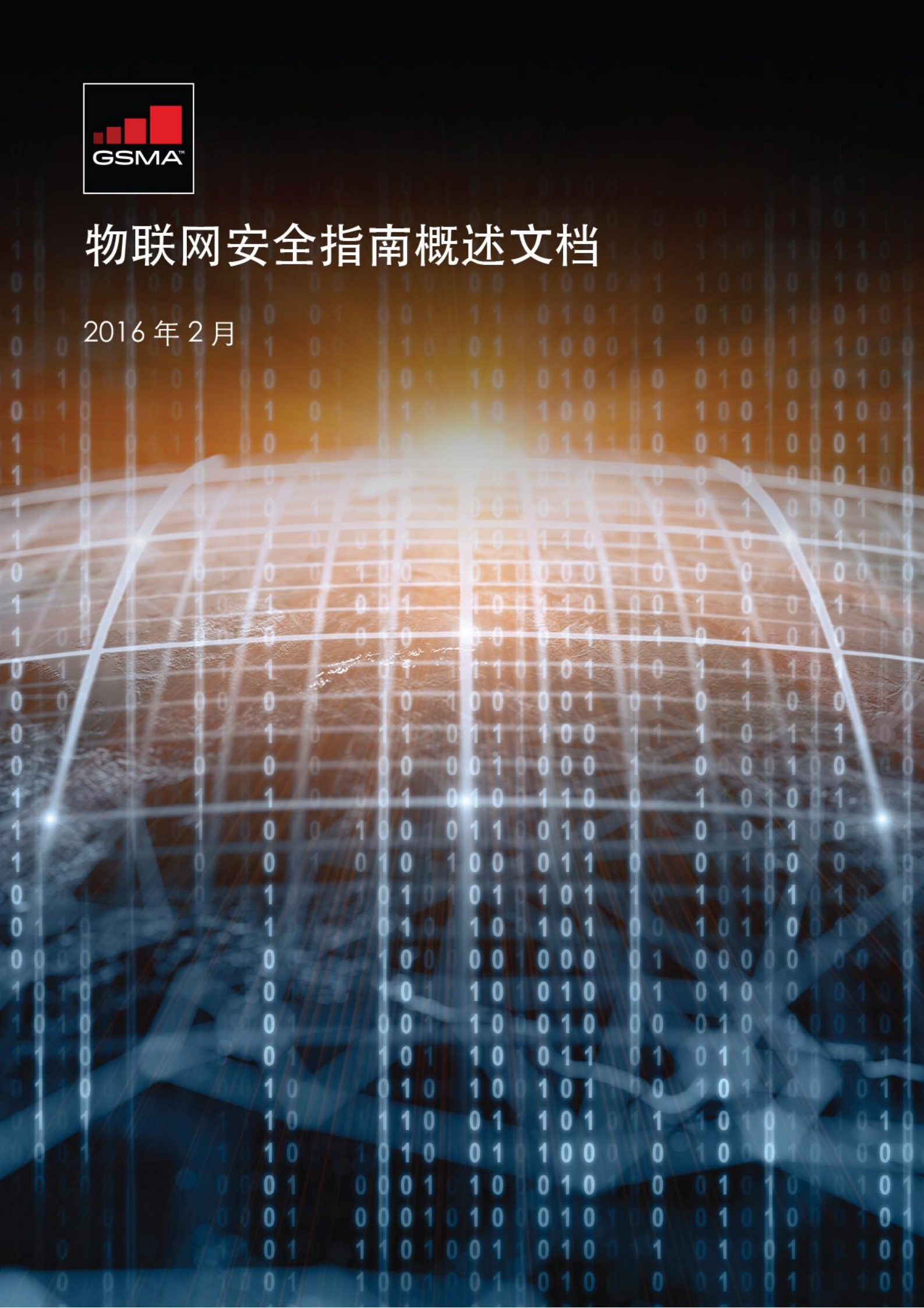

物联网安全指南概述文档

2016 年 2 月

物联网安全指南概述文档

版本 1.0

2016 年 02 月 08 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。

目录

1 简介

1.1 执行概述

物联网 (IoT) 的出现使得一批新型服务供应商应运而生，致力于开发创新互联的全新产品和服务。有分析师预测，未来十年，成千上万的全新物联网服务将连接数十亿的全新物联网设备。物联网的迅猛发展将为新生态系统的所有成员创造重要机遇，有利于拓展服务，增加客户群。

分析师表示，安全问题是阻碍很多新型物联网服务部署的绊脚石，同时，针对不断壮大的物联网服务提供的广域连接，也让整个生态系统中的诈骗和攻击行为随之增加。众多迹象已经表明，攻击者对该领域的兴趣已初露端倪。

新型服务供应商在为某些市场领域开发全新的创新服务时，或许对其服务可能产生的威胁全然不知。有时候服务供应商开发出的服务可能无法连接至之前的通信网络或互联网，可能也没有掌握相关技能或专业知识，用以降低启用设备网络连接造成的风险。相比之下，其对手更了解技术和安全的薄弱环节，一旦暴露出弱点，他们就会趁机下手。

汽车、医疗保健、消费电子产品和市政服务等领域的服务供应商，可能认为其特定的安全需求在市场中是独一无二的，但实际情况通常并非如此。几乎所有物联网服务在构建时，使用的终端设备和服务平台组件中包含的技术与其他很多通信、计算和 IT 解决方案使用的技术都很相似。而且不同服务所面临的威胁以及缓解这些威胁可能采取的解决方案通常十分相似，即使攻击者的动机和安全漏洞的影响大相径庭。

GSMA 代表的电信行业向客户提供安全产品和服务由来已久。为帮助确保进入市场的新型物联网服务之安全性，网络运营商及其网络、服务和设备装置合作伙伴希望与志在发展物联网服务的服务供应商分享安全知识。

因此，GSMA 推出这套安全指南，为志在发展新型物联网服务的服务供应商提供帮助。

1.2 GSMA 物联网安全指南文档集

本文档是 GSMA 安全指南文档集的第一部分，该文档集旨在帮助发展初期的物联网行业获得对物联网安全问题的一般了解。指南文档集倡导发展安全物联网服务的方法，意在确保整个服务周期实施最佳安全实践。文档就如何应对物联网服务的常见安全威胁及薄弱环节提供了建议。

GSMA 安全指南文档集结构如下所示。建议先阅读本文档（即概述文档），然后再阅读支持文档。

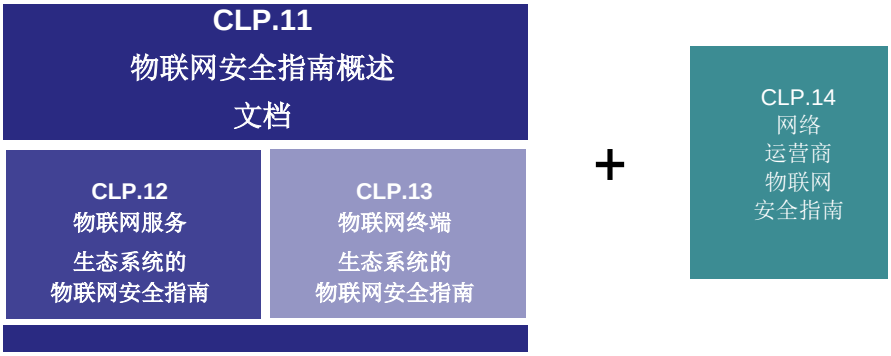

图 **1 - GSMA 物联网安全指南文档结构**

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“网络运营商物联网安全指南”[13]，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。

1.3 文档目的

物联网安全指南文档集旨在为物联网技术或服务执行者在构建安全产品时提供一系列设计指南。为实现此目的，本文档将作为一套整体模型，用来解释技术或服务的哪些方面与执行者相关。

确定这些方面或组件后，执行者就可以评估与每个组件相关的风险，并确定如何弥补风险。每个组件又可以细分为*子组件*，其中会说明更细微的风险。每项风险应分配优先事项，帮助执行者确定攻击费用、补救费用以及不处理风险可能造成的任何费用（如有）。

本文档的范围限于与物联网服务设计和执行相关的建议。

本文档并非意在推动建立新物联网规格或标准，但会涉及现行解决方案、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。

请注意，必要时，某些国家/地区的国家法律法规可能否决本文档中提及的指南。

1.4 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。
- 物联网设备制造商 - 为物联网服务供应商提供物联网设备，以实现物联网服务。
- 物联网开发人员 - 代表物联网服务供应商构建物联网服务。
- 自身是物联网服务供应商或代表物联网服务供应商构建物联网服务的网络运营商。

1.5 定义

术语	描述
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，通常企图获取、破坏、限制或篡改信息。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。
复杂终端	终端模型可以通过长距离通信链路，如蜂窝、卫星或以太网等电路连接，持久连接后端服务器。更多详情请参考 CLP.13 [4]。
组件	指文档 CLP.12 [3] 和 CLP.13 [4] 中包含的组件。
嵌入式 SIM	无法从设备中移除或更换的 SIM，确保根据 GSMA SGP.01 [2] 安全更换文件。
终端	轻型终端、复杂终端、网关或其他互联设备的通用术语。更多详情请参考 CLP.13 [4]。
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。更多详情请参考 4.2 章节。
物联网	物联网 (IoT) 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通信功能的汽车、监视器和传感器。
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。
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商和所有者。
组织信任根	一系列密码政策与流程，掌控着如何为身份、应用程序和通信安全加密。
建议	指文档 CLP.12 [3] 和 CLP.13 [4] 中包含的建议。
风险	指文档 CLP.12 [3] 和 CLP.13 [4] 中包含的风险。
安全任务	指文档 CLP.12 [3] 和 CLP.13 [4] 中包含的安全任务。
服务接入点	通过通信网络进入物联网服务后端基础设施的点。
物联网服务生态系统	服务、平台、协议及其他技术，可提供相关功能并从该领域部署的终端中收集数据。更多详情请参考 3.1 章节。
用户识别模块 (SIM)	移动网络智能卡，用于在连接移动网络，接入网络服务时识别设备。
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识别应用程序。可体现为 ETSI TS 102 671 标准中指定的嵌入式形状因素。

1.6 缩略语

术语	描述
3GPP	第 3 代合作伙伴项目
API	应用程序接口
APN	接入点名称
CERT	计算机应急响应小组
CLP	GSMA 互联生活项目
CPU	中央处理器
EAP	可拓展认证协议
EEPROM	电子可擦除可编程只读存储器
GBA	通用引导架构
GPS	全球定位系统
GSMA	GSM 协会
GUI	图形用户界面
HIPAA	健康保险携带和责任法案
IoT	物联网
LPWA	低功率大范围
NIST	国家标准和技术研究所
OBD	车载诊断系统
OCTAVE	可操作的关键威胁、资产和薄弱点评估
OMA	开放移动联盟
PIA	隐私影响评估
PII	个人验证信息
RAM	随机存取存储器
SIM	客户识别模块

1.7 参考文献

参考文献	文件编号	标题
[1]	无	**“The Mobile Economy 2015”** http://www.gsmamobileeconomy.com/
[2]	**SGP.01**	**“Embedded SIM Remote Provisioning Architecture”** http://www.gsma.com/connectedliving/embedded-sim/
[3]	**CLP.12**	**IoT Security Guidelines for IoT Service Ecosystem** www.gsma.com/connectedliving
[4]	**CLP.13**	**IoT Security Guidelines for IoT Endpoint Ecosystem** www.gsma.com/connectedliving
[5]	无	**NIST Risk Management Framework** http://csrc.nist.gov/groups/SMA/fisma/framework.html
[6]	**CMU/SEI-2007-TR-012**	**Introducing OCTAVE Allegro:Improving the Information Security Risk Assessment Process** http://www.cert.org/resilience/products-services/octave/
[7]	未使用	未使用
[8]	**TS 33.220**	**Generic Authentication Architecture (GAA); Generic Bootstrapping Architecture (GBA)** www.3gpp.org
[9]	**RFC 4186**	**Extensible Authentication Protocol Method for Global System for Mobile Communications (GSM) Subscriber Identity Modules (EAP-SIM)** www.ietf.org
[10]	无	**Conducting privacy impact assessments code of practice** https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf
[11]	无	**Open Mobile Alliance** http://openmobilealliance.org/
[12]	无	**oneM2M** http://www.onem2m.org/
[13]	**CLP.14**	**IoT Security Guidelines for Network Operators** www.gsma.com/connectedliving
[14]	**GE.11-13201**	**Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue*** http://www.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf
[15]	无	**Right to Internet Access** https://en.wikipedia.org/wiki/Right to Internet access

2 物联网产生的挑战

几年前，联合国的一份特别报告建议将互联网列为人类的基本权利，世界上所有人都有权享受宽带服务 [14]。法国、希腊、西班牙及其他国家 [15] 最近正通过法律，旨在确保互联网接入在大范围内的可用性，和/或防止各州不合理地限制个人对信息和互联网的访问。

这些声明是互联网发展促使社会和技术迅猛变革的成果。这使得互联网演变为一种生活方式，成为各类信息的主要来源以及与亲友保持联系的最常见方式。互联网不仅是一种技术，更成为我们的*一部分*。

我们对于保持互联的需求日益强烈，为应对这种需求，过去几年对技术进行了颠覆式的革新。十年来，技术人员一直高呼“物联网时代来了！”尽管如此，我们五年前才将在普及信息获取，建立所需成本模型方面的兴趣变为实际的业务模型。此后，组件成本大幅下降，无线服务的获取和服务速度方面有了显著提高。协议、电池寿命乃至业务模型不断发展，以满足我们对信息与互联日益强烈的需求。

从根本上而言，这就是对物联网最好的诠释。物联网并不是生硬的物体，而恰恰关乎你我。它是由我们构建的网络。在新的生活方式下，人类和数字体验不再孤立存在，二者的关系变得亲密。

人类真实体验与数字世界的纽带空前紧密，因此必须受到保护，因为当前的数字安全将直接影响真实世界。物联网是推动世界向前发展的绝佳机遇，有利于创建知识、共享体验和创新的庞大数据库。但是，为了让物联网有效地发挥作用，我们必须确保推动互联的技术之安全性，保证必要服务的隐私、可靠和质量，以确保所有需要访问互联网的人都可以享用这项伟大的公共事业，满足自身必要的基本需求。

为了使物联网有效地发展，我们必须解决其发展过程中固有的安全挑战。挑战包括：

- 可用性：确保始终连接终端及其各自的服务
- 认证：对终端、服务和运行终端的客户或终端用户身份进行验证
- 隐私：降低伤害个体终端用户的可能性
- 安全：确保可核实、追踪并监控系统完整性

2.1 可用性挑战

为确保物联网以预期速度发展，终端设备必须能够始终与其他终端设备、终端用户和后端服务沟通交流。若想实现这一点，需要设计出可保证始终连接的新技术。这与在现代世界普及互联网接入的挑战相契合。要想实现这一挑战，必须回答几个问题：

- 低功耗广域网 (LPWAN) 如何在应用时达到与现代蜂窝系统类似的安全级别？
- 多个移动运营商如何支持与新型物联网终端在网络边界迁移相同的安全级别？
- 网络信任如何*推进到*依靠网关终端进行通信的毛细终端？
- 如何在安全通信环境中应对轻型终端的功耗限制？

2.2 身份挑战

终端要想在物联网产品或服务生态系统中发挥作用，就必须能够向同行和服务商安全地表明自身身份。这是物联网技术中一个重要而基础的方面，可以确保服务和同行能够保证数据交付的对象。获取信息及服务并不是与身份直接相关的唯一问题。我们还要问以下问题：

- 运行终端的用户是否与终端身份紧密相连？
- 服务和同行如何通过识别终端身份确认终端用户身份？
- 终端安全技术是否能够安全地验证同行和服务？
- 异常服务和同行能否冒充授权服务和同行？
- 如何确保设备身份不受干涉或操纵？

2.3 隐私挑战

隐私不再是现有产品与服务的附属品。真实世界直接受到数字世界活动的影响，所以必须从头至尾地为产品设置隐私，从而确保每项活动获得授权，每个身份得到证实，同时确保不将这些活动及相关元数据泄露给未授权方。只有恰当定义产品或服务架构，才能应对隐私挑战。要想逆动执行，更是异常艰难，需要付出代价。

医疗设备、汽车解决方案、工业控制系统、智慧家庭、建筑和安全系统等，都将直接影响人类的真实生活。工程人员有责任以尽量高的保证级别支持产品和服务，降低实际伤害和泄露隐私相关数据的可能性。

因此，我们必须要问的不仅是隐私如何影响终端用户，还有如何设计物联网技术：

- 终端身份是否泄露至未授权用户？
- 唯一终端或物联网服务标识符是否允许终端用户或终端受到实际监控或追踪？
- 终端或物联网服务中发出的数据是否表示或直接与真实终端用户属性相关？如位置、活动、或状态，如*正在睡觉*或*醒着*。
- 对机密和完整性是否设有充分的保护，以确保组合密码文本的模式不会被看到？
- 产品或服务如何存储或处理用户特定的个人可标识信息 (PII)？
- 终端用户能否控制 PII 在物联网服务或产品中的存储或使用？

2.4 安全挑战

虽然互联网安全在过去几十年有了显著提高，但现代技术的整体健康依然存在巨大差距。在物联网技术的两大主要组件：嵌入式系统和云服务中，差距最为明显。

物联网若想不断发展，但又不使大量用户和真实系统置于威胁中，就必须对终端和物联网服务进行信息安全实践。

- 是否在项目之初就对产品或服务进行了安全最佳实践？
- 安全生命周期是否结合至软件或产品开发生命周期？
- 应用程序安全是否应用于在嵌入式系统中运行的服务和应用程序？
- 是否在终端和服务生态系统中执行了可信计算基 (TCB)？
- TCB 如何对应用程序图片和服务进行自我验证？
- 终端或物联网服务能否检测出其配置或应用程序中存在异常？
- 如何监控终端中指示恶意行为的异常现象？
- 认证和身份如何与产品或服务安全流程相关联？
- 制定了哪些事件响应计划以应对检测到的指示损害的异常现象？
- 如何对服务和资源进行分段，以确保快速而有效地遏制损害行为？
- 损害行为后如何恢复服务和资源？

3 移动解决方案

虽然大量技术可以为物联网提供互联解决方案，但在塑造物联网未来方面，没有哪项技术优于移动网络。二十多年前，移动网络让消费者和行业第一次享受到无线服务，此后一直致力于构建可靠可用、安全经济的服务。由于长距离传输无线电网络的不稳定性，移动行业在网络可用性方面已经积累了丰富的经验。网络身份也是一项挑战，产生了多项标准、设备技术、协议和分析模型。一直以来，隐私和安全都是移动行业关注的问题，行业一直致力于降低所有移动技术中滥用、身份盗用和诈骗的可能性。

3.1 应对可用性挑战

GSMA“2015 年移动经济”报告指出 [1]：

- 移动行业一直以迅猛之势扩大规模，截至 2014 年底，独立手机用户已达 36 亿。10 年前，手机订阅用户仅占世界人口的五分之一，现在已飙升至世界人口的一半，预计到 2020 年，还会新增 10 亿用户，届时全球普及率将达 60%。截至 2014 年底，共计 71 亿次全球 SIM 连接和 2.43 亿次机对机连接。
- 在全球，移动宽带网络技术正迅速获得人们的青睐。截至 2014 年底，移动宽带连接（即 3G 和 4G 技术）在所有连接中所占比例不到 40%，但是到 2020 年，该比例将达 70%。
- 2G 现在依然是全球的主要网络技术，但其地位已大不如从前。2008 年，2G 连接占所有连接的 90%，但是截至 2014 年底，已跌至大约 60%。按照绝对值计算，2G 连接在 2013 年达到最高值，2014 年下降 6%。
- 在技术上不断朝高速网络发展也得益于运营商的大量投资。GSMA 近期研究预测，到 2020 年，使用 3G 网络的人将从现在的 70% 增加至超过 80%。报告还强调，4G 网络正以高速推进，远超 3G 网络当时的推进速度。3G 网络历时 10 年才覆盖全球一半的人口，而 4G 网络自发布起 8 年就可以达到这一高度，即 2017 年完成。

将来我们还有望看到低功耗广域 (LPWA) 无线技术集成至蜂窝通信空间，满足物联网需求。这种通信技术以有效沟通所需的功耗，为当前的移动网络提供广域无线连接。移动运营商会将 LPWA 协议和技术集成至其产品中，在将来为企业提供服务和解决方案。

3.2 应对身份挑战

几十年来，身份管理方面一直面临挑战，并大幅度强化了移动行业标准和技术供应。移动行业通常采用可拆卸 SIM 卡，但 GSMA 创建了一项基于 SIM 卡的解决方案，名为“嵌入式 SIM 远程配置架构”[2]，适用于在物联网中使用，可将更高级别的组件集成至终端设备，降低生产成本，并通过空中下载 (OTA) 平台管理连接，从而实现物联网终端设备在整个生命周期中的互联。

嵌入式 SIM 等身份识别技术可设计为默认整合安全的信任密钥。其制造目的在于抵御如下攻击：

- 故障
- 旁道攻击
- 被动数据拦截
- 实体干扰
- 身份盗用

该项安全加固技术的一大进步是新一代信任密钥新增了物联网格局。这些技术将发挥双重作用。不仅可以验证网络安全，也能够确保应用程序通信及程序自身安全，与传统的计算信任密钥类似。

结合移动行业安全规范，如 3GPP GBA [8]、OMA [11]、oneM2M [12] 及其他技术提供的规范后，双重作用将进一步增强。这些技术有助于安全地在该领域提供设备和促进无线固件更新，并管理设备性能和认证。

如果将这些技术整合并用，将简化当前复杂的工程流程，并合并到一个简单的组件中。不再需要应用程序工程师构建复杂技术并亲自进行管理，管理网络身份的网络运营商完全可以代表应用程序自己操作。这样不仅可以降低工程复杂度，也会缩减企业的日常管理需求。

3.3 应对隐私及安全挑战

除了 SIM 功能，移动行业还开发出弹性协议、流程和监控系统以确保安全，降低诈骗及其他恶意活动的可能性。例如，3G 和 4G 技术采用相互认证的方式，验证终端及网络身份。该流程可确保对手无法拦截通信。

还可以通过使用 SIM 及 GBA [8] 或 EAP-SIM [9] 等技术，确保网络安全。通过使用这些技术，SIM 可配置会话安全密匙，用于与应用程序网络同行沟通知名协议。该流程可降低对手操纵应用程序协议以损害设备或服务的可能性。因此，可使用该模型确保网络及应用程序安全。

4 物联网模型

下图显示的是，文档中使用的标准物联网模型被描述为服务及终端生态系统的组件。每个组件都包括子组件，将在单独介绍主要组件的文档中详细说明这些子组件。例如，终端组件及各自的风险在该文档集的终端生态系统文档 [3] 中进行了概述，服务组件在服务生态系统文档 [4] 中进行了概述。

图 2 **- 物联网模型示例**

该表可以介绍在几乎所有物联网服务或产品模型中使用生产就绪技术所需的主要组件。

通信网络组件为物联网所固有，为发挥该模型的目的，其连接了两个生态系统，通信链路的各“端”在相应的终端生态系统及服务生态系统文档中有讨论。

关于网络运营商的网络安全指南具体建议，请参阅 GSMA“网络运营商的物联网安全指南”[13]。

4.1 服务生态系统

服务生态系统代表为提供功能并从该领域使用的终端中收集数据所需的服务、平台、协议及其他技术。该生态系统通常从终端收集数据，并将其存储至服务器环境中。将数据的生动描述在多个用户界面呈现，用户就可以了解该数据。数据经常采用指标、参数或命令的形式，也可以通过服务基础设施中生成的 API 交给授权第三方，物联网服务供应商通常借助这种方式实现服务货币化。

关于使用服务生态系统安全指南，以及该概述文档中描述的流程，请参阅 CLP.12 物联网服务生态系统的物联网安全指南 [4]

4.2 终端生态系统

终端生态系统 [4] 包括低复杂性设备、富设备和网关，它们通过多种有线和无线网络将真实世界连接数字世界。常规终端示例包括运动传感器、数字门锁、汽车远距离通信系统、传感器驱动工业控制系统等。终端从其周围的真实环境中收集指标，并以多种形式通过毛细或蜂窝网络将数据传输至服务生态系统，通常会接收到回应的指示或行动。可能也包括描述从终端本身或服务生态系统中获取的数据的富用户界面。

关于使用终端生态系统安全指南，以及该概述文档中描述的流程，请参阅 CLP.13 物联网终端生态系统的物联网安全指南 [13]

5 风险评估

虽然风险评估这一概念已经出现数十年了，但是很多企业更熟悉将概念应用于综合业务风险，而非信息安全。但是，企业要想实现安全运营，技术方面获得长期发展，信息安全风险评估流程也很有必要。在物联网技术中，工程团队在企业的成功中扮演重要角色，很显然，风险评估流程应成为组织构建安全实践而采取的首要步骤。

每家组织都应该对技术风险形成细致入微的观点，以下高层级问题应作为风险评估流程的起点

- 需要保护哪些资产（数字或实体）？
- 哪些人群（有形或无形）是潜在威胁因素？
- 什么会对组织构成威胁？
- 什么是薄弱点？
- 如果受保护的资产遭到损坏，将产生什么后果？
- 资产遭到损坏的可能性多大？
- 如果面临多*组*攻击者，将有什么后果？
- 资产对于组织及其合作伙伴有何价值？
- 资产遭到损坏对安全有什么影响？
- 怎样修复或降低隐患可能性？
- 如何监控安全方面的新漏洞或正在形成的漏洞？
- 哪些风险无法解决，其对于组织有何意义？
- 多少预算应该用于事件响应、监控和风险修复？

这些起点有助于工程与信息技术团队在组织中更高效地开展工作。目的是确保企业的技术方面在风险、价值观和修复计划方面与执行方面达成一致。让团队并肩作战，有利于对企业风险以及资产价值形成更真实的认识。这将直接影响应该用于解决突出安全漏洞的预算。

一些风险确实无法解决，我们会在指南中讨论此类风险。组织应该对这些风险进行评估，确认是否可以接受。这有助于企业更真实地了解其局限、技术限制以及应对某些威胁的能力。越是想以经济有效的方式解决所有安全漏洞，反而越耗费财力。

5.1 目标

风险评估的目的是创建（或更新）一系列政策、程序和控制方式，以修复、监控并应对组织技术环节中发现的安全漏洞。风险评估结果不仅应帮助企业调整技术，还应调整技术管理、设计及使用方式。只要风险评估结果充分说明组织使用的信息及资源价值，就可以通过优化人员、流程和政策确保整个组织的安全。

请记住，使用风险评估结果的核心优势包括：

- 通知人员
- 优化流程
- 制定（或更新）政策
- 进行修复
- 监控新漏洞
- 优化产品或服务

从本质上而言，这可以帮助组织部署基础平台，确保人员和流程安全。该平台应整合至周期中，不断评估并改善组织的整体角色和责任。

5.2 风险模型参考文献

先不要尝试制定风险评估和威胁模型流程，而是查看以下参考文献，获得对风险评估流程的充分描述和逐步解释：

- 国家标准和技术研究所 (NIST) 的风险管理框架 [5]
- 计算机应急响应小组 (CERT) 的 OCTAVE 模型 [6]

6 隐私注意事项

很多物联网服务和产品将用于创建、收集或分享数据。部分数据不属于“个人数据”，或者不会影响消费者隐私，因此不受制于数据保护和隐私法。此类数据可能包括机器真实状态、内部诊断数据或网络状态相关指标等信息。

但是，很多物联网服务会涉及个体消费者相关的数据，因此将受制于通用数据保护和隐私法。如果网络运营商提供物联网服务，也将受制于通信特定的隐私和安全法规。以“消费者”为本的物联网服务可能涉及详细数据的生成、发布和使用，或将影响个人隐私。例如，推断消费者健康状况或根据其购物习惯和位置生成人物形象。消费者物联网服务获得普及后，将实时生成并分析更多消费者数据，并与跨国多方分享。

如果数据与具体个人相关，复杂“互联”的生态系统可能收到消费者以下方面的问题：

- 谁在收集、分享并使用个人数据？
- 具体获取哪些数据？
- 从何处获取数据（什么技术或界面）？
- 何时收集数据？
- 为什么收集用户数据？
- 如何确保个人信息的隐私（不只是安全）？
- 个人是否可以控制如何分享其数据，公司如何使用其数据？

依靠消费者数据的所有物联网服务供应商、以及获取或使用数据的任何合作伙伴公司，都有责任尊重个人隐私，保证个人可标识或隐私侵入性信息的安全性。

物联网服务供应商面临的重要挑战是，应对隐私和数据保护的法律五花八门，有时候还会前后矛盾。不同国家会采用不同的法律，这取决于涉及数据的类型以及服务供应商提供的行业领域和服务。这涉及很多以消费者为导向的物联网服务供应商；

例如，互联汽车可以在多个国家之间穿梭，也就是说，相关数据传送可能受到不同法定辖区的管理。车载传感器可追踪车辆位置（静态或动态）及常用目的地，可用于推断司机的生活方式、爱好或宗教信仰等信息，但司机认为这都是自己的个人信息。此外，通过“车载诊断系统”传感器获取的驾驶习惯信息可能与保险公司分享，后者可能使用这些信息收取更高的保险费，在司机不知情的情况下对其区别对待。

物联网服务和设备（包括互联汽车）也可能在不同的主权领土，也就是不同的法定辖区之间移动。很多时候，个体的个人数据传输或存在的位置可能不在个体所属辖区。在使用跨国物联网服务前，以上都是需要考虑的重要问题。

另一项挑战是大多数数据保护法要求收集消费者数据的公司在处理某类“个人数据”，如健康相关数据前，需征得消费者（也称“数据当事人”）的同意。大多数法律将“个人数据”定义为与“已表明身份”或者“可识别身份”的活着的自然人相关的任何信息。

随着越来越多的设备连接至互联网，越来越多的个人数据将被收集、分析甚至可能影响个人隐私，但并不一定被法律定义为“个人”数据。海量数据、云存储和预测分析相结合，可获取详细的用户资料。更严重的是，很难真正实现信息匿名化，个人信息也可以从其他数据类别中推断得出。

人们日益意识到对于维护敏感、健康数据记录的隐私需求，尤其是因为此类记录可能被商业滥用。美国 1996 年健康保险携带和责任法案 (HIPAA) 中包括隐私和安全要求，旨在缓解对健康记录的未授权披露风险。

和很多其他法规，如欧盟法规一样，HIPAA 只适用于健康数据具有*个人可标识性*的情况。血液监控设备（不会识别用户身份）中存储的数据不需要遵守这些要求，但是智能手机 app 或云服务器中存储的此类数据理应遵守，因为这些信息能够连接至个人（因为如果在智能手机上，收集几乎一定会包含可识别用户身份的其他数据，如果在云服务器中，数据属于可识别身份的用户账户）。世界各地的决策者正逐渐意识到，与人们相关的信息和数据分析可能影响人们的隐私，即使这些信息并非“身份识别”信息。因此，这些决策者开始着手采纳更注重风险的法律手段，并考虑赋予数据使用更加宽泛的隐私含义，而不仅仅局限于法律定义。

为了在物联网生态系统构建信任，政府应确保数据保护和隐私立法与技术无关，而且规定始终适用于互联网生态系统的所有参与者。此外，为帮助物联网服务供应商将正式监管干预需求降至最低，我们建议其在物联网服务或产品开发初期遵守附录 A 中描述的步骤。

7 有效使用该指南

如果在工程项目一开始就维持了最佳安全水准，该指南也可以帮助已经设计、制造甚至使用物联网产品或服务的组织。无论读者产品或服务处于哪个阶段，都有应该遵守的有效流程，从而从本文档集中获得最佳效益：

- 评估技术模型
- 审查当前产品或服务的安全模型
- 审查并评估建议
- 执行和审查
- 持续的生命周期

7.1 评估技术模型

该流程第一步，也是最重要的一步就是理解组织自身的物联网产品或服务。为了进行安全审查和风险评估，团队应熟悉组织解决方案中使用的各个组件、组件如何相互交互以及组件如何与环境交互。如果未能清楚了解产品或服务是怎样构建的（或者将如何构建），审查就不完整。

首先要制作文档，描述系统使用的每个组件。确认组件来源、用途、需要什么特权级别以及如何整合至整个解决方案。将每个组件与技术形成映射，对技术的描述位于每个终端生态系统 [3] 和服务生态系统 [4] 指南文档的“模型”部分。如果文档没有具体匹配某个组件也是可以接受的，因为文档应匹配组件的通用类别。只需要使用组件的类别作为语境，如微控制器、通信模块或信任密钥。思考以下问题：

- 使用哪些组件构建产品或服务？
- 哪些输入和输出适用于指定组件？
- 哪些安全控制已应用于这些输入和输出？
- 对组件应用了什么特权级别？
- 组织中谁负责执行组件？
- 组织中谁负责监控并管理组件？
- 采取了什么流程以应对组件中发现的风险？

回答这些问题有助于理解技术组件如何相互交互，整体产品或服务如何受到每个组件的影响。

该流程请参考 CERT OCTAVE 风险评估模型 [6] 的第一二阶段，或 NIST 风险管理框架 [5] 的框架阶段。这有助于为每项重要业务资产制定档案、建立安全目标并为企业评估、监控和应对风险建立根基。

7.2 审查当前安全模型

下一步，通读接受评估的终端或服务的安全模型部分。该部分有助于读者理解攻击者用于损害指定技术的模型。该模型基于多年以来在安全评估、逆向工程和设计嵌入式系统方面积累的经验。

审查安全模型后，读者应该可以更好地理解开发的产品或服务中哪些技术最薄弱，或者哪些技术最吸引攻击者。应该与组织分享该信息，确保工程师和领导者了解当前模型的风险和威胁。

但是，请注意，本阶段组织*不*应该采取措施调整安全模型。此时进行简明的架构更改还为时过早。

该流程请参考 CERT OCTAVE 模型 [6] 的前两个阶段，或 NIST 风险管理框架 [5] 的框架阶段。审查安全模型可以发现潜在安全漏洞，突出应优先处理的安全目标，从而提升技术模型。

7.3 审查并评估建议

此时应审查建议，以评估其*如何*解决安全任务。该部分不提供执行建议的方法，但会说明执行特定建议涉及的挑战。

每个建议中都提供*方法*部分。本部分将概述有助于修复或缓解相应安全风险的方法。这些方法着眼于较高层面，将概述从整体上降低风险的概念，以确保如果做出切实合理的努力，就可以取得最高收获。

*费用*部分将讨论组织执行特定建议时应准备的额外财务费用，如适用。大多数费用，如工程时间和原材料，都显而易见，但是不太明显的费用可能会改变那些企业领导者已经界定利润率和预算限制的产品和服务的费用。虽然没有提供具体数字，但已经说明了可能产生额外费用的技术和服务。

还设有*风险*部分，这样读者就可以理解*不*执行指定建议可能造成的安全漏洞。虽然企业可能会接受企业运营指南中列出的某些风险，但读者仍应查看每个风险部分，确保企业完全理解不执行（或不正确执行）指定建议的负面影响。“加密数据”等建议似乎看起来有些直白，但是有些威胁，如对于未设置独立密码的信息的重放攻击，可能会令读者在日后对其攻击敏锐性大为震惊。

还会根据情况提供*参考文献*以便进一步学习。虽然本文档未详细介绍每种技术、风险或修复计划，但这些内容在其他标准和已获认可的战略中都有提供。本文档集将在每项建议中提供材料的参考文献，如适用。

建议部分的查看结果应直接与安全任务部分关联。安全任务中应实施适合正确执行安全任务的建议。然后这些安全任务再转而关联到分配至组织成员的特定组件。

评估建议请参考 NIST 风险管理框架 [5] 的评估阶段，以及 CERT OCTAVE 方法的六、七、八阶段 [6]。

7.4 执行和审查

在该阶段，已列出清晰的安全任务，企业可以更好地理解其安全薄弱环节、价值及风险。企业现在应为要调整的每个组件创建清晰的架构模型，使用组织选择的风险评估流程为每个组件开发出威胁模型，并结合适合每个组件和安全任务的建议和风险。完成架构模型后，组织可以开始执行每项建议以实现安全任务。

执行完成后，组织应审查建议分部分和组件部分的风险。组织应确保执行能满足这些部分阐明的要求。然后组织还应确保执行可解决组织产品或服务设计组件相关的安全问题，因为这些文档无法充分处理领域中设计的每个产品或服务。如果可能，让第三方咨询公司评估执行，确保其确实符合安全最佳实践。

执行和审查请参考 NIST 风险管理框架 [5] 的回应部分，以及 CERT OCTAVE 模型 [6] 的第八阶段。

7.5 持续的生命周期

安全生命周期在此阶段不但没有结束，相反，它是一个流程整体架构的固有部分。终端和物联网服务都有生命周期，在此期间必须像生物体一样始终进行维护。

要求会随时间而变化。密码算法已经过时或遭到弃用。新协议和无线电技术必须与产品或服务交互操作。必须不断查看嵌入式产品使用的不断变化的生态系统，确保维护机密性、完整性、可用性和真实性。

管理持续的安全生命周期请参考 NIST 风险管理框架 [5] 的监控和框架部分，以及 CERT OCTAVE 模型 [6] 的第一、四和五阶段。

8 案例 - 可穿戴心率监视器

在本案例中，将使用该文档集对简易心率监视器 (HRM) 设计进行评估。将使用终端生态系统文档对终端进行评估，使用服务生态系统文档对设计服务进行评估。

8.1 终端概述

首先我们来评估一下终端的硬件设计。

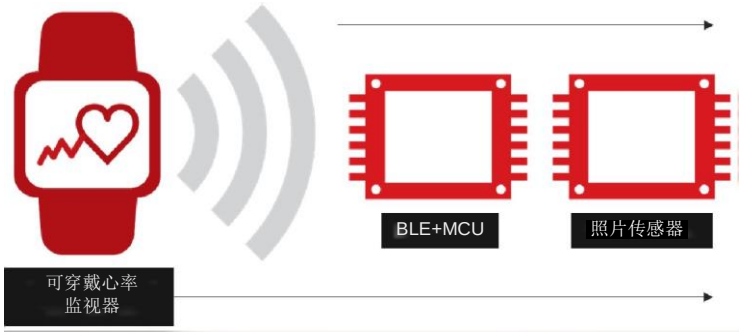

图 3 **- 简易 HRM 和主要组件**

HRM 由用于简易无线可穿戴设备的标准组件构成：环境光线照片传感器和蓝牙低功耗 (BLE) 微控制器。传感器用于获取脉搏率数据，而微控制器将分析传感器中发出的数据，并选择通过内置 BLE 收发器发送的数据。本案例中使用的 BLE 存储器为 4.2 版。

本案例采用纽扣电池，用于从 HRM 传输数据至其他设备，如智能手机或平板电脑。该设备运行不再需要其他组件。

根据终端生态系统文档，该设备属于轻型终端设备。

8.2 服务概述

从服务角度而言，智能手机或平板电脑中的应用程序可通过任何可用网络连接，将终端中的指标传输至后端服务。应用程序后端服务只是将设备所有者与获取的指标相关联，并将其存储至应用程序服务器本地数据库。

可通过移动应用程序或服务器网站实现数据可视化。可穿戴技术用户可登录服务器供应商网站，使用终端获取的指标进行更多操作。

这是一款简单而常见的服务模型，免去了定制或不必要的麻烦。

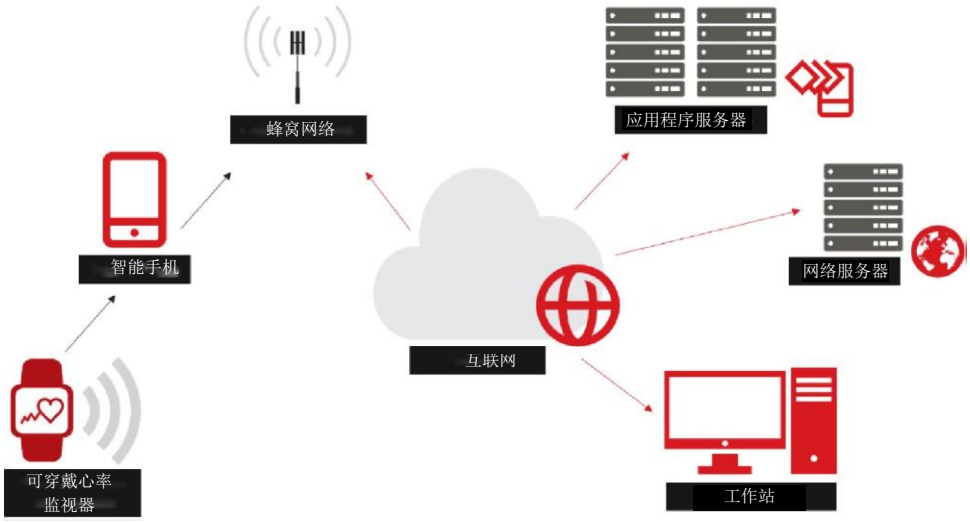

图 4 - **导向简单后端服务的数据流**

8.3 用例

使用该技术的企业旨在让终端用户全天候追踪脉搏数据，并将其存储至应用程序和后端数据库。这样用户可长期查看自身心率，以追踪整体健康状况。用户可以持续监控其健康状况有所改善还是恶化，当然这取决于是否保持健康的生活习惯。通过评估其 HRM 数据的积极与消极趋势，用户可得到相应的激励。

企业计划使用这些数据与医疗设备制造商、医疗保健供应商及其他组织合作，他们将通过这些指标确认消费者是否可能出现医疗相关事件，如心脏病或中风。

8.4 安全模型

在该案例中，工程团队利用终端和服务文档中常见安全问题部分确定与产品和服务最相关的问题。

从终端的角度来看，团队了解到要关注以下问题：

- 克隆
- 终端模拟
- 服务模拟
- 保证隐私

从服务的角度来看，团队确定要关注以下问题：

- 克隆
- 黑客服务
- 识别异常终端行为
- 限制损害
- 减少数据丢失
- 减少开发
- 管理用户隐私
- 提高可用性

团队审查了每个相关常见安全问题部分对上述每个问题的建议。然后团队选择执行建议，这些改进具有成本效益，可确保最高安全级别。

在该案例模型中，不需要对终端进行很多改变。由于终端作用微小，可以在应用程序安全和通信终端可使用最低安全级别。由于终端应用程序在单个设备上会闪动，只要设备固件*上锁*，在该用例中就不会产生针对终端的实际攻击威胁。

不过，出于隐私问题，组织应至少配备可信计算机的个性化 PSK 版本。这样可以保证每个终端具有唯一的加密令牌，一个终端受损不会导致所有终端受损。如果个性化（唯一）密钥编码为锁定微控制器，那么我们有理由相信，该用例可以完全不受克隆、模拟和隐私问题的威胁。审查物联网服务 [3] 和终端 [4] 文档，获得每个生态系统中哪些是可信计算基的完整讨论。

不过，这需要对服务器基础设施进行大量改变。工程师意识到，根据建议，他们面临严重的滥用风险。已确认以下问题：

- 没有可降低拒绝服务攻击效果的安全前端
- 没有限制服务流入和流出的入口或出口控制
- 服务层级之间没有职责分离
- 没有包括个性化 PSK 令牌的分开的安全数据库
- 服务操作系统中未采取足够的安全措施
- 未选取指标以评估异常终端行为

8.5 结果

执行建议后，组织有了更清晰的后端服务构架，完全可以应对指南中发现的风险。

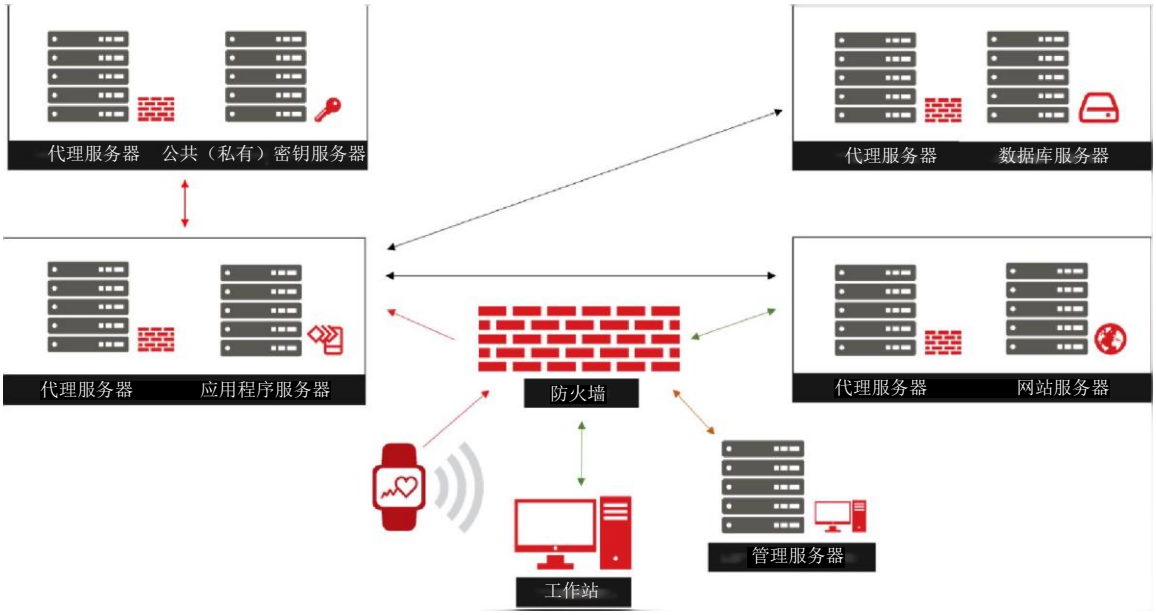

图 5 - **服务生态系统结果**

在上图中，可以清楚看到服务生态系统的变化。每个级别的服务被分成单独的级别，这样可以在需求激增时确保技术安全*并*轻松衡量技术。还添加了两个级别：数据库级别和认证级别，将重要系统从直接与外界交互的服务中分离出来。执行了安全前端，帮助保护内部网络不受多种攻击，包括降低系统整体可用性的 DoS 和 DDoS 攻击。最后还制定了管理模型，允许管理层安全访问生产环境。上图中未描述出的一个组件是分析模型，如果终端行为表示固件或硬件设计中存在损害或错误，该模型可以发现。

8.6 总结

总体而言，如果使用原始版本，这项简单的技术很容易受损。但是，如果对终端进行一些简单快速、成本效益高的更改，该技术足可以在领域中使用很多年，无需更换架构。

改善服务生态系统后，对于用户*和*企业的威胁就会减少。克隆和模拟将不再成为威胁。通过为每个终端授予唯一的密码令牌，就可以确保隐私。包含重要信息的系统从严重滥用、面向公众的系统中分离出来，还能确保安全。该模型虽然有些复杂，但可以减少生产环境的整体风险。

9 案例 - 个人无人机

在本案例中，将使用该文档集对小型个人无人机设备进行评估。将使用终端生态系统文档对终端进行评估，使用服务生态系统文档对设计服务进行评估。

9.1 终端概述

首先我们来评估一下终端的硬件设计。

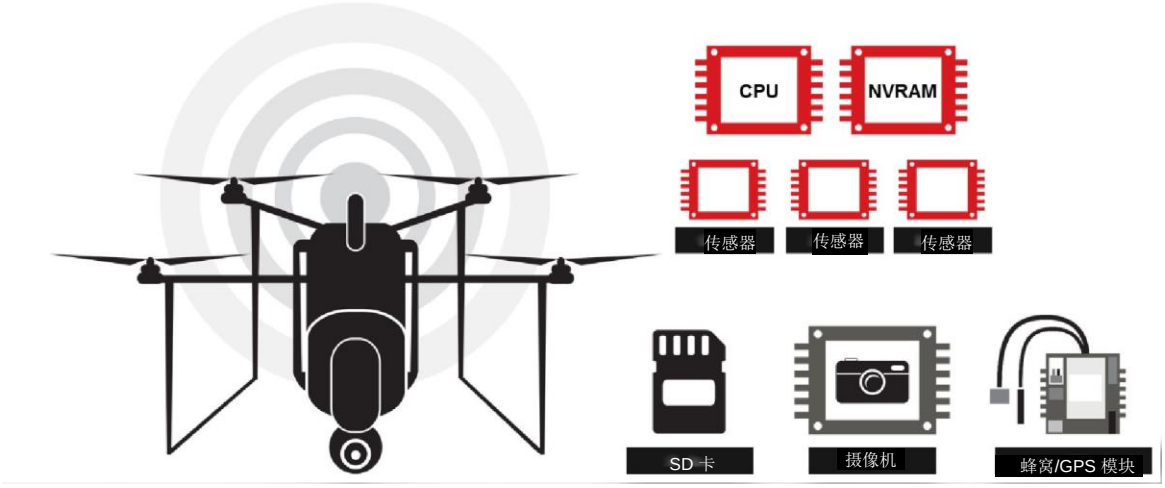

图 6 - **无人机及其主要组件**

这款个人无人机包括一系列强大的组件。无人机的处理功能强大，这主要得益于多个马达、传感器及必须并联发挥高效作用的其他装置。该模型采用 ARM Cortex-A8 CPU，基本操作系统 (Linux) 存储在独立芯片上的 NVRAM（非易失性随机访问存储器）中。需要各种传感器用于检测运动、光、速度等。SD/MMC 卡用于存储视频、传感器指标和元数据。配置有一台摄像机，这样操作人员可以从无人机的角度进行观察。还采用蜂窝/GPS 结合模块，以确保无人机与操作人员保持互联，即使已超出专有协议范围。GPS 还用于导航和最低程度的自动化。

锂聚合物 (LiPo) 电池用于驾驶无人机。如果同时开启所有功能，飞行大约两小时后将需要充电。

根据终端生态系统文档，该设备属于复杂终端设备。虽然无人机包括蜂窝模块，但它不是网关，因为不会向其他终端发送信息，或接收其他终端的信息。

9.2 服务概述

从服务的角度来看，只有飞行过程中检测到专用无线电接口缺失，才会使用后端，与操作人员进行互联。如果无人机飞行时还可以使用蜂窝连接，将尝试等待操作人员通过 LTE 网络进行连接。但是，如果无法通过 LTE 进行控制，它会尝试在本次起飞位置自动着陆。

然而，由于无人机具有轻微自动化功能，可获取移动坐标和路径，同时拍照或拍摄短视频。这些媒体文件可通过 LTE 实时上传至后端服务，向操作人员显示其自动执行过程中的轨迹和视角。

因此需要强大的后端服务，以确保可能连接系统的每架无人机都具有高度服务可用性。还需要高速网络流量，以通过蜂窝连接传输视频和高分辨率图片。网络界面也必不可少，它可以让操作人员在网络浏览器中查看媒体上传文件。

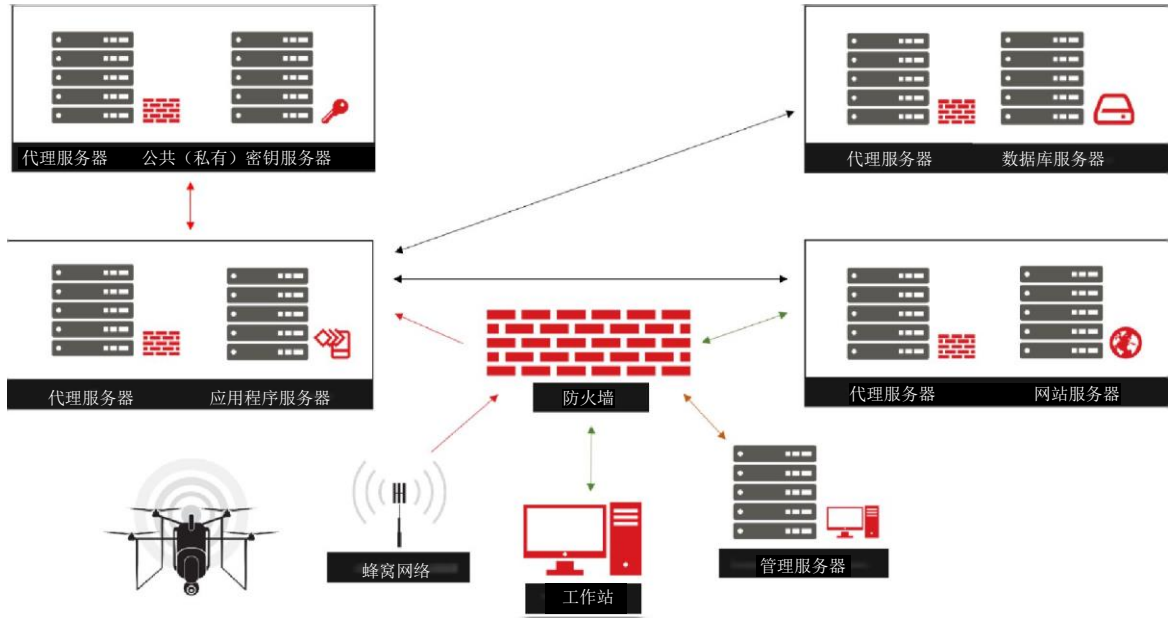

图 7 - 导向后端服务的数据流

9.3 用例

开发该技术的企业最初针对使用无人机进行野外拍摄的终端用户。但是，部分客户用无人机拍摄电影场景，因为从成本方面考虑，无人机的拍摄功能和稳定性非常强大。因此，无人机将会用到耗资大的拍摄项目中，而这些项目极其注重知识产权和隐私问题。

9.4 安全模型

在该案例中，工程团队利用终端和服务文档中常见安全问题部分确定与产品和服务最相关的问题。

从终端的角度来看，团队了解到要关注以下问题：

- 终端身份
- 终端模拟
- 信任密钥攻击
- 软件和固件干扰
- 安全远程管理
- 检测受损终端
- 服务模拟
- 保证隐私

从服务的角度来看，团队决定要关注以下问题：

- 管理用户隐私
- 提高可用性

团队审查了每个相关常见安全问题部分对上述每个问题的建议。然后团队选择执行建议，这些改进具有成本效益，可确保最高安全级别。

在该案例模型中，不需要对服务基础设施进行大规模改变。这是因为已经对服务基础设施进行了全面构建，以满足服务终端产品所需的流量。架构已经要求完整安全的架构，以能够有效扩大规模，保持资源的可用性，即使某些服务暂时出现故障。但组织选择进一步调查用户隐私，因为这已成为企业意外商机中争论的焦点。

但是，需要对终端基础设施进行大量改变。工程师意识到，根据建议，他们面临严重的滥用风险。已确认以下问题：

- 引导装载程序在执行操作系统内核前未恰当验证应用程序，导致造成干扰风险
- 未使用 TCB 管理应用程序或通信安全
- 由于没有恰当执行的 TCB 或信任密钥，终端模拟成为难题，可能导致数据泄露
  没有恰当执行的 TCB，终端无法正确验证服务
- 没有恰当执行的 TCB，终端无法通过专用无线电接口验证操作人员
- 工程师依靠 LTE 安全确保通信通道不受损，但未考虑终端模拟或 Femtocell 重构，这两项都会忽视 LTE 安全，不利于级别较低的服务安全

9.5 结果

执行上述问题相关建议后，组织对终端架构有了更完善的定义，足够应对通过指南文档识别的风险。

对于当前已投产的无人机，工程团队进行了固件更新，实施了个性化公钥安全模型。固件更新改善了引导装载程序，同时将安全性引入核心架构。由于采用了个性化公钥模型，任何企图滥用终端初始安全漏洞以试图冒充另一用户终端的行为都会失败，因为工程师利用现有的用户终端映射数据库为每个用户创建了个性化密钥。这样，没有适当网页凭证的用户不能下载并安装另一个用户的个性化公钥更新。虽然实现这一过程复杂且耗时，但却极有必要。

在未来的无人机技术中，将采用一个内部 CPU 信任锚。信任锚将与个性化公钥 TCB 相连接，确保每个终端配备独一无二而又完备的极度安全性。

按照这种方式配置强大的加密势在必行，因为对于公司已经确认关注的其他攻击类别，它也能够消除其潜在威胁。通过利用强大的加密和 TCB 的认证和验证，工程团队能够很轻松地识别是否流氓服务正被用于无人机。无人机一经检测到流氓服务，便能轻松降落至初始起飞地点。

检测到无人机出现安全漏洞的任何服务都能够从内部发出警告。届时管理团队便能确定如何应对存在潜在漏洞的无人机。这样处理安全事件就变得更加灵活，而且也为组织提供了一种新的方式，来评估是否有软件或硬件问题导致终端异常。

9.6 总结

虽然工程团队花费超乎预期的时间来创建一个从机械工程和后端服务视角出发的弹性架构，但要想打造安全终端技术就必须投入巨大工作量。此案例中没有提出针对整体业务的重要威胁，这是因为幸运的找到了*足以*满足客户需求的解决方案。倘若面对对安全更加严苛的技术，即便部署此解决方案也并不充足。

获取关于可信计算基变式（如个性化公钥 TCB 或个性化 PSK TCB）更多信息，请审查物联网服务 [3] 及终端 [4] 生态系统文档。

10 案例 - 车辆传感器网络

在此案例中，将使用这套指南评估部署在新类型汽车中的车辆传感器网络。将使用终端生态系统文档对终端进行评估，使用服务生态系统文档对设计服务端进行评估。

10.1 终端概述

首先我们来评估一下终端的硬件设计。

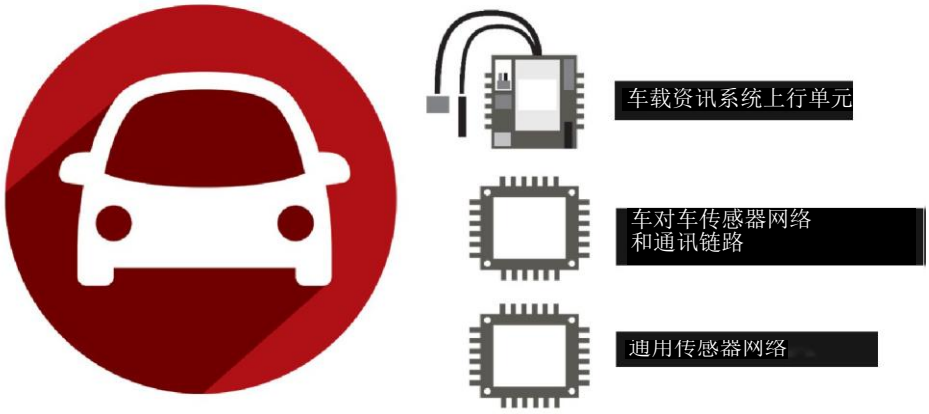

图 8 - **整车传感器网络及通讯系统**

尽管上述模型过于复杂，无法用一张简单的图表精确描述，但我们仍然可以看到其中的三个高级别组件：

- 车载资讯系统上行单元，管理传感器网络，按照驾驶员的指令作出决定，并保持与后端系统的连接
- 车对车 (V2V) 系统，用于对 V2V 事件进行检测和反应
- 通用传感器网络，为车载资讯系统上行单元提供性能指标

在现代汽车系统中，车载资讯系统单元是汽车计算机网络的一部分，并基于传感器数据和后端通讯做决定。该单元会与车辆驾驶员一起或代表其做出决定。该单元确保车辆能正确操作，并在紧急情况下尝试做出明智决定，而且接收来自后端网络的命令。

V2V 传感器网络识别周围区域的车辆，并基于传感器收集的指标做出决定。车载资讯系统单元主要基于组件（如制动器或轮胎压力监视器）的状态作出决定，而 V2V 系统根据其他车辆的存在作出决定，或者在关键事件情况下向附近车辆发出警报。

通用传感器网络是一系列组件，向车载资讯系统单元（有时也向 V2V 单元）提供数据。这些单元应用通用传感器网络收集的信息在关键事件时作出正确决定。

根据终端生态系统文档，该系统具有适合于每个物联网终端类的组件。车载资讯系统上行单元作为网关。V2V 单元作为一个复杂的终端。通用传感器设备是所有实质上的轻型终端。

10.2 服务概述

从服务的角度来看，车辆传感器网络将为后端环境提供性能指标。该数据可能会也可能不会提供给消费者，而是由制造商储存，用来观察或识别组件潜在的问题。这可能会触发服务警报，然后向消费者发出。

该系统还可以扩展功能，以便为消费者提供有用的服务，如“远程解锁门”、“启动引擎”以及类似的功能。在不久的将来，这些系统还可以通过自动导航系统远程驾驶车辆。

尽管大部分关键性决定是由车辆自身的处理单元做出，但是我们可以做一个合理的推测，随着更多的机器学习 (ML) 和人工智能 (AI) 与行为或统计模型结合用于制定更为复杂的决定，一些决策可以在云计算中做出。

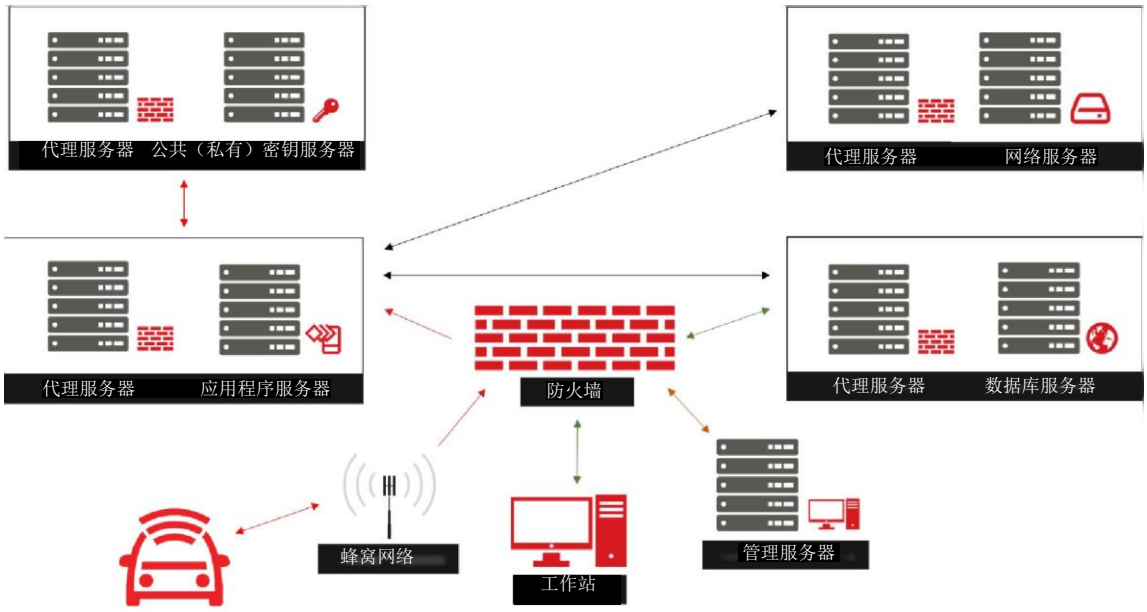

图 9- 导向后端服务的数据流

10.3 用例

这项技术的用例显而易见：打造可以在安全严苛场景下做出复杂决定的更加智能的车辆。目标是利用大量传感器的智能，在极短时间内做出关键性决定。自动阻断、爆胎广播警报、暂时禁用运营商的警告及其他通过使用传感器和精心设计的计算机系统可潜在地处理关键情况。

这项技术一个有趣的特征是它可能会对用户完全透明。用户不需要将这些计算机设置为以某种方式执行。相反，系统应该能够应用传感器性能指标顺利应对当前状况。这种设计可以使计算机无论在任何环境下都能正确操作。

10.4 安全模型

在该案例中，工程团队利用终端和服务文档中常见安全问题部分确定与产品和服务最相关的问题。

从终端的角度来看，团队了解到要关注以下问题：

- 终端模拟
- 服务或对等体模拟
- 旁道攻击
- 检测受损终端
- 在安全风险下确保安全

从服务的角度来看，团队决定要关注以下问题：

- 识别异常终端行为
- 管理用户隐私

该环境最大的风险，即对等体的模拟风险尚未在以前的案例中讨论过。在此类环境中值得工程师关注的风险是，计算机应用没有经过正确验证的数据做出关键决定。

由于在关键场景下传感器数据需要格外短暂的处理时间，因而理论上实施非对称加密或基于 PKI 的通讯可能并不总是可行。不过，这个断言可能并不准确。相反，一个准确的安全模型应该提前考虑时间紧急的情况，并为附近的终端缓存会话密钥。例如，如果两个物体以一个已知的速率接近彼此，服务生态系统的安全应用程序能够在他们到达在物理上可以相互影响的一定距离之前，准备好针对这两个终端的特定的会话密钥。这将确保终端和传感器之间的安全通信仍然可以在事件中使用，即便当潜在的关键情况（如即将发生的汽车碰撞）被检测到时，没有时间重新安排瞬时安全会话。

因此，扩展到 TCB 实施大有必要。GBA 是一个有趣的解决方案，其中用于车载资讯系统上行单元的 UICC 能够将密钥准确地分配到整个系统的终端。该协议甚至可以将安全会话密钥植入最基本的终端，可用于多种关键场景。这样，环境将始终源于信任根，即便轻型终端不具备公共密钥会话初始化的关键数字。

这些环境中另一个关键问题是检测被破坏的终端。例如，环境如何能够识别是否一个简单的传感器，如一个轮胎压力监视器 (TPM)，已经被破坏？如果计算机基于 TPM 爆胎信号做出关键决定，可能会出现安全问题。因此，设备的行为及其可信赖性，必须在每一个启动阶段进行重新评估。所有设备应具有防篡改性，并且如果被破坏必须能够通知网络。而且应该有一种方式可以让传感器网络上的其他设备能够评估网络上其他对等体的可信度。

10.5 结果

实施该建议后，车辆传感器网络得到很好的防护，以抵御车辆通讯网络上的攻击。GBA 用于将密钥分配到系统中的所有终端，并且在每一次启动时都运行此过程，以确保旧的密钥不被重复使用。除了以上方案，再结合防篡改性、每个终端强大的 TCB 以及一个组织信任根，便可以让环境在极低的风险下运行。

然而，不管是否有这些变化，安全仍然是一个关键因素。工程团队和业务领导，与公司的法律团队和保险经纪人一起，应该评估安全关键技术，并确定是否安全性可以在不危及使用者安全的情况下实现。虽然安全通常可以实现，甚至对于安全严苛场景亦是如此，但随着一些架构上的调整，安全有时必须是首先要关注的问题。

10.6 总结

此例中的系统通常经过精心设计，并且要付出巨大精力来攻击生态系统。然而在通讯体系结构中，即便是很微小的缺陷也会导致环境被破坏。在“围墙花园”中，比如一些 CAN 总线网络，单个有缺陷的终端能够让整个系统变得易受攻击。这对安全严苛环境来说是不可接受的。

附录 A 为物联网服务供应商建议的隐私注意事项

为了在物联网生态系统中建立信任，将正式监管干预的必要性降到最低，GSMA 提出以下高级别步骤作为指导，以最大限度地减少任何隐私风险。我们建议，物联网服务供应商遵循这些步骤，并在他们的物联网服务或产品的早期发展阶段考虑这些问题。

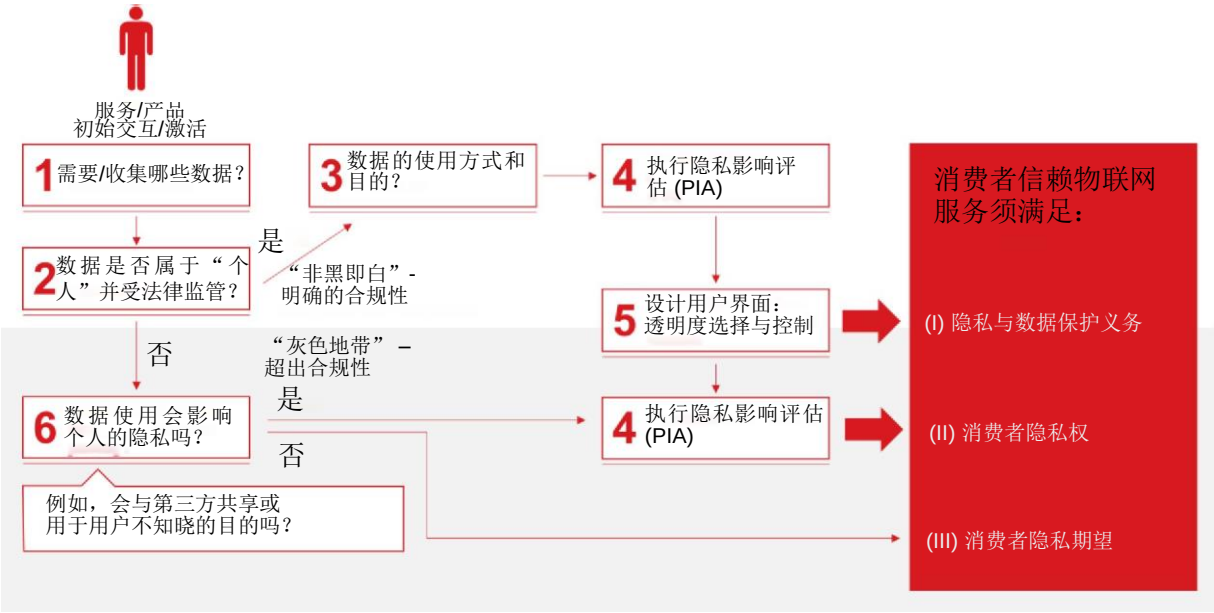

图 10- **GSMA 物联网隐私设计决策树**

步骤	事项
第 1 步	**您需要从用户收集哪些数据，以便您的物联网服务或产品能够正常运行？** 任何一个依赖于数据的商业模式第一步要做的就是确定实际上需要从消费者那里收集什么信息，以便服务或产品能够正常运行。服务需要的数据类型可以分为静态数据（如消费者的姓名或家庭地址）和动态数据（如实时位置）。所以如果您正在提供信息，例如健身腕带追踪某人的步伐和燃烧的热量，那么您需要知道体重、年龄、性别、移动距离和佩戴腕带者的心率，但您可能不需要个体的实际位置。 当评估所需数据类型时，同样重要的是确定使用这些数据是否需要个人的同意，以及如何获得同意，或切实提供能够控制其隐私偏好的选项。智能手机可以作为一种媒介，提供用户隐私选项（例如，移动应用程序或在线仪表板），该产品本身没有屏幕。

第 2 步	**数据是否属于“个人”并受法律监管？** 接下来应该确定法律规定的数据保护和隐私要求。考虑的问题包括： • 国家/市场相关的“个人”数据定义是什么？ • 收集的数据属于“个人”并受法律监管吗？如果是，您是否已确定允许您处理这些数据的法律依据？ • 您是否遵守任何与隐私相关的许可证条件（比如作为电信供应商）？ • 除常规数据保护法律外，是否有任何联邦、州、地方或部门的具体法律适用于您提出的数据采集模式？例如： o 金融/付款服务、医疗法规 o 跨境数据传输的潜在限制
第 3 步	**数据的使用方式和目的？** 法律合规要求一经确立，下一步就是筹划如何使用收集的数据以及需要与谁共享，以便实现预期结果，作为服务提供的一部分。以下问题应该能帮助您解决与数据处理有关的安全性和隐私方面的注意事项： • 在存储和传输时数据能够保持安全吗？ • 您清楚地列出了数据流吗？即，确定数据将如何使用并在整个价值链共享，用途是什么 • 为何每一种类型的数据收集都需要在提供预期服务的特定背景下进行，您如何解释？ • 您从一开始就定义/同意与您的合作伙伴的隐私责任（您的产品设计是否反映了这些责任？） • 与您目前正在共享消费者数据的公司是否有相应的合同协议？（例如，为自身商业目的限制分析供应商数据的使用）。这样的协议或限制可以是双向的，或者您可以建立一个行为准则或指导方针，并要求您的合作伙伴如果违反将承担定义的后果和责任。

第 4 步	**进行隐私影响评估** 进行隐私影响评估 (PIA) 包括： • 如果您的产品或服务会对个人隐私带来风险，确认是什么风险。 • 减少对个人信息可能出现的滥用可能引起的对个人的危害风险 • 设计一个更加有效的处理个人数据的程序 PIA 要求在数据保护和隐私法中越来越常见。具有多种有关如何进行 PIA 的指南，包括由英国信息专员办公室 [10] 和隐私权专家国际协会推出的版本。 进行 PIA 时需要处理的典型问题包括： • 该项目会导致您/您的合作伙伴作出决定，或对个人采取行动，从而对他们产生重大影响吗？ • 该个人信息是特别容易引起隐私关注或期望的信息吗？例如，健康档案、犯罪记录或其他人们认为私有的信息？ • 该项目是否要求您以可能让个体感到侵扰的方式与之联系？
第 5 步	**用户界面的隐私设计** 在评估消费者的隐私风险后，您应该考虑如何提高这些消费者发现风险及降低风险的意识，并为其提供能表达隐私偏好的选项。最后一步是确保您以用户友好的方式提供服务，并满足您的法律义务及消费者的需求和期望。这样可赢得消费者信任，使其确信自己对隐私更有把控力。考虑的问题包括： • 如何让消费者意识到其隐私风险，并如何做出明智选择？ • 您是否按照法律要求获得其许可？许可的关键要素包括：披露、理解、自愿、权限及协议 • 数据在传输和静态时是否安全？ • 您保留消费者数据是否需要一个规定时间，为什么？ • 消费过程有助于赢得他们的信任吗？比如： o 他们是否了解使用服务需贡献哪些数据? o 消费者可以通过简单的步骤来表达他们的隐私偏好，例如，基于网络的“权限控制台”、“及时”提醒、呼叫中心、移动应用程序、语音激活命令等等。

第 6 步	**数据使用会影响个人的隐私吗？** 您的产品或服务收集的数据可能按照法律不会归为“个人”，但可能仍然涉及消费者的隐私，因此应该按如上所述进行考虑。要确定相关数据是否会影响消费者的隐私，需考虑以下问题： • 您的服务/产品所收集的非个人数据结合其他渠道的数据，是否能推断出消费者个人生活？比如推断与其相关的生活方式、习惯或宗教，是否： o 会对他/她获得医疗保险产生影响？ o 会被第三方（零售商、保险公司）利用，从而对特定消费者产生价格歧视？ • 如果您的产品或服务在将来某个时候发生改变，那么可能会对消费者的隐私产生什么变化？比如： o 这些变化是否牵涉消费者的新数据收集（如位置数据）？ o 是否将现存或新的消费者数据共享或出售给第三方（如广告商），且将消费者数据用于与最初获得数据时截然不同的目的？ • 如果发生任何变化，您应： o 检查对您业务的可能影响（如果因此变化导致新法律实行） o 创建流程以通知消费者，并在必要时获得其同意 o 为消费者提供改变其隐私偏好的方式 • 我们为物联网服务供应商建议的其他注意事项为： o 确保您有适当的合同协议，定义价值链中每一个合作伙伴的责任 o 有明确的补救过程，让消费者清楚如果出现问题或遭遇隐私侵犯应向谁求助

下图展示的是如何证明上述建议步骤的一个选项：

附录 B 基于汽车跟踪系统的案例

在该案例中，将从物联网安全准则的角度对汽车跟踪系统进行评价。这一过程基于本概述文档的第六节 -“有效使用本指南”。

B.1 评估技术模型

第一步“评估技术模型”，工程团队根据其产品架构评估设备如何运行。工程团队创建了一个文档，逐条列举了用于解决组织人员、分配安全任务和跟踪进度的各项技术。

简单起见，我们的汽车跟踪系统将具有以下功能：

- **终端生态系统：**
  - 一个简单的图形用户界面 (GUI)，用户可用来：
    - 以用户名和密码登录
    - 禁用跟踪
    - 启用跟踪
    - 确认并可视化当前位置
  - 连接到后端服务的蜂窝模块
  - 用于蜂窝模块的 SIM 卡
  - 用于备用电源的锂聚合物电池
  - 中央处理器 (CPU)
  - 一种在非易失性 RAM（内存）中的嵌入式应用
  - RAM
  - EEPROM

- **服务生态系统：**
  - 蜂窝数据连接
  - 安全专用 APN （Access Point Name，接入点名称）
  - 服务接入点
  - 蜂窝调制解调器 OTA 管理服务
  - SIM 卡 OTA 管理服务

在标记每一项技术相关的信息后，团队回顾了每一个指南文档的模型部分，并确定适当的技术模型。这是一个复杂终端。服务和网络模型是一个标准的移动式物联网服务。

B.2 检查安全模型

随着技术模型已初步完成，组织现在应该准备进入检查安全模型环节。在安全模型中，团队将评估对手如何攻击解决方案。

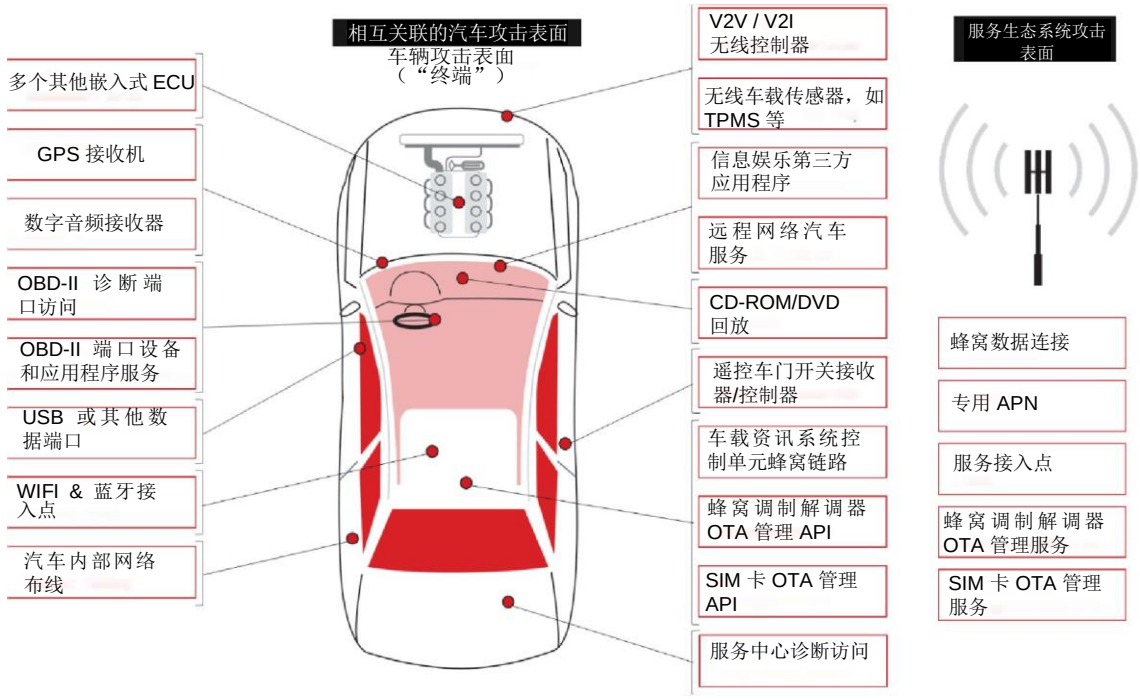

图 11- 相互关联的汽车攻击表面

在我们的案例解决方案中，只有两个与攻击有关的威胁表面：

- 蜂窝网络
- 对车辆的局部攻击

由于没有本地网络连接，只有移动网络连接，攻击者必须折中选择蜂窝网络连接，从私人 APN 进入通讯通道，或者通过服务接入点、蜂窝调制解调器 OTA 管理服务器或 SIM 卡 OTA 管理服务器进入。

物理攻击是损害设备的唯一其他方式，其中有多个入口点（如上图所示），因此在此物联网服务环境下，应重点关注终端。

B.3 审查和分配安全任务

完成安全模型评估后分配安全任务就简单易行了。每个团队都应分配一个特定人员，负责需要评估的解决方案的每个组件。评估不应该只从高层级（终端、网络和服务）进行，还应从子部件进行。这意味着 CPU 应该分配一名操作员，以及操作系统和网络服务等等。

一旦每个组件都被分配给一个所有者，这个过程就可以开始了。也就是说，在这个阶段团队要明确：

- 技术是如何构成
- 哪些技术影响安全性
- 哪些工程利益相关者拥有既定的技术

B.4 审查建议

在建议审查阶段，团队的每个成员应该阅读并理解尽可能*多*的建议。这样做极为必要。工程人员不能仅关注特定部分的建议，而是应该花时间去了解尽可能多的建议，即便仅从较高层级获得更佳视角，了解组件如何影响其产品或服务的整体安全性。这样一来，针对何种整治或缓和策略能够实现成本效益、长久性和管理层面的最佳平衡状态，该团队就能进行有价值的讨论。

这些建议一旦审查，*组件所有者*可以判断是否建议已被应用，或将其标记成一个*未决建议*。团队便可以在其部署前就建议的适用性进行讨论。这项政策更具实际意义，因为一些建议可能有副作用，会对其他建议的实现或现有的控制产生影响。

在该案例中，团队已经确定：

- 应使用应用程序信任基
- 应定义组织的信任根
- 应实现设备个人化
- 应实施防篡改保护
- 应执行终端密码管理
- 应执行终端通讯安全
- 应实现加密签名的图像
- 应实施隐私管理
- 应集成设备电源警报

B.5 组件风险评估

接下来，组件部分应进行评估，以确定在实施或整合一个特定组件到产品或服务时所涉及的各种风险。本节一般只能由组件所有者来进行审查，以尽量减少工作。尽管如此，尽可能多的了解这些建议将大有裨益。

审查建议和组件风险部分后，下列安全漏洞被确定：

- 存储在 EEPROM 未受保护的隐私
- 未经处理的内部 RAM 中的隐私
- 用户界面必须保护密码
- 用户隐私应向用户列明

B.6 执行和审查

现在团队可以调整解决方案，以遵守商定的安全要求。若有需要，团队需重新实施组件或添加安全控制。

在此特例中，团队确定其正与 GSMA 成员一起共事，该成员能够提供包含支持应用的信任锚技术的 SIM 卡。他们通过现有的 SIM 卡解决其对信任锚的需求。这同时解决了个人化问题，因为每个 SIM 可以在使用标准 GSMA 技术的领域实现个人化。

SIM 技术还有助于提供空中通信安全密钥，解决实现通信认证和隐私的需要。

SIM 专门针对公司的区域编程出一个信任基，使企业能够通过证书链进行同侪验证。这解决了组织信任根和同行验证的要求。

产品包装更新为相应的防伪包装。

EEPROM 由数据进行编码，并由储存在 SIM 信任锚的安全密钥进行加密。

引导装载程序经过改良，使用信任锚进行应用图像的验证。

终端被重新设定程序，通过在用户输入密码时使密码字符不可见支持安全密码输入。

增加一个隐私管理 GUI，用户可以查看和控制业务所收集的信息。

隐私仅在同一芯片的内部存储器中处理。

一旦这些实施确定，该团队重新评估所有的安全性建议和风险，并审查安全模型，以确定这些变化措施是否已经解决其问题。

B.7 持续的生命周期

既然团队已经完成了批准配置，接下来就可以部署其技术了。然而安全性要求并不止于此。该团队需要探讨监测异常终端及识别所应用技术是否包含新发现的安全漏洞的方法。

该团队将为如何识别、修复及恢复每次事件或漏洞制定计划。这将确保，随着时间的推移，不断变化的技术和安全形势不会出现让组织措手不及的情况。

附录 C 文档管理

C.1 文档历史

版本	日期	变更简要说明	批准机构	编辑/公司
1.0	2016 年 2 月 8 日	新版 PRD CLP.11	PSMC	Ian Smith GSMA & Don A. Bailey Lab Mouse Security

C.2 其他信息

类型	描述
文件所有者	互联生活项目
联系信息	Ian Smith - 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，请联系我们表达您的意见。您可发送邮件至 prd@gsma.com。

随时欢迎您向我们提出建议和问题。