创建使用者 API 以控制隐私属性

所有用户都必须能够通过服务 API 控制提供给第三方的信息。信息应分成不同的数据类型，并分配不同的安全密级。用户应该能够检索其帐户建模中使用的数据类型和密级。用户应能够对数据类型进行约束，以便能授权或撤销合作伙伴访问数据的权限。

这可能会以经过验证的 API 或 GUI 的形式，从而能对每位合作伙伴进行通常意义上的“是”或“否”的控制。

8.3.1 风险

如果用户不能对分发给物联网服务供应商的数据进行控制，其数据可能会因服务供应商或其所使用合作伙伴的安全漏洞而导致泄露。由于某些用户比其他用户承担的风险要高得多，因而每个用户应能够根据自己的个人需求调整其隐私限制。提供相应界面有助于确保此功能正确实施。用户必须自行调整控制措施以满足自身需求。例如，oneM2M（通过 TS-0003）允许用户针对服务供应商设置隐私偏好。

8.4 定义假阴性/阳性评估模型

虽然假阳性分析是一个非常复杂的话题，但有一个简单的方法可以判定某项技术是否更容易呈现假阳性结果。即通过评估以下方面：

- 数据来源是否*可靠*
- 数据来源是否能被篡改或造假
- 数据来源是否来自模拟域
- 数据是否能从多个来源点证实
- 证实的数据来源是否存在于相同的终端系统
- 证实的数据来源是否易于篡改或造假
- 是否有工具可以操纵数据来源
- 操纵数据来源需要何种程度的专业知识或成本
- 连接到数据来源的设备是否*可靠*

所有这些属性以及其他因素都可用于评估数据是否*可靠*。这非常重要，因为影响真实世界的关键决策可能会导致潜在的有害影响。工程团队必须创建一个可靠度模型，并将其应用到参与制定关键决策的每一个数据来源中。如果数据来源不可信，则应采取最合理、最安全的行动。

值得注意的是，工程团队并*不是*制定此类决策的唯一实体。业务领导层、律师团队和保险团队也应参与到潜在危险情况下应采取何种正确行动的决策中。然后，工程师必须以一种*可验证和重复的方式*，将正确的决策流程编入技术之中。

这一过程非常具有挑战性，因为其要求组织关注在危急情况下该技术应该如何作出反应。可靠度是应用于一项技术的具有挑战性的属性，尤其是对嵌入式技术来说更是如此。

8.4.1 风险

如果没有假阳性的评估模型，工程师们可能需要花费过多时间来分析良性事件，而真正重要的事件却正在发生之中。此时，组织所分析的指标将无法清晰告知生产中发生的事件类型，使得风险增大。这样会使得记录和监测基础设施的作用降低，使组织无法将这些昂贵的资源发挥效用。

9 总结

总而言之，通过明确定义的架构、在安全相关事件发生前或发生过程中识别风险的智能技术，以及处理此类事件的政策和程序，几乎所有物联网产品或服务中的安全风险都能成功应对。通过分析对物联网服务供应商而言至关重要的高级别安全概念，可审查常见的安全问题。该过程可指导工程团队执行解决其安全架构漏洞最相关的建议。

随着团队不断完善其架构定义，在实施中会碰到越来越独有的安全问题和疑虑，此时可查看各个独立的建议。

整体而言，每个工程团队都会面临极其相似的风险。组织必须选择与同行分享其遇到的问题，以便建立风险和补救策略的公共知识库。大家一起努力，共同构建相关技术和知识，以帮助彼此保护未来物联网的安全。

附录 A 文档管理

A.1 文档历史

版本	日期	变化的简要描述	授权批准	编辑/公司
1.0	2016 年 2 月 8 日	新 PRD CLP.12	PSMC	Ian Smith GSMA 和 Don A. Bailey Lab Mouse Security
1.1	2016 年 11 月 07 日	新增 GSMA 物联网安全评估计划参考资料。 小幅编辑更正。	PSMC	Ian Smith GSMA
2.0	2017 年 9 月 29 日	新增更多 oneM2M 参考资料	物联网安全团队	Rob Childs GSMA

A.2 其他信息

类型	描述
文件所有者	GSMA 物联网项目
联系人	Rob Childs – GSMA

为您提供卓越的产品是我们不懈的追求。如果您发现任何错误或遗漏，请告诉我们。您可发送邮件至 prd@gsma.com

欢迎您随时向我们提出建议和问题。