China unicom中国联通
创新 改变世界

HUAWEI

物联网安全技术白皮书 2018

——安全架构的不断演进

前言

物联网（Internet of Things，简称IoT）将海量的设备互联，以联接为基础，以数据为核心，以价值创造为突破，正在成为我们社会生活的一部分。同时，新业务变化也为各行各业带来了新的安全威胁和挑战。

2017年2月，华为公司与西班牙网络安全局（INCIBE）、Red.es在2017世界移动大会期间联合发布了名为《共建可信可管的物联网世界》的白皮书。2017年10月，华为公司进一步提出创新的“3T+1M物联网安全架构”，覆盖从终端到应用的E2E安全需求。发布《物联网安全技术白皮书2017》，呼吁业界共建安全。

本白皮书是中国联通网络技术研究院和华为公司，在继承以上成果的基础上，进一步展示IoT安全领域的最新研究与优秀实践。探讨通过政府、行业、标准组织、认证机构、产业联盟等多利益方的开放合作，共同探索和应对新技术应用的安全风险及隐私保护要求，共建IoT安全生态，促进物联网产业的快速、健康发展。

目录

1 IoT趋势和威胁

1.1 IoT发展趋势

第四次技术革命正在引领人类社会迈向万物感知、万物互联、万物智能的全新时代，IoT是整个新时代的基石。IoT本质是借助ICT技术对传统产业进行重构，通过物理世界和数字世界的融合，缩短业务流程、提升生产效率，为客户提供更好的产品和服务，释放出产业创新的巨大潜能。

未来所有的物都将被联接起来，而联接物的场景，比联接人的场景更丰富、更多元化。政府在消防、路灯、井盖、停车、单车、水表气表、环境监测等应用上的智慧化建设诉求（提高城市管理效率，提升市民生活质量），带来新一波联接发展的巨大机遇。同时，通过IoT平台整合跨行业的开放数据，把消费者相关的资产数据进行关联（水电气、智能门锁、宠物跟踪、家庭安防、行李箱、车辆等），并通过统一入口为个人提供更智能、更便利的生活体验。

IoT驱动全球各行各业数字化、智能化，带来巨大的经济价值。IoT已经成为全行业数字化转型的驱动力，全球的公司、政府、组织和团体都在积极投入和研究这一仍处在发展中的技术，利用遍布各处的传感器，广泛收集和分析数据并应用，以更好地支撑各行各业的快速发展。

根据华为GIV预测，随着万物感知和万物互联的升级，一切都将被带入万物智能的世界。到2025年，个人智能终端数将达400亿，全球联接总数达到1000亿，这些联接将泛在于公用事业、交通、制造、医疗、农业、金融等各个领域，推动数字化转型，创造23万亿美金数字经济[1]。伴随着感知、联接能力全面提升，IoT以联接为基础，以数据为核心，以价值创造为突破，正在成为我们社会生活的一部分。

1.2 威胁和挑战

正如硬币有正反两面，IoT驱动全行业数字化的同时，也带来了新技术应用的安全风险。首先，用于攻击物联网的工具越来越先进，机器学习和人工智能将加剧攻防对抗，防护方面通过AI快速检测到新的安全威胁，攻击者也在利用AI技术发起攻击。其次，实施攻击的技术门槛越来越低，IoT终端设备成为新的攻击对象，冰箱、扫地机器人、水表、路灯都会成为潜在攻击目标。根据Gartner预测，到2020年，企业发现的攻击中超过25%涉及物联网[2]。同时，传统的网络安全边界被打破，不同物理位置和网络层级的设备联网后，产生出更多的攻击点。攻击者可以在不同地理位置进行不同程度的攻击，为内网跳板攻击提供了便利。值得注意的是，攻击者正在从直接利用设备漏洞攻击设备，转向通过自动化工具进行模拟合法操作，再利用设备作为跳板发起攻击的新兴方式。

随着IoT业务越来越多的进入落地运营阶段，行业客户也明显认识到IoT安全的重要性，Gartner预测全球物联网安全支出将在2018年达到15.06亿美元，比2017年的11.74亿美元增长28%[3]。不同的商业应用面临的威胁也是差异巨大的，可以想象，智能路灯和车联网所面临的风险是完全不相同的。物联网安全也需要从单一的产品安全，走向端到端解决方案安全，并要从端到端解决方案的安全提升到整个架构的安全。通过不断演进的安全架构，来满足未来更多新的商业应用场景，如智慧城市、智慧能源、智慧交通、智慧制造/工业4.0、智慧生活、自动驾驶等。

[1]GIV 2025, https://www.huawei.com/minisite/giv/cn/

[2]Leading the IoT, https://www.gartner.com/imagesrv/books/iot/iotEbook_digital.pdf

[3]Gartner, https://www.gartner.com/newsroom/id/3869181

2 不断演进的3T+1M安全架构

物联网安全涉及低功耗广域网络（LPWA）、车联网、工业物联网、可穿戴等领域。与传统网络安全威胁相比，在物联网万物互连互通的环境中，海量的物联网终端生成并使用海量的数据，管道为这些数据提供高并发的安全通信保障，云端和物联网平台支撑着丰富的物联网应用，这些支撑的系统和应用有可能沦为潜在恶意攻击的目标。“3T+1M安全架构”聚焦端、管、云和平台的安全特性的组合协同，应对物联网基础架构中的感知层、网络层和应用层的安全威胁；同时立足于平台安全和云端安全，依托传统电信网络安全保障能力优势，提供物联网安全态势感知与分析检测；联合生态合作伙伴，共同致力于解决物联网的安全威胁与挑战。基于不同行业应用对IoT云管端的安全需求，尤其是具有行业特点的差异化安全需求的分析，促进“3T+1M安全架构”的不断演进和技术创新。在创新中构筑安全，在演进中满足多元化的应用需求。

图1：物联网安全解决方案3T+1M安全框架

T：安全技术族，M：安全运维与管理

3T+1M物联网安全解决方案，核心在于基于IoT应用场景（车联网、LPWA应用、工业物联网等）安全威胁，构建起IoT终端防御、管道保障、云端保护三个IoT安全技术族（Technology）和安全运维与管理(Management)，以此满足国家和区域法律法规、行业标准等合规要求，构建物联网安全端到端纵深防御体系，抵御威胁。这其中包括：

1. 物联网终端防御技术族（1T）：针对IoT不同应用场景、具备不同处理能力的终端，提供与其能力相匹配、端云协同的关键安全技术族。对于弱终端（如：LPWA智能抄表、共享单车锁等）需满足基本安全能力，如数据传输层加密协议DTLS或DTLS+、终端可信DICE、FOTA升级、安全启动等，而对于强终端（比如车联网T-Box、OBU等），还进一步需满足安全证书管理、入侵检测、加密认证、TPM等。

2. 物联网管道保障技术族（1T）：IoT管道安全最核心的能力在于恶意行为检测与隔离，特别是针对物联网终端（比如车联网T-Box、LPWA智能路灯等）异常行为（比如流量异常、上报频次异常等）进行快速检测和隔离。同时针对不同场景增强物联网管道安全能力，比如针对NB-IoT场景增强防DDoS攻击和防信令风暴能力，而针对车联网C-ITS则需重点构建车路网协同通信可信能力等。

3. 物联网平台保护技术族（1T）：重点在IoT平台和云端提供LPWA场景的大数据安全分析的态势感知、车联网安全分析感知能力，同时聚焦平台的IoT数据安全与隐私保护，为客户提供可配置的云安全保障能力。

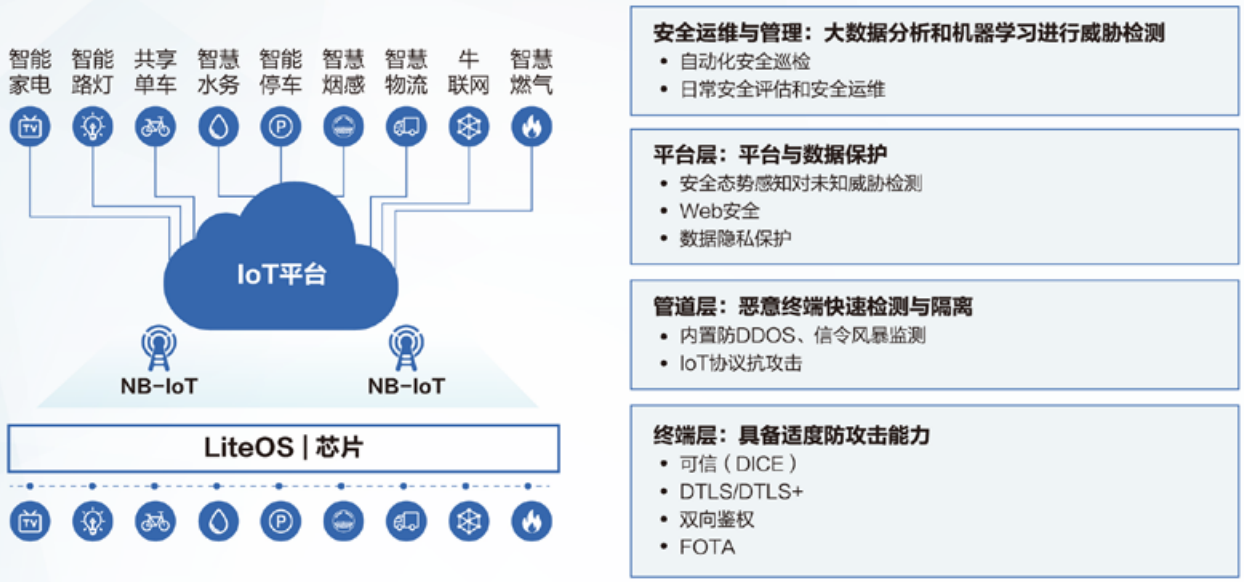
4. 物联网安全运维和管理（1M）：重点在于制定安全运维操作规范和流程并构建端到端的安全运维工具，提高安全运维人员和开发测试人员效率，提升整个IoT安全体系事前预防预警、事中检测分析和事后响应等能力，包括安全巡检工具、定期物联网安全评估、自动化终端和应用安全检测工具等。

需要强调的是，3T+1M架构中IoT安全关键技术能力构建，虽然侧重点有所不同，有些侧重于端侧，有些侧重于管道或者云端，但都不是孤点的防御，需要通过端、管、云以及运维的相互协同，构筑整体的安全防御体系。特别是物联网终端受限于资源和应用场景，在构建防御能力上，需要通过云端或管道来进行协同，比如终端可信、恶意终端检测、DTLS+等。

3 3T+1M安全架构在LPWA领域的应用

LPWA专为低带宽、低功耗、远距离、大量连接的物联网应用而设计，多用于基础设施领域，如智慧照明、智能停车、智能抄表等。物联网3T+1M安全架构采用多道防线，多层防御：

图2：LPWA领域的3T+1M安全架构



终端适度防攻击能力：

物联网终端应具备适度防攻击能力。对于资源受限，成本功耗敏感的弱终端提供匹配的安全能力，例如：远程安全升级管理服务（FOTA），轻量级系统安全（LiteOS），支持轻量级可信计算（DICE）的芯片，轻量级安全传输协议DTLS+等。

恶意终端检测与隔离：

海量物联网终端中异常行为的检测与隔离能力，例如：为NB-IoT网络提供管道侧的防海量终端浪涌式风暴检测服务；基于大数据分析检测NB-IoT终端异常，将确定的恶意终端进行隔离；支持网络访问黑白名单等。

平台数据安全与隐私保护：

云端平台数据安全防护与隐私保护能力，例如：数据隐私保护和生命周期管理、数据的API安全授权、租户数据隔离，采用云安全（如WAF、防火墙、HIDS等）和大数据安全技术，保护平台不受恶意攻击等。

安全管控与运维：

智能化安全态势感知能力，包括安全运维、定期物联网安全评估、安全报告和基于最佳实践策略自动识别安全事件。可选提供基于策略编排、策略制定和安全策略执行的安全管理平台。

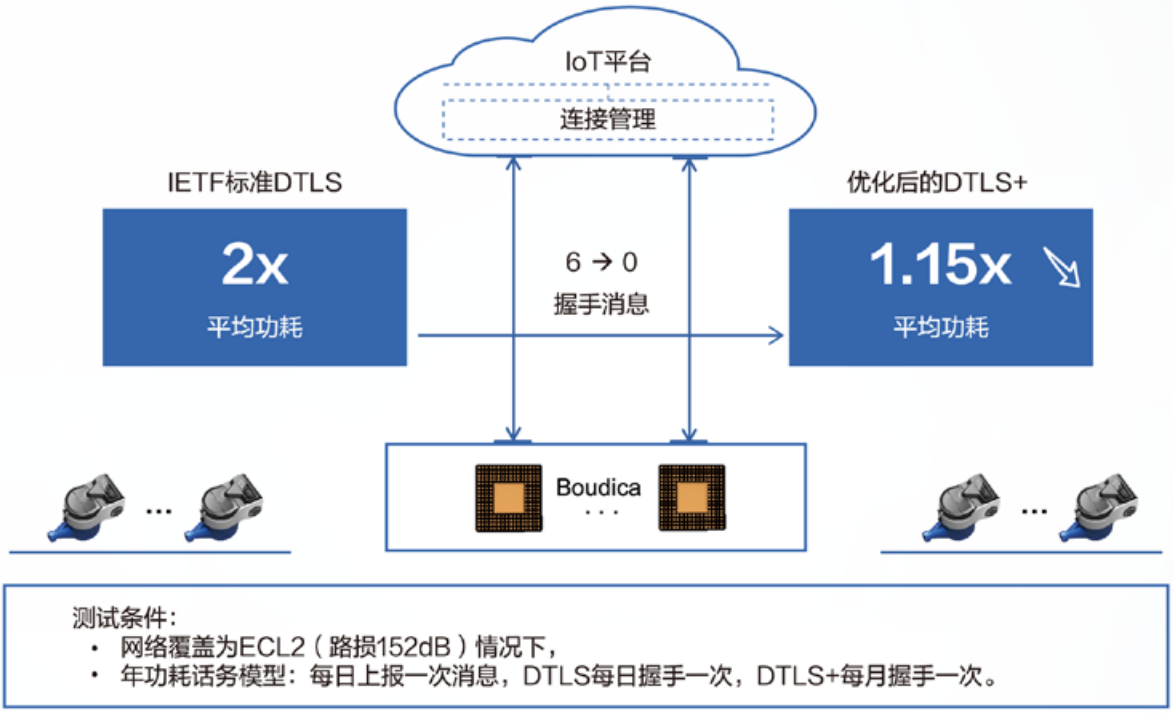
3.1 LPWA领域关键安全技术介绍

设计 LPWA 安全解决方案时需考虑其场景特点，安全技术需综合考虑成本、电池寿命等LPWA网络特有的因素。下面介绍在业务场景应用的几个关键的网络安全技术：

▶ DTLS+

为降低电池功耗，NB-IoT终端通常大部分时间处于休眠状态。传统的DTLS对通信进行加密需要在每次终端结束休眠执行一系列握手动作以重新建立安全信道，严重影响功耗。DTLS+创新地引入connection id，重用原有安全信道，解决该问题，降低40%功耗。DTLS+已经在IETF TLS工作组提交草案（DTLS Connection Identifier），即将发布为正式标准。下图是对DTLS及DTLS+的概要对比分析。

图3：DTLS及DTLS+的概要对比



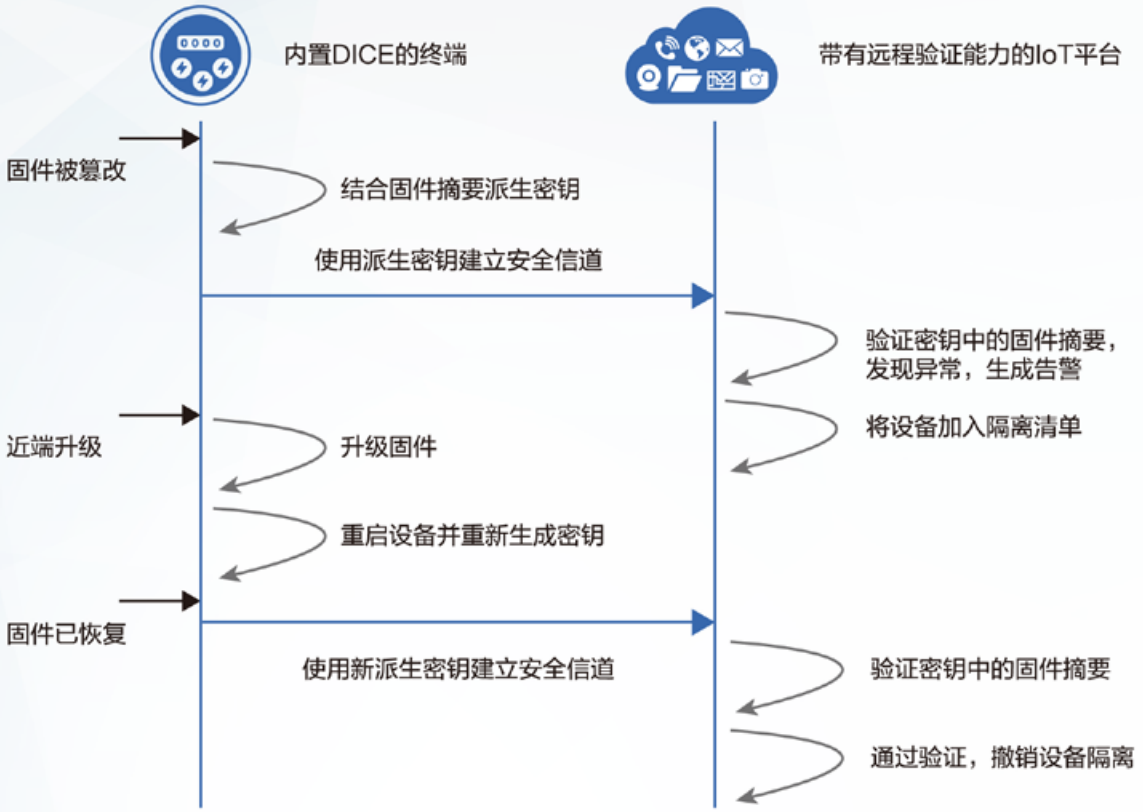
▶ DICE

NB-IoT终端大多部署在户外，易受攻击和篡改，同时这些终端性能低、资源受限（如电池供电）。Boudica芯片参考TCG（可信计算组织，制定可信计算相关的规范和标准）制定的DICE（Device Identifier Composition Engine）规范，为资源受限的NB-IoT设备引入轻量级可信计算能力。

IoT终端利用DICE功能建立身份认证标识后，IoT平台对终端固件进行远程验证，识别异常则告警并将相应终端转入隔离区域。应用DICE方案，可以带来以下价值：

- 设备防伪造，提供基于硬件的身份标识
- 远程证明设备的完整性
- 实现设备零接触安全部署

图4：DICE工作流程



▶ 终端异常行为检测与隔离

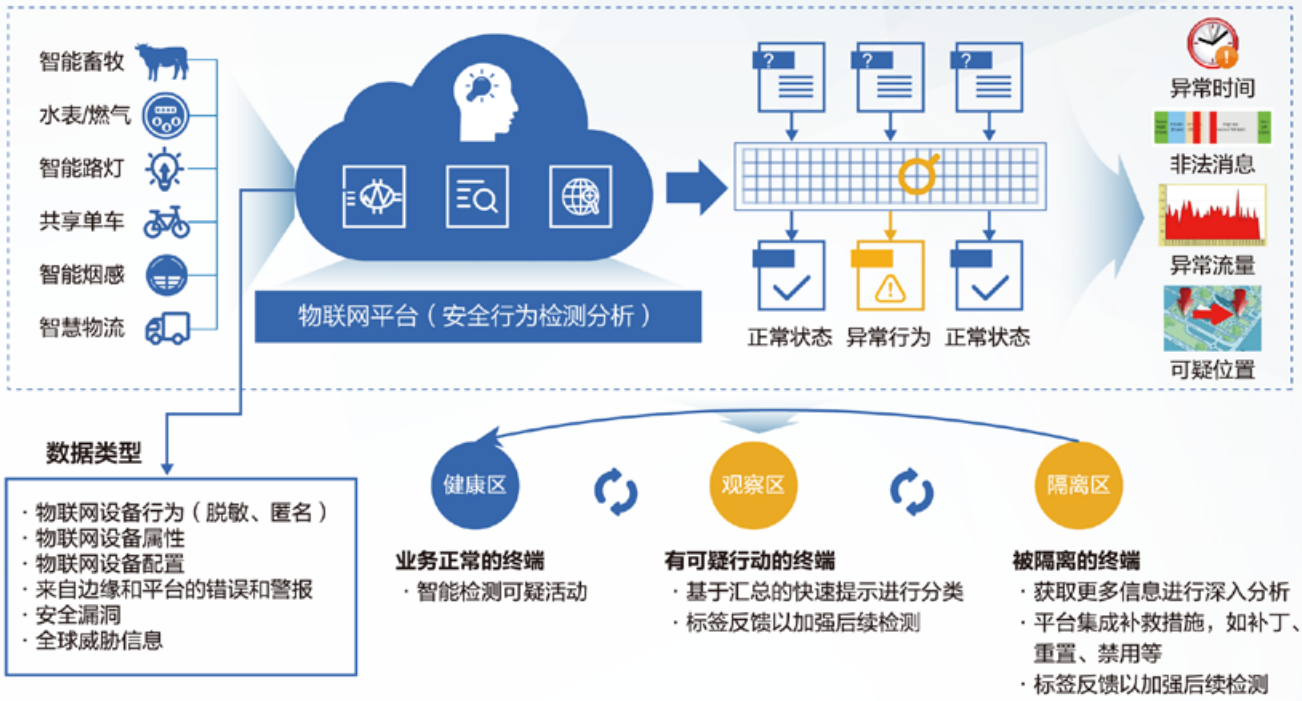
IoT终端种类日益众多，各个厂商的设备具有不同的功能以及实现方式，安全水平参差不齐，难免出现众多安全问题。这些终端一旦被控制，可以被用于影响业务正常运行或向平台及网络发起攻击，甚至进一步影响其他互联网用户。如何在海量终端中快速识别异常终端并隔离，是IoT安全解决方案重要的一个技术关注点。

异常终端检测特性可以为客户带来如下价值：

- 海量的终端设备安全状态可视化；
- 提升安全管理效率；
- 降低安全风险；
- 实现分级管理，兼顾效率和安全。

在保护隐私的基础上，结合物联网设备的属性、配置，对设备的告警、行为等进行领域建模、大数据分析，结合外部的威胁信息，识别和检测出物联网设备异常，将确定的恶意设备进行隔离，实现对设备正常、可疑、异常三种状态可视检测。

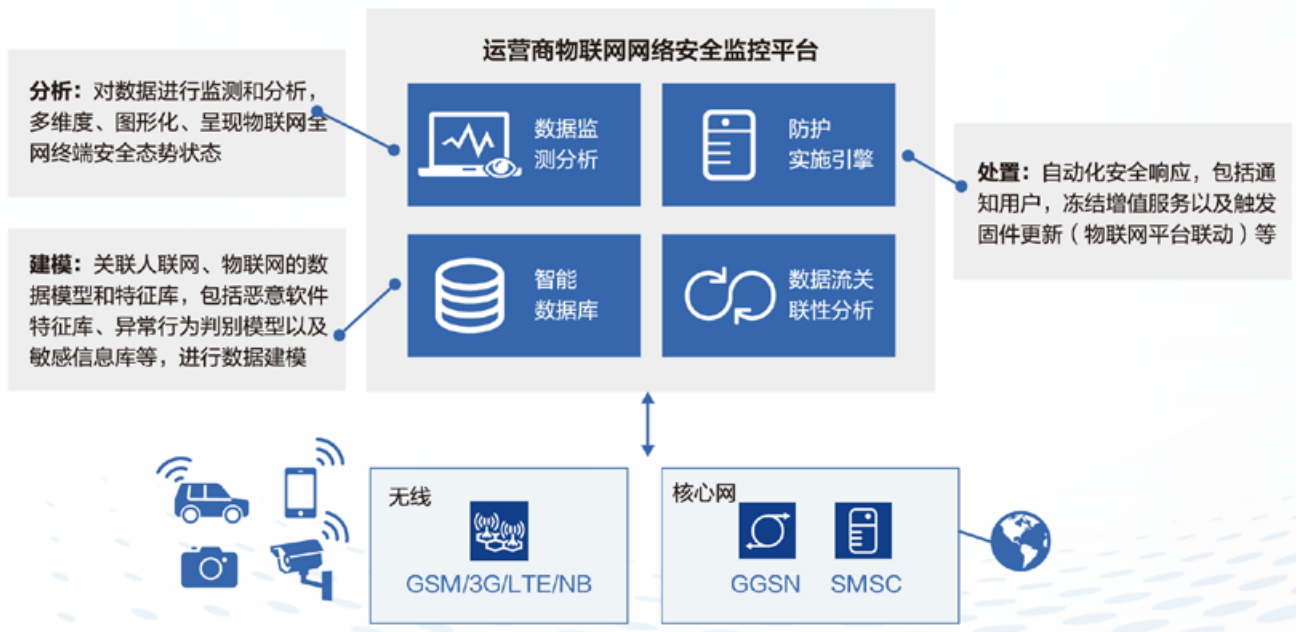
图5：终端异常行为检测与隔离



▶ 物联网网络安全监控

针对NB-IoT终端体积小、数量多、位置分散、安全防护能力差，易遭受网络攻击的问题，监控平台从网络侧入手通过流量采集、分析发现异常行为，通过各类安全引擎判别恶意攻击类型，根据策略进行威胁处置，对客户提供终端安全告警和各类定制安全服务，同时提高网络整体安全态势感知能力。

图6：网络侧安全监控平台

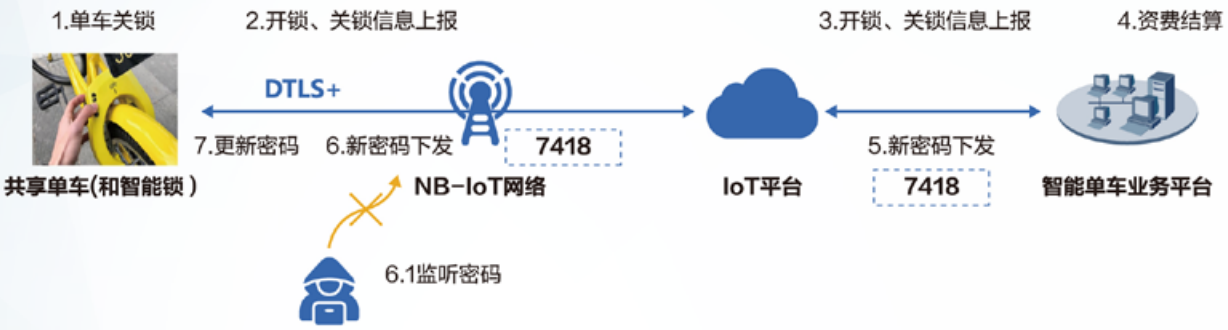


3.2 共享单车

共享单车通过无线技术进行自行车的位置定位、开解锁等功能，极大的提升市民出行的便捷性。通过自行车的共享使用，达成绿色出行，节能减排，满足市民最后3公里的出行需求。共享单车使用后，锁车时单车业务平台将向智能锁下发新的开锁密码。攻击者可以通过中间人攻击，窃取密码，实现免费骑行。

针对这种攻击场景，重点在于网络通信数据的加密。由于单车智能锁使用电池供电，所以仅在需要上报或接收消息时与平台建立短暂连接。传统的网络通信加密协议DTLS在该场景下功耗高，影响电池寿命。采用DTLS+的方案，在保证单车智能锁与IoT平台通信安全的同时，极大地降低智能锁电池消耗。

图7：共享单车的攻击和防御



3.3 智能抄表

智能水表实现低功耗、广覆盖诉求，并通过平台实现不同厂家水表统一接入，数据统一融合，给自来水公司应用提供统一数据管理能力，完成智能抄表业务。

水表会记录住户/商户用水情况进行上报，自来水公司根据上报的用水情况进行计费。攻击者或不法住户/商户会通过水表的近端接入方式（无线或串口）篡改水表固件以达到篡改水表计数，进而减少付费的目的。

为防止水表件被篡改，华为提供内置轻量级可信计算DICE的Boudica芯片。使用Boudica芯片的水表，若固件被篡改，一旦重新接入IoT平台，平台侧会基于DICE技术判断水表固件已被篡改，并进行隔离及告警。据此，自来水公司可对相应水表固件进行恢复。恢复后的水表重新接入IoT平台，平台验证通过其合法性后可正常上报业务数据。

图8：智能水表的攻击和防御

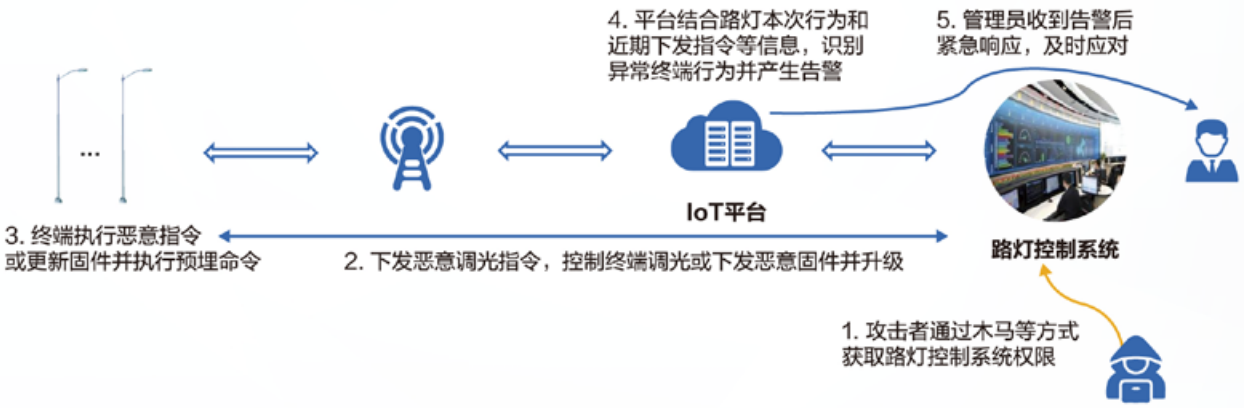
3.4 智能路灯

智能路灯方案为市政路灯照明系统提供定时控制、远程实时控制、单灯故障检测等功能。

路灯作为公共基础设施，与人们的夜间出行安全息息相关。不法分子可以通过控制路灯控制系统或App等手段影响全城或关键街区的夜间照明，造成群众的恐慌，存在安全隐患。而管理员收到电话报障后才能响应，动作滞后。

不法分子通过路灯控制系统下发非法指令或通过恶意软件执行非法操作，其设备行为与正常设备行为会有所不同，IoT平台通过收集设备行为并进行分析，识别其中的异常并告警，使路灯管理团队能够及时响应，减少不良影响。

图9：智能路灯的攻击和防御



3T+1M安全架构在车联网的应用

车联网经过诸多行业组织的数十年发展，在试点项目催化和车联网领域联盟推动下，相关标准逐步完善，技术已经趋于成熟。与此同时，众多国家纷纷投入资金和专家支持。

车联网包含车、路、网和车联云平台等，车联网通过车、路、网和云的协同和智能化技术的应用，提升出行效率并保障人身安全。车联网的组成部分面临着不同的安全威胁：

车联网部件	特点	关键威胁
智能车	多个无线连接访问入口： 蓝牙，wifi，2G/3G/4G/5G，V2X等。	攻击者可以通过多样化无线接入方式进行入侵和控制车辆。
	多个有线物理访问入口： CAN，OBD-2，Ethernet，USB等。	在车辆的维修、维护等过程中，攻击者通过插入带有入侵程序的硬件，或升级带有入侵控制程序的软件包进行入侵和控制车辆。
	车内的电子系统越来越复杂，现代车辆大部分拥有超过100个ECU，这些ECU上运行着超过1亿行代码。	攻击者通过逆向工程等发现可利用的软件漏洞，实施远程控制车辆，比如在车辆运行过程中远程控制车辆进行刹车或转向，对车辆造成极大的安全威胁。
	自动驾驶系统正在被开发和部署在高端智能汽车上，随着科技的发展，部分新开发的中档汽车也具备了L2级的自动驾驶能力。	攻击者实现对部分探测器的诱骗，比如卫星定位信号欺骗，图像欺骗，wifi定位欺骗，雷达信号欺骗等。
	市场上已经存在大量采用无钥匙进入系统的车辆，无钥匙进入系统给车主带来使用上的便利。	通过无钥匙进入系统的漏洞盗取车辆的案例已经屡见不鲜。
智能路	通过网络摄像头，交通显示屏等交通终端以及RSU等V2X业务终端与车辆以及驾驶员进行交互，提升出行效率，降低拥塞。	摄像头等交通终端普遍存在安全漏洞且易被入侵和控制，如设备弱口令问题，权限绕过漏洞，XML注入漏洞等。攻击者利用后可以通过广播虚假消息造成交通混乱。
网络	通信系统作为信息传输的管道，要保证敏感数据不被泄漏，保证数据保密和安全。成熟的通信技术通过采用身份认证、安全通道、数据加密等技术，保护通信数据的安全。	通信系统容易发生数据泄漏，中间人攻击等；通信协议的漏洞是导致攻击的一个重要原因。
车联云平台	车联云平台中存储了大量的车主和车辆数据，比如：用户ID，位置，行驶轨迹等个人信息，这些数据是攻击者的高价值目标。	攻击者通过平台漏洞，或身份认证和鉴权流程缺陷，已经实施过大量的入侵和窃取数据的实例，并成功获取上亿条个人隐私信息。

车联网的安全架构覆盖车联网各个组成部件，构建立在传统的IT安全能力基础上，比如车端的安全启动、安全存储和访问控制等，云端的防火墙、身份认证鉴权、DDoS防御和病毒检测等。同时结合大数据智能分析、车辆入侵检测和防御等新技术。

图10：车联网安全架构

车辆是人们通勤旅游等必备的交通工具，地球的道路上行驶着数亿台汽车，这些车辆的生命周期中，很容易遭受攻击和入侵。及时检测入侵是保证车辆安全的重要措施。入侵检测和防御系统在于对车辆的各个无线和物理攻击入口进行防御；这些入口包括wifi、蓝牙、蜂窝网络、OBD-2、USB、TPM、GPS、Radar等各类对外接口；这些种类繁多的接口，要通过不同的安全技术来检测和防范外部的攻击。同时车内部的各个功能模块间要严格进行隔离，比如，严格禁止通过导航娱乐系统发给车辆控制系统的指令。异常行为需要要进行实时记录，并定期上报到车安全运营中心。

在车安全运营中心，这些从大量车辆上收集的异常数据，将通过智能分析进一步确认是否是真实威胁。对于确认的真实威胁事件，进一步追溯威胁根源，并最终生成应对此类威胁的有效检测和防御规则。将规则通过安全通道下发到各个车辆中，使车辆能够实时检测和防御此类威胁。

仿冒某个实体将对车联网业务造成重大危害，比如仿冒的RSU对车流发送假冒的交通事故消息，可能造成交通混乱。因此，需要建立车、RSU、车联云平台以及通信网络之间的互信。对于车联网业务，要建立独立的身份认证体系以保证业务之间的互信，及时识别仿冒实体。

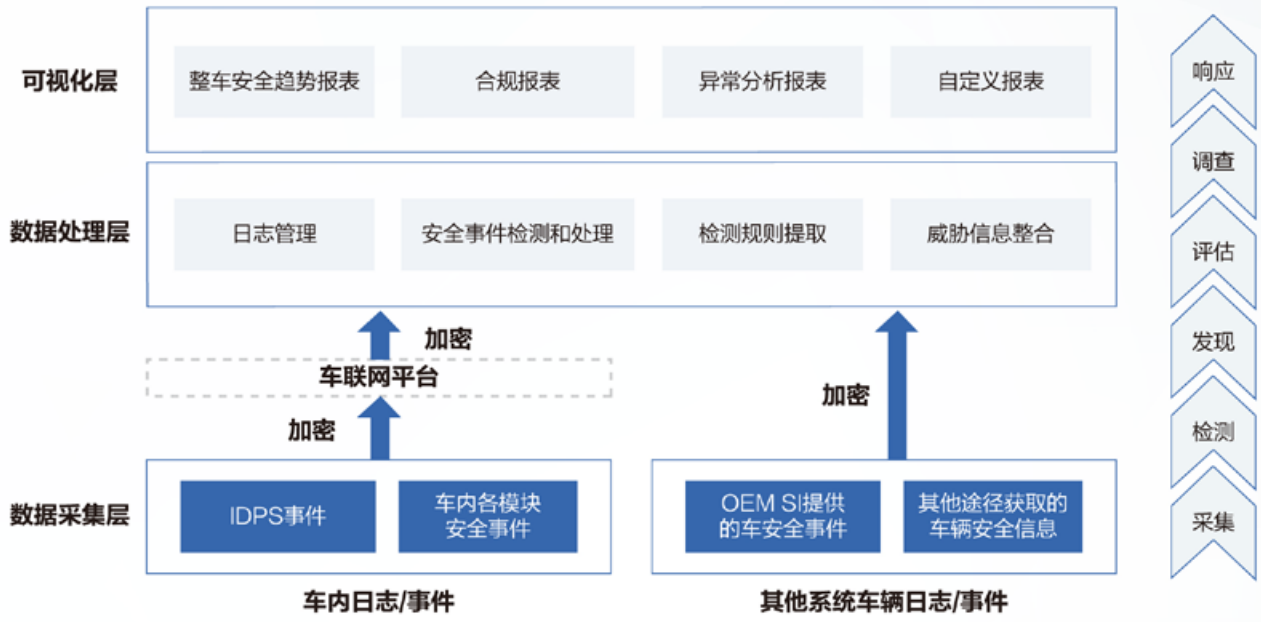
车联云平台上的数据包含大量的用户隐私，任何人都不希望自己的隐私被泄漏。《中华人民共和国个人信息保护法（草案）》已经发布征求意见稿，欧洲的GDPR对隐私保护做了详细的要求。因此，保护车联网数据中的个人隐私，是用户的强烈诉求，也是法律法规的要求。

4.1 联网车辆安全检测分析与感知

车内安全是目前车厂非常关注的问题，主要担心由网络安全引发的人身安全问题或车辆盗窃引发的财产损失问题，因此针对联网的车辆安全防护方案和威胁可视化不可或缺。

车安全运营中心，主要在云端完成联网车辆安全事件采集、分析和可视化。整个系统分为三层：

图11：车安全运营中心



数据采集层：从端侧的联网部件，如车内ECU、Gateway、IVI等部件，采集安全日志和安全事件。在车联网安全运营中心进行统一处理和分析。同时可导入车辆OEM厂商和其他车辆业务服务提供商提供的安全日志和事件进行综合处理。

数据处理层：处理层对采集的安全日志和事件进行分类，生成索引并实现关联分析，自动检测安全事件并生成告警，评估风险的严重性，在Dashboard呈现或邮件通知运营人员。数据处理层判断所上报的安全事件是否真实的安全威胁，对真实的安全威胁进行分析后输出“检测和防御规则”。同时还可根据安全专家的分析结果自定义安全检测和防御规则，持续提升车辆检测和防御威胁的能力。

可视化层：系统提供的分析报表和Dashboard将整个车辆的安全态势向运营人员呈现，协助运营人员快速掌握整体车辆安全状况，例如，被攻击/入侵车辆数，存在安全漏洞的车辆等。运维团队可以根据当前的安全态势，确定安全管理策略，最大限度保障车辆的安全。

运营中心通过挖掘隐藏在海量日志下的安全攻击行为线索，运用ML（机器学习）和AI等技术进行安全大数据分析和异常行为分析，结合第三方威胁信息和汽车网络安全专家的分析，对联网车辆潜在的安全威胁进行监控和预防，保障联网车辆安全运行。同时帮助运营人员实时洞悉联网车辆安全态势，更加主动、智能的完成对复杂、未知、多变的威胁和风险进行持续监控和应对，有效避免因安全问题导致的人身安全和财产损失事件发生。

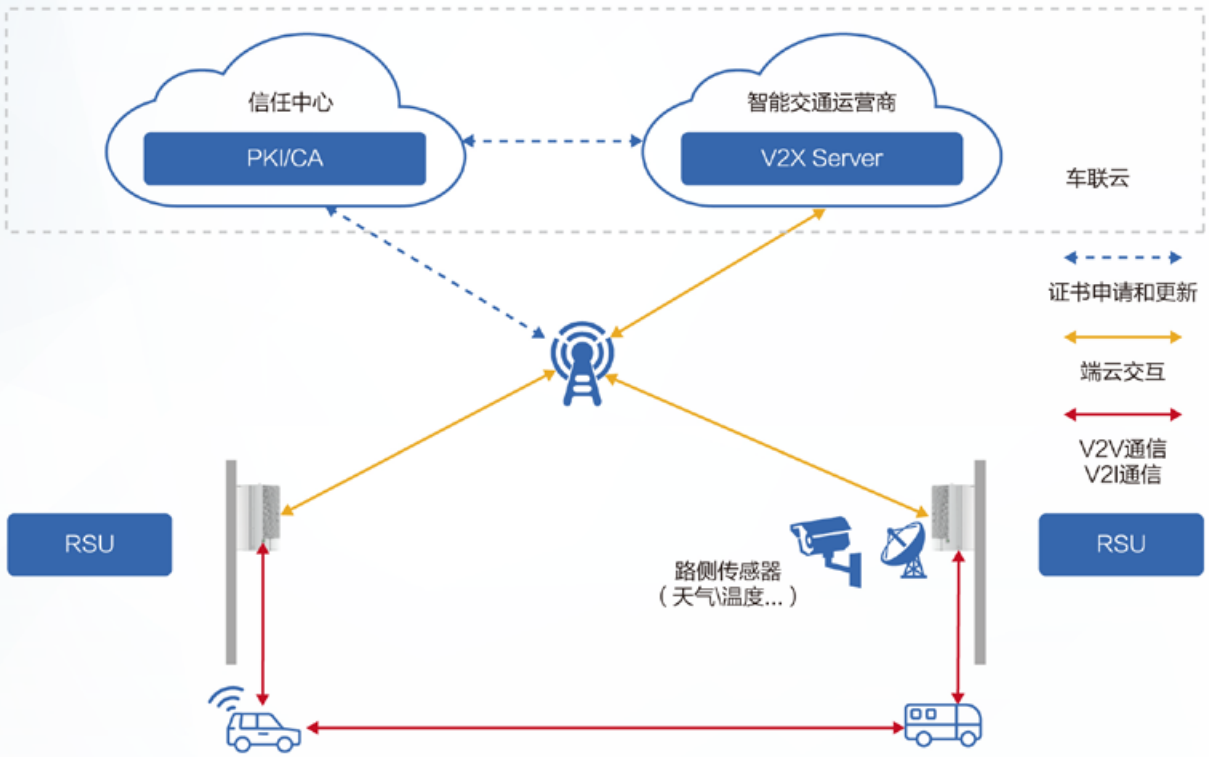
4.2 车路网协同鉴权认证

车联网中的实体被仿冒，将导致车联网提升出行效率的目的大打折扣，可能造成交通堵塞，甚至交通事故。因此，建立车、路、网和云等之间的信任关系，将仿冒实体阻止在业务范围外，是实现车联网业务的基础之一。

一些以车联网为基础的业务，比如车队管理业务要保证车队内部车辆和车队管理平台之间的互信；而共享出行业务要保证共享车辆和共享平台之间的互信。总而言之，不同的车联网业务或应用需要采用不同的信任主体以构建这些业务内部的互信关系，从而防止身份仿冒，并进一步保证数据完整性和来源可靠性。

车路协同业务（即：V2X）的各个实体之间需建立信任关系，以便信任各自发送的消息，识别和阻止仿冒实体。实现车路协同业务的实体包括：车、RSU和V2X平台等。通过CA来建立信任关系时，需要通过一个智能交通运营商授权的信任中心，为各个合法实体发放V2X业务证书，从而建立实体间的信任关系。通过建立这样的信任关系，合法实体发送的V2X业务消息，将包含发送方的签名；当此消息被接收后，能够验证此消息的来源是否合法，以及消息是否被篡改，从而避免仿冒实体发送虚假消息引发的混乱。

图12：车路网协同鉴权认证



网络层作为所有业务共用的信息传递通道，需要识别终端的合法性。目前通常采用运营商的SIM等身份识别技术以保证终端和网络之间身份认证。部分传输敏感数据的业务需要进一步保护，如采用TLS等安全协议。网络层结合身份认证和安全通道技术，保证所传输数据的完整性、保密性以及数据的来源可信。

4.3 车数据安全与隐私保护

车联网业务平台上存储着大量的车主、车辆数据和交通基础设施数据。车主和车辆的数据包括：用户ID，位置，行驶轨迹等，这些数据是攻击者的高价值目标。2017年某企业的某外包人员利用职务之便窃取大量用户出行记录并售卖获利。2016年某互联网平台遭受黑客攻击，五千多万用户和司机个人信息被泄露。这些信息泄露给运营方带来巨大的声誉损失以及用户流失导致的商业损失，甚至法律诉讼。而信息泄露可能会对个人造成更严重的心理和声誉影响，甚至可能危及生命安全。

隐私保护关注点主要问题是：不可关联，透明性和可干预性。隐私技术通过技术手段保护个人隐私，降低管理成本和隐私泄露风险。常用的隐私保护技术包括：数据屏蔽、等价类匿名和差分隐私保护等。数据屏蔽技术是通过掩码、截断、哈希、加噪、置换等方式降低数据的敏感程度，是保护个人数据的基本手段。等价类匿名技术，可以有效防止关联攻击，防止从多个用户属性中关联出用户敏感信息和真实身份。这类技术可以通过对单个用户信息的泛化形成等价类，每个等价类里的用户拥有共同的属性，从而无法使攻击者关联到单个用户，进一步降低了隐私暴露的风险。差分隐私技术通过添加随机噪声方式使攻击者无法学习出单个用户的信息，同时又可以满足对群体数据的统计分析和数据发掘需求。差分算法的隐私保护程度可证明可度量，是目前最强的隐私保护技术。

随着差分隐私保护技术逐步成熟，以及法律法规对个人隐私的严格保护，差分隐私等更加高效的先进技术逐步应用到各种业务上是必然的趋势。车联云平台在保护用户隐私数据时，需要尽量采用先进技术，保障数据收集使用合法合规，降低数据泄露风险。

参考GDPR相关要求，车联网平台隐私保护工作需遵从隐私管理政策，完善隐私组织建设，使用PIA（Privacy Impact Assessments）方法展开隐私风险评估，并落地隐私保护技术等实现个人数据的生命周期管理，同时与第三方合作伙伴紧密协同，防范数据泄露风险。

保障用户的隐私是企业的基本职责，企业在通过技术保护用户隐私的同时，还需要制定完善的管理规定来应对隐私保护诉求。

5 安全共建、价值共享

IoT产业的健康发展离不开安全保障，在很多行业中，安全需求不同，各行业安全方案既不全面也不成熟，在安全风险评估及应对方面尚在探索。物联网安全研究属于新兴的技术领域，整个业界的安全生态建设才刚刚起步。

IoT产业需要通过持续技术创新，同政府、行业伙伴及用户共同探索和应对物联网在不同应用领域的新技术风险，共建物联网安全，共享物联网新技术新应用带来的社会价值、经济价值及个人生活和工作的便利。

图13：IoT安全生态框架

5.1 在标准中定义安全

在技术的发展和演进过程中，标准起到了至关重要的作用，产品和解决方案均须依赖或遵从其适用的标准。在IoT中，标准扮演着越发重要的作用，因为IoT是多类技术的结合，覆盖从底层接入技术到上层跨垂直行业应用。相应地，IoT安全正在逐渐成为各大标准组织的关注热点。整个物联网安全标准处于初始阶段，无论是通用ICT标准组织（比如3GPP、OneM2M、ITU、IETF、IEEE、CCSA等），还是各种垂直行业协会或标准组织（车联网、燃气、水务、路灯、环保等）各标准组织，都在针对IoT安全的各种挑战，积极建议和设计安全技术标准，以满足更智能、全联接的生态系统需求。

目前，许多物联网通用标准和垂直行业标准组织都在推进IoT安全标准。尤其是针对终端安全、NB-IoT网络的安全、物联网分布式安全认证等方面进展明显。以LPWA场景为例，在抄表、停车、消防等采用电池供电，对功耗敏感的场景下，存在传统DTLS无法适用的问题，华为进行创新性的协议优化和改进，推出DTLS+优化方案，使得优化后的方案在功耗上相比传统DTLS方案降低了40%，并在IETF接受成为TLS1.2和TLS1.3标准草案，从而为物联网产业的快速发展提供安全保障。此外在整体安全需求方面的标准制定也在逐步推进，中国联通已经完成了窄带物联网安全需求及框架在ITU的立项，将会为窄带物联网技术的应用提供技术支持和参考。

同时，中国联通等业界主流运营商及设备商也在积极推动车联网、智能制造、燃气、门锁等垂直行业安全标准，促进这些行业领域物联网安全标准的制定。在国内外主流垂直行业物联网标准和联盟组织，比如5GAA、工业互联网联盟、汽标委、建标委等，都发挥了行业领导作用。

5.2 在开放中促进安全

物联网行业伙伴安全能力参差不齐，能力不一，许多物联网垂直行业企业的安全技术有限，防护意识千差万别。因此，行业伙伴间的安全能力开放和共享对整个行业合作伙伴的安全能力提升具有巨大的促进作用。

中国联通和华为从整个IoT产业责任出发，致力于提升整个IoT产业链的安全能力，将自身积累的解决方案安全能力和安全实践经验，通过各种渠道开放共享给物联网垂直行业伙伴。为行业合作伙伴提供物联网解决方案层级的安全设计指导和集成验证服务，并致力于构建开放、安全的物联网生态体系，与各行业合作伙伴共同孵化产业和做大产业规模。

中国联通在物联网网络和业务领域持续发力，已实现物联网全国范围覆盖，同时以平台为核心，对外实现连接管理能力开放，满足多种运营需求、支持“全球连接”，打造端到端整体服务能力。目前中国联通物联网的连接管理平台已经成为全球最大的单一连接的平台，成功接入了近两万行业用户，连接数超过了八千万，每月新增的连接数在300-400万左右。

针对各垂直行业安全特点，设计场景化的解决方案安全能力，华为制定并提供端到端的安全设计技术规范和测试用例，向合作伙伴进行安全赋能并提供认证服务。这对于全面提升合作伙伴的安全能力尤为重要，包括解决方案功能开放、终端和应用安全技术建议书、安全自检列表、系统运维及终端检测工具、运维指导规范，以及一站式的IoT系统安全验证服务。基于云化的IoT平台，通过各类云进行部署，更快的将合作伙伴成果复制到客户现网。通过华为三级认证，促进合作伙伴产品快速成熟。三级认证分别是：针对设备接入（Compatible）和应用互通（Enabled）的两类兼容性认证，以及在兼容性认证基础上，增加行业功能、性能、安全、可靠性、可维护性的更高级别认证（Validated）。

以LPWA场景为例，这些安全能力的开放和共享的典型场景覆盖智慧气表、智能锁、牛联网、烟感、停车、共享单车、水表、跟踪器、邮筒、电表等，并与数十家行业合作伙伴进行解决方案联合创新和端到端的解决方案安全能力构建。

图14：终端安全生态

5.3 在联盟中共筑安全

产业联盟建设是IoT生态的重要组成部分，IoT安全建设离不开整个物联网领域企业、行业协会、研究院所、标准组织、政府监管部门等各利益相关方的通力合作。通过联盟合作，可以重点推动IoT安全的标准规范、最佳实践、政策引导、联合创新、开放实验室等建设。通过行业联盟合作推动IoT安全的发展，是一条行之有效且快捷的途径。

IoT安全联盟建设方式上包括两个方向：一是垂直行业联盟安全合作，成员主要是以IoT行业厂家为主，通过IoT行业联盟，比如工业互联网联盟(AII)、中国智能交通产业联盟（C-ITS）、移动物联网产业联盟（MIoTA）等，推动IoT安全在智能制造、车联网、LPWA移动物联网等领域的应用和标准；二是专门的IoT安全联盟合作，成员主要以专业安全公司为主，通过IoT安全联盟，制定通用类的IoT安全技术白皮书、安全技术框架、最佳安全实践案例等。

中国联通和华为作为IoT行业的领导企业，积极参与到IoT细分领域的联盟安全合作中，推动IoT安全在各个细分领域的最佳实践和标准制定。依托MIoTA移动物联网联盟，与工信部、信通院、泰尔实验室、主要ICT厂家、垂直行业领导企业（燃气、路灯、消防等）合作，制定MIoTA联盟IoT安全技术规范，并在中国江西省打造IoT安全实践案例，比如智慧城市抄表、路灯、停车等的行业应用。

5.4 在合作中增进安全

IoT安全攻防两方处于不平衡的状态。从技术角度看，防护永远落后于攻击，当新的攻击方法、攻击模式出现后，防护方会随之修补漏洞、建设防护网；专业的安全公司是物联网生态圈重要的成员之一，安全公司与通讯服务商一起为行业伙伴提供安全产品和服务，来应对已知、未知的安全威胁，保障客户的数据和业务安全，支撑物联网商用的安全孵化，加速燃气、水务、车联网、工业互联网等行业的数字化转型。

华为积极与业界领先的安全公司、高等院校、研究机构等专业伙伴进行技术方案合作，比如数据安全与隐私保护、恶意终端检测与隔离、终端防攻击能力、大数据安全分析、身份认证等，增强整个IoT行业的解决方案安全能力，同时与专业安全公司或机构进行安全的责任共担，价值共享。

总结

物联网是多类技术的结合，构建开放、合作、共赢的安全生态是产业发展的必然，需要政府、产业界、开发者、学术界、产业标准组织等密切合作，激活商业和科技创新，共同建立合作共赢、公平竞争的产业健康发展生态。我们一直坚信标准是最可信的标尺，创新是最好的防火墙，联盟是最好的防护网，合作是最可靠的密钥。通过技术创新，开展前沿性的IoT安全技术研究，用各个行业的应用需求促进3T+1M安全架构的不断演进，才能持续为客户创造价值。让我们共同积极应对，开放合作，拥抱挑战，共同迈向万物感知、万物互联、万物智能的全新时代。


33.2.55.33
IoT
CONNECTIONS
DISTRIBUTIONS
SEGMENTATIONS
SOCIAL NETWORK

免责声明

本文档可能含有预测信息，包括但不限于有关未来的财务、运营、产品系列、新技术等信息。由于实践中存在很多不确定因素，可能导致实际结果与预测信息有很大的差别。因此，本文档信息仅供参考，不构成任何要约或承诺。中国联通、华为可能不经通知修改上述信息，恕不另行通知。