2016
物联网安全白皮书

2016 IOT SECURITY WHITE PAPER

信息安全与通信保密杂志社
梆梆安全研究院 著

信息安全与通信保密杂志社 出版

2016
物联网安全白皮书

信息安全与通信保密杂志社
梆梆安全研究院
著

信息安全与通信保密杂志社 出版

2016 物联网安全白皮书

著　　者：信息安全与通信保密杂志社　梆梆安全研究院
出版单位：信息安全与通信保密杂志社
地　　址：北京市西城区三里河三区 60 号独栋
邮政编码：100045
网　　址：http://www.cismag.net
电　　话：010-88203306
印　　刷：北京天恒嘉业印刷有限公司
开　　本：710mm x 1000mm　1/16
印　　张：2.25
字　　数：20.5 千字
版　　次：2017 年 2 月第 1 版
印　　次：2017 年 2 月第 1 次印刷
国际标准刊号：ISSN 1009-8054
国内统一刊号：CN 51-1608/TN
邮发代号：62-208

前　言

物联网被人们视为继计算机、互联网之后信息技术产业发展的第三次革命，其泛在化的网络特性使得万物互联正在成为可能。智能家居、车联网、人工智能……这一切的背后正是物联网在加速落地、快速成熟，物联网时代的到来已经毋庸置疑。

物联网是新一代信息技术的高度集成和综合运用，对新一轮产业变革和经济社会绿色、智能、可持续发展具有重要意义，我国已将物联网作为战略性新兴产业的一项重要组成内容。

党和国家高度重视推动物联网的发展，发布了《国务院关于推进物联网有序健康发展的指导意见》《中国制造 2025》《国务院关于积极推进“互联网＋”行动的指导意见》和《关于深化制造业与互联网融合发展的指导意见》等文件，统筹协调和指导物联网产业发展。国家相关部门制定和实施 10 个物联网发展专项行动计划，加强技术研发、标准研制和应用示范等工作，积极组织实施重大应用示范工程，推进示范区和产业基地建设。中央财政连续几年安排物联网发展专项资金，物联网被纳入高新技术企业认定和支持范围。各地区也加大政策支持力度，设立专项资金，多层次、全方位推进地方物联网发展。“十三五”时期，我国经济发展进入新常态，物联网正进入跨界融合、集成创新和规模化发展的新阶段，将迎来重大的发展机遇。

在物联网蓬勃发展的同时，物联网的安全形势也非常严峻。物联网的基础与核心仍然是互联网，它是在互联网基础上的延伸与拓展，而云计算、移动互联网、智能终端等则帮助物联网的体系架构变得愈

发丰富饱满。正是由于物联网络对于互联网的天然继承性，使得针对互联网所发起的各类恶意攻击开始蔓延到物联网领域，物联网安全隐患突出，设施安全、数据安全、个人信息安全等问题亟待解决。《国务院关于推进物联网有序健康发展的指导意见》中指出，我国物联网建设的目标是要实现物联网在经济社会各领域的广泛应用，掌握物联网关键核心技术，基本形成安全可控、具有国际竞争力的物联网产业体系，而物联网的安全保障就是要完善安全等级保护制度，建立健全物联网安全测评、风险评估、安全防范、应急处置等机制，增强物联网基础设施、重大系统、重要信息等的安全保障能力，形成系统安全可用、数据安全可信的物联网应用系统。

本白皮书试图对国内外物联网产业现状和发展趋势进行分析，梳理了物联网面临的安全威胁和挑战，提出了运用物联网方法论建立的物联网安全保障体系，给出了加强物联网“端－管－云”的安全防护的一些建议，展示了典型的物联网安全防御案例。本白皮书的出台，由于时间、投入、视角等诸多方面的局限，难免挂一漏万，却是一次为物联网安全发展提供科学决策依据，促进物联网安全产业发展的积极尝试。

目 录

国内外物联网产业现状和发展趋势

新一代信息技术飞速发展，万物互联时代开启，智能可穿戴设备、智能家电、智能网联汽车、智能机器人等数以万亿计的新设备将接入网络，形成海量数据，应用呈现爆发性增长，物联网在全球范围内呈现加速发展的态势。根据 BI Intelligence 预测，到 2020 年将有 340 亿台设备接入互联网，安装的物联网设备数量将达到 240 亿台，从 2015 年到 2020 年间，总共将有 6 万亿美元投资于物联网解决方案，见图 1。

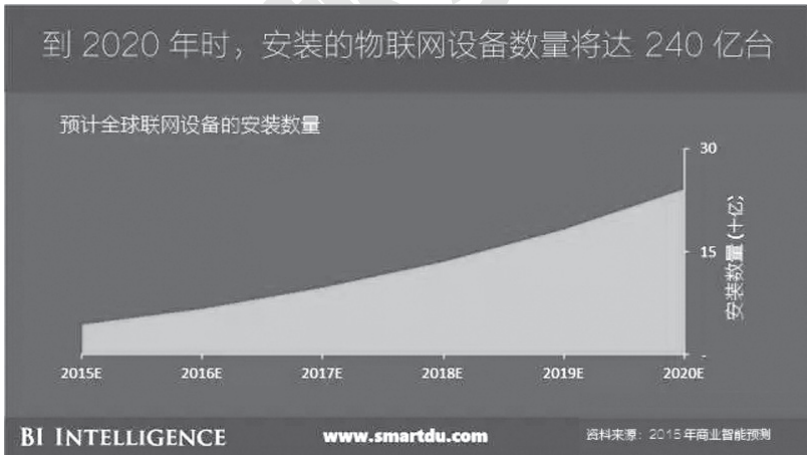

图 1 全球 2015–2020 年安装的物联网设备数量预测

根据 Gartner 预测，到 2020 年全球联网设备数量将达到 260 亿个，物联网与移动互联网融合推动着智慧城市的快速发展， Gartner 预计 2020 年全球智慧城市在医疗健康、公共服务、智能家居、智能交通、

公共事业等领域使用物联网物件数量将高于 60 亿个，见表 1。

表 1 全球智慧城市各领域使用物联网物件估计值（单位：百万件）

类别	2014	2015	2016	2020
医疗健康	2.3	3.4	5.3	32.5
公共服务	57.7	78.6	103.6	260.1
智能商业大楼	283.4	377.3	518.1	2282.2
智能家居	86.2	174.3	339.1	2760.8
交通	215.9	276.9	347.5	723.3
公共事业	217.7	260.6	314	686.6
其他	5.9	8.6	13.3	71.9
总计	**869.1**	**1179.7**	**1640.9**	**6817.4**

Gartner 还指出，专业服务细分市场将为物联网带来最大机会，2017 年物联网服务支出将达到约 2850 亿美元，预计在 2020 年将超过 4820 亿美元。此外，Boston 的数据分析公司在对物联网的一份预测报告中指出，到 2020 年全球工业物联网产值将达 1510 亿美元。

在我国，物联网加速进入“跨界融合、集成创新和规模化发展”的新阶段，与我国新型工业化、城镇化、信息化、农业现代化建设深度交汇，拥有广阔的发展前景。根据工信部数据，十二五末期物联网产业规模已达到 7500 亿元，公众网络机器到机器（M2M）连接数突破 1 亿，占全球总量 31%，预计我国十三五期间，到 2020 年，包含感知制造、网络传输、智能信息服务在内的总体产业规模突破 1.8 万亿元，公众网络 M2M 连接数突破 17 亿，我国 2016–2020 物联网市场规模预测数据见图 2。随着行业标准完善和技术不断进步，在国家政策扶持下，

中国的物联网产业将延续良好的发展势头，将在我国创造出相比于互联网更大的市场空间和产业机遇。

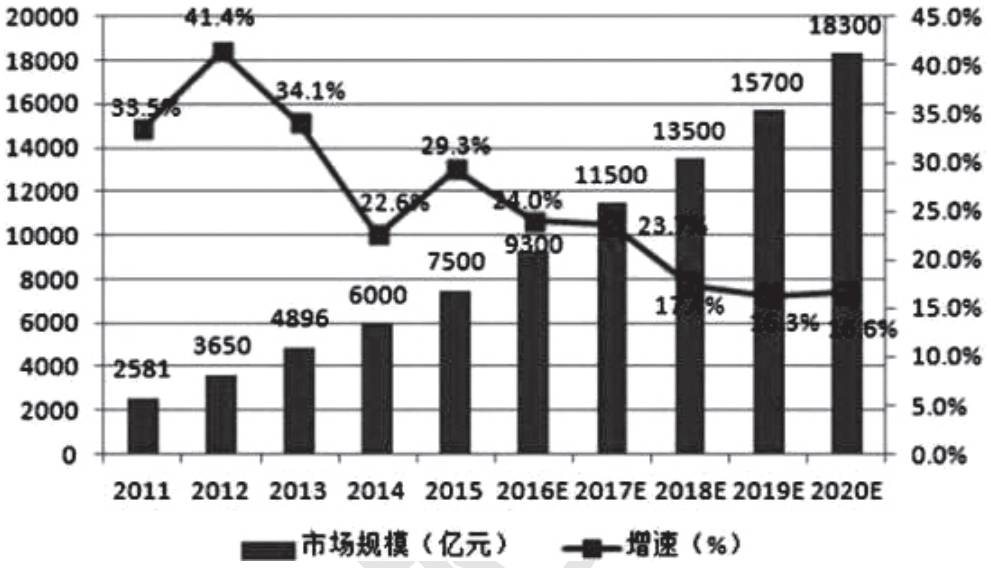

图 2 我国 2016–2020 物联网市场规模预测

面对物联网迎来的重大发展机遇，各国高度重视并纷纷抢占时机进行产业布局。美国、欧盟等发达国家和地区在战略设计、产业生态组织、政策环境建设、大规模应用示范等方面大力推进物联网发展以提升竞争力。我国也非常重视物联网产业规划和布局，以促进物联网规模化应用为主线，以创新为动力，以产业链开放协作为重点，以保障安全为前提，突破关键核心技术，健全标准体系，创新服务模式，构建有国际竞争力的物联网产业生态，为经济增长方式转变、人民生活质量提升及经济社会可持续发展提供有力支撑。

物联网技术是支撑物联网发展的关键，各国企业抓紧掌握核心技术占领产业制高点。第五代移动通信技术（5G）、窄带物联网（NB — IoT）等新技术为万物互联提供了强大的基础设施支撑，随着大数据整体技术体系的基本形成，信息提取、知识表现、机器学习等人工智能

研究方法和应用技术发展迅速，大数据技术在物联网中的应用能够有效释放物联网数据的潜在价值， 云计算的成熟、开源软件等有效降低了企业构建生态的门槛，推动全球范围内水平化物联网平台的兴起和物联网操作系统的进步，以信息物理系统（CPS）为代表的物联网智能信息技术也在制造业智能化、网络化、服务化等转型升级方面发挥重要作用。国际企业利用自身优势加快物联网核心技术和产品研发进行产业链布局，同时，我国的电信、互联网和制造企业也加大力度整合资源，突破核心技术，积极构建产业生态体系。

物联网安全为物联网的健康发展提供前提和保障，各国也将物联网安全提高到战略高度。当前，物联网应用在车联网、健康、家居、智能硬件、可穿戴设备等消费市场需求非常活跃，并且扩展到工业、能源、电力、交通等国家战略性基础行业，相应地安全问题也十分突出。为了应对物联网的安全问题，2016 年 11 月美国国土安全部（DHS）发布《保障物联网安全战略原则》，表示 “保障物联网安全已演变为国土安全问题”，并规定了基本安全措施和对美国市场上的物联网产品的安全要求。2017 年 1 月，美国在线信任联盟也发布了更新的《物联网信任框架》，作为物联网设备开发商、采购商和零售商的产品开发与风险评估指南。我国把网络安全提升到国家战略高度，在物联网安全方面也强调，我国在推动物联网健康有序发展过程中对涉及国家公共安全和基础设施的重要物联网应用，其系统解决方案、核心设备及运营服务必须立足于安全可控。

物联网面临的安全威胁和挑战

物联网有着不可计数的感知终端，有着复杂的信息通讯渠道，有着庞大的数据存储与处理中心。但抽象来看，物联网正是一个十分标准的“终端 – 传输管道 – 云端”架构。

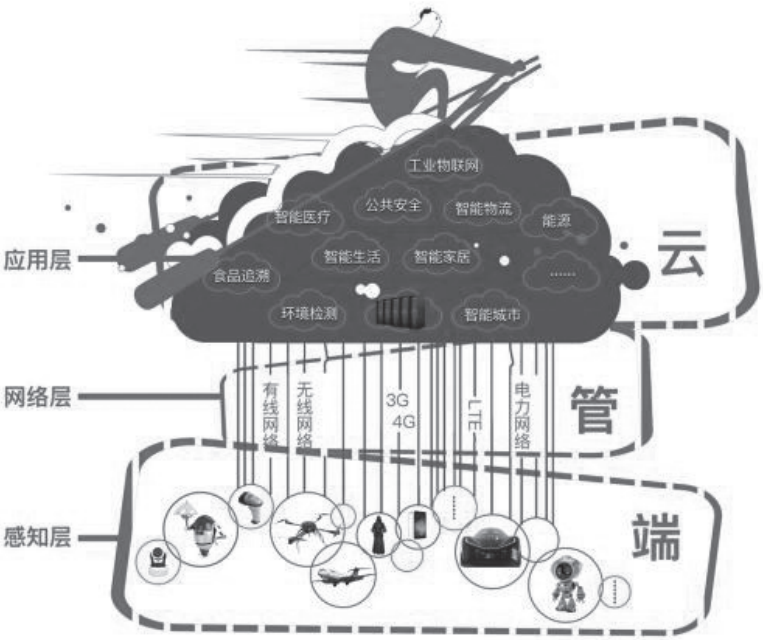

图 3 物联网“端 – 管 – 云”架构

与计算机时代、网络时代相比较，物联网的终端具有移动化、微型化等特征，其传输管道更是在有线网络之外又增加了无线网络，物

联网的云端数据中心不仅更大也更为灵活。物联网“端－管－云”体系架构分别由感知层、网络层和应用层构成，其网络泛在、全面感知、可靠传递、智能处理的特征要素愈发凸显，也使物联网各层面临各种安全威胁：

●物联网感知层安全威胁

物联网的感知层主要进行信息采集、捕获和物体识别，通过传感器、摄像头、识别码、RFID 和实时定位芯片等采集各类标识、物理量及音视频数据，然后通过短距离传输、自组织组网等技术实现数据的初步处理。感知层是实现物联网全面感知的核心能力。目前，针对物联网感知层的攻击越来越多，包括物理攻击、伪造或假冒攻击、信号泄露与干扰、资源耗尽攻击、隐私泄露威胁等。物理攻击即攻击者对传感器等实施物理破坏，使物联网终端无法正常工作，攻击者也可能通过盗窃终端设备并通过破解获取用户敏感信息，或非法更换传感器设备导致数据感知异常，破坏业务正常开展。伪造或假冒攻击是攻击者利用物联网终端的安全漏洞，获得节点的身份和密码信息，假冒身份与其他节点进行通信，进行非法的行为或恶意的攻击，如监听用户信息、发布虚假信息、置换设备、发起 DoS 攻击等。信号泄露与干扰是攻击者对传感网络中传输的数据和信令进行拦截、篡改、伪造、重放，从而获取用户敏感信息或者导致信息传输错误，业务无法正常开展。资源耗尽攻击则是攻击者向物联网终端发送垃圾信息，耗尽终端电量，使其无法继续工作。此外，RFID 标签、二维码等的嵌入，使物联网接入的用户不受控制地被扫描、定位和追踪，极易造成用户个人隐私泄露。

●物联网网络层安全威胁

物联网的网络层主要是将感知层采集的信息通过传感网、移动网

和互联网进行传输，由于物联网中采集的信息需通过各种网络的融合，将信息实时准确地传递出去，其传输距离远，通信范围广，传输途径会经过各种不同的网络，因此面临严重的安全威胁，包括网络安全协议自身的缺陷、拒绝服务攻击、假冒基站攻击、隐私泄露威胁等。网络层功能本身的实现中需要的技术与协议(网络存储、异构网络技术等)存在安全缺陷，特别在异构网络信息交换方面，易受到异步、合谋攻击等。拒绝服务攻击是因为物联网终端数量巨大且防御能力薄弱，攻击者可依靠物联网终端，向网络发起拒绝服务攻击，导致核心网络拥塞。假冒基站攻击即攻击者通过假冒基站骗取终端驻留其上，并通过后续信息交互窃取用户信息。攻击者在攻破物联网网络之间的通信后，窃取用户隐私及敏感信息造成隐私泄露。物联网网络层这些安全威胁可能使网络通信无法正常运行，使网络服务中断，甚至陷于瘫痪状态。

●物联网应用层安全威胁

物联网应用层是对网络传输层的信息进行处理，实现智能化识别、定位、跟踪、监控和管理等实际应用，包括信息处理和提供应用服务两个方面。物联网技术与行业信息化需求相结合，产生广泛的智能化应用，包括智能制造、智慧农业、智能家居、智能电网、智能交通和车联网、智能节能环保、智慧医疗和健康养老等，因此物联网应用层的安全问题主要来自各类新业务及应用的相关业务平台。物联网的各种应用数据分布存储在云计算平台、大数据挖掘与分析平台，并在各业务支撑平台中进行计算和分析，其云端海量数据处理和各类应用服务的提供使得云端易成为攻击目标，容易导致数据泄漏、恶意代码攻击等安全问题；操作系统、平台组件和服务程序自身漏洞和设计缺陷易导致未授权的访问、数据破坏和泄漏；数据结构的复杂性将带来数据处理和融合的安全风险，存在破坏数据融合的攻击、篡改数据的重编程攻击、错乱定位服务的攻击、破坏隐藏位置目标攻击等。此外在

物联网应用层，各类应用业务会涉及大量公民个人隐私、企业业务信息甚至国家安全等诸多方面的数据，存在隐私泄露的风险。

物联网安全需求：物联网是新一代信息技术的高度集成和综合应用，将进入万物互联发展的新阶段。万物互联的泛在接入、高效传输、海量异构信息处理和智能设备控制，对物联网安全提出更高的要求。面对物联网各种安全威胁，物联网安全保障能力亟待提升，需加快建立健全物联网安全保障体系，推进物联网架构安全、异构网络安全、数据安全、个人信息安全等关键技术研发及产业化，构筑物联网智能生态安全，建立健全物联网安全防护制度，建立“早发现、能防御、快恢复”的安全保障机制，确保物联网重要系统安全可控，重要信息安全可控，个人信息保护得到加强。

万物互联时代，物联网安全形势严峻，物联网安全保障能力亟待提升。

物联网安全方法论的提出

传统安全解决方案面对接入网络的新型智能设备以及针对智能设备的新兴恶意攻击缺少有效保护方案与应对策略，因此物联网安全需要考虑特殊的解决方法。要做到安全入微，更要实现统筹安全、度量安全。

每个智能设备都是物联网中的一个微点，会受到各种攻击。这些微点极小又极多，而且脱离了传统安全防御的范畴。考虑到有些微点里可能仅有几 K 字节的运行代码，这就需要对微点的安全防护做到极轻，以轻量级的安全防护保障微点的正常运转。然后通过构造多层次、多样性保护系统，使得微点拥有足够强度的安全防护及抗攻击能力。进而让安全能力泛在化物联网的每个环节、每个角落，从全生态系统、全生命周期维度对物联网体系安全进行考虑与规划，做到物联网安全极大化。最为关键的是要逐步建立起物联网安全度量方法与规范，并据此设立物联网安全基线，由此让繁琐的物联网安全清晰可判断。

在这里尝试首次建立物联网安全方法论：

· 物联网安全要从设计阶段便予以考量，需要深入到代码层面；

· 赋予物联网端点智能安全能力，构建端点智能自组织安全防护循环微生态；

· 构筑极微安全防御体系，以细粒度安全防护叠加方式使得终端的轻量级安全拥有足够强度的抗攻击能力；

· 实现对终端立体防御体系内安全机制的即时动态聚合，运用整

体力量对抗单点式恶意攻击；

· 物联网不仅需要使其安全能力可以实现在自身体系架构内部的全方位覆盖，同时还要延伸泛在化到物联网安全生态的各个维度中；

· 通过安全度量，为各个物联网安全系统设立恰当的安全基线；

· 耦合不同安全运维平台，实现对物联网整体安全的全面管控。

物联网安全保障体系

大力发展物联网技术及其应用，需以安全保障为前提。构建物联网安全保障体系的目的是服务于我国新型工业化、城镇化、信息化、农业现代化建设，增强物联网基础设施、重大系统、重要信息的安全保障能力，强化个人信息安全，构建泛在安全的物联网。物联网安全范围涉及国家安全、关键基础设施、应用服务平台和数据共享服务平台安全，数据安全、行业应用服务安全、公共服务安全、个人敏感信息安全等方面。

物联网安全保障的目标是保证物联网基础网络、重要信息系统的可靠性和安全可控，保证物联网信息资源的保密性、完整性、可用性、合规性，保证物联网智能应用服务正常运行。物联网安全保障的对象是物联网关键信息基础设施、重要信息系统、信息资源以及物联网智能应用服务。物联网安全保障体系需从标准完善、技术保障、管理保障等方面着手，结合国内外物联网安全实践，以物联网的安全风险和安全需求为导向，与物联网信息化建设保持同步，逐步建立完善物联网安全体系，提升物联网安全保障能力。

建立健全物联网安全标准体系，主要是完善物联网安全标准化顶层设计，做好标准路线图规划，加快感知技术和设备安全标准制定、异构网络安全标准制定，加快操作系统、中间件、数据管理与交换、数据分析与挖掘、服务支撑等信息处理安全标准的制定，加快物联网行业应用信息安全共享标准的制定。

物联网安全技术保障主要做好物联网感知层、网络层、应用层的安全防护，需要构建好物联网安全体系架构，使其安全能力全方位覆

盖物联网安全体系架构，并延伸泛在化到物联网的各层。在物联网感知层，重点加强节点和汇聚节点之间以及节点和网络之间的安全认证，加强加密信息的传输，严格进行密钥分配与管理，完善身份认证机制，提高入侵检测的手段，增强物联网端点智能安全能力，构建端点智能自组织安全防护循环微生态，以细粒度安全防护叠加方式使得终端的轻量级安全拥有足够强度的抗攻击能力。在物联网网络层，重点建立完善异构网络统一、兼容、一致的跨网认证机制，完善网络安全协议，加强密钥管理，完善机密性算法，加强数据传输过程的机密性、完整性、可用性的保护。在物联网应用层，重点加强数据库访问控制、不同应用场景的认证机制和加密机制，加强业务控制，确保中间件安全，加强数据溯源能力和网络取证能力，完善网络犯罪取证机制，确保应用安全。

物联网安全管理保障主要是让安全能力泛在化物联网的每个环节、每个角落，从全生态系统、全生命周期维度对物联网体系安全进行规划、组织、实施、评估和改进，做到物联网安全极大化。物联网安全管理规划要从物联网建设阶段就提出系统性的安全设计和规划要求，明确物联网安全建设的目标和重点，抓好设计阶段的安全审查，并深入到代码层面。在物联网建设过程需建立安全实施和运维的组织，并按照安全要求实施管理活动，确保安全活动全过程实施可追溯，安全管理和服务水平可评估。针对物联网安全的管理，应加强对物联网感知层、网络层、应用层等各个层次中硬件设备、控制执行系统、应用程序的运行状况监管，耦合不同安全运维平台，实现对物联网整体安全的全面管控，及时发现安全风险，对安全事件及时响应。此外，还应建立安全管理和服务优化与改进机制，为各个物联网安全系统设立恰当的安全基线，通过安全度量，持续提升运行物联网安全管理和服务能力。

构建泛在安全的物联网，需运用物联网方法论，构建物联网安全保障体系，加强物联网“端－管－云”的安全防护。

化境入微的物联网终端安全

物联网终端设备种类繁多，RFID 芯片、读写扫描器、温度压力传感器、网络摄像头、智能可穿戴设备、无人机、智能空调、智能冰箱、智能汽车……体积从小到大，功能从简单到丰富，状态或联网或断开，唯一的共同之处就是天生都处于白盒攻击环境中。想要通过安装传统安全软件或者架设安全硬件的方式为其提供安全防护能力，明显行不通。

计算机时代，终端面临的最大安全威胁就是各类计算机病毒，防毒卡、杀毒软件等能够提供有效的安全防护。而网络时代，终端所面临的安全威胁剧增起来，木马、间谍软件、劫持攻击、钓鱼邮件、钓鱼网站等。此时除了在终端上安装安全软件外，还需要在网络边界架设防火墙、IDS/IPS，在服务端进行系统加固、邮件过滤等更多的安全防御方法。

物联网时代许多终端的存储能力、计算能力都极为有限，在其上部署安全软件或者高复杂度的加解密算法都会大大增加终端运行负担，甚至导致终端无法正常运行。移动化更使得传统网络边界“消失”，依托于网络边界的安全软、硬件产品都无法正常发挥作用。

而通过对典型物联网攻击案例分析可以发现，物联网时代攻击者主要瞄准的目标依然是物联网终端里的智能设备“大脑”——代码。黑客在掌握了恰当的终端设备硬件平台、操作系统入侵方法后，就会设法对核心代码 IP（算法）进行窃取，尝试破解密钥、加密算法，挖掘控制协议、后台交互逻辑漏洞，发现后台漏洞等。进而实现暴露系

统漏洞、对系统后台进行攻击（协议攻击）、控制系统、劫持/控制设备、获取用户信息/机密数据等操作。

虽然，物联网的移动化特性打破了传统的网络边界，但在每个终端微点之间实际上还是存在着一条新的无形边界——微边界，物联网领域攻防对抗的第一战场就是于微边界处展开。微边界上聚集着数以百万千万计的终端微点，一个感知终端的安全漏洞将会沿着微边界横向纵向扩展，并在物联网上被级数放大，由单个微点所最终导致的安全风险损失不可估量。因此，要将安全泛在化于每个微边界点上，使每个终端微点都具备安全防护及抗攻击能力。安全的部署和运维也要能够适应海量并且多样化、多元化的感知设备。安全威胁的发现、监测与响应更要能够细粒度到每个微边界点上。

综合考虑物联网终端自身特性，以及其所面临恶意威胁的特征，物联网终端安全控制重点需要确保硬件安全、接口安全、操作系统安全、业务应用安全以及用户数据安全等方面：

·硬件安全：硬件安全控制的目标是确保芯片内系统程序、终端参数、安全数据和用户数据不被篡改或非法获取。在硬件安全方面将主要解决物联网终端芯片的安全访问、可信赖的计算环境、加入安全模块的安全芯片以及加密单元的安全等。将身份识别、认证过程“固化”到硬件中，以硬件来生成、存储和管理密钥，并把加密算法、密钥及其他敏感数据存放于安全存储器中，可增强物联网终端的硬件安全防护。

·操作系统安全：操作系统安全控制的目标是实现操作系统对系统资源调用的监控、保护、提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知情情况下某种行为的执行，或者用户不可控的行为的执行，另外，操作系统还要保证自身的升级是受控的。在操作系统安全方面，将主要解决安全调用控制和操作系统的更新来确保操作系统的能力，通过对系统资源调用的监控、保护、提醒，确保涉及安全的系统行为总是在受控的状态下，不会出现用户在不知

情情况下某种行为的执行，或者用户不可控行为的执行。

·接口安全：接口安全控制的目标是确保用户对接口的连接和数据传输可知、可控。在外围接口安全方面，将主要解决包括无线安全接口防护技术、无线外围接口开启 / 关闭受控机制、无线外围接口连接建立的确认机制、无线外围接口连接状态标识、无线外围接口数据传输的受控机制，以及有线外围接口连接建立的确认机制。

·业务应用安全：业务应用安全控制的目标是保证终端对要安装在其上的应用软件进行来源识别，对已经安装在其上的应用软件进行敏感行为的控制，还要确保预置在终端中的应用软件无恶意吸费行为，无未经授权的修改、删除、窃取用户数据的行为。在应用软件安全方面，主要解决应用软件认证签名机制和敏感 API 管控技术。

·用户数据保护安全：用户数据保护安全控制的目标是保证用户数据的安全存储，确保用户数据不被非法访问、不被非法获取、不被非法篡改，同时能够通过备份保证用户数据的可靠恢复。在用户数据安全方面，将主要解决包括移动智能终端的密码保护、文件类用户数据的授权访问、用户数据的加密存储、用户数据的彻底删除、用户数据的远程保护。

综上，物联网终端的安全体系架构包括三大层面：硬件层、操作系统层和应用软件层。安全架构首先是保证安全的硬件，打造硬件级的可信平台，作为设备安全的基础，通过安全的硬件绑定安全的操作系统，提供容器隔离和安全增强的方案，安全的操作系统绑定安全的应用软件，打造增强应用安全解决方案，这样层层绑定确保可信的数据处理和智能服务的提供。物联网终端安全体系也将与云计算安全体系、大数据安全和隐私保护安全体系结合，采用终端输入验证 / 过滤技术、实时安全监控技术、安全数据融合技术、全同态加密技术、隐私保护技术，对敏感数据进行身份识别与访问控制，在关键技术上使物联网拥有足够的安全防护能力。

多重隔离的物联网通信安全

数据通信传输也是物联网体系里十分重要的一环，现在越来越多的黑客开始瞄准通信传输协议下手进行破解攻击，加强数据通信传输管道的安全性已经迫在眉睫。

意大利 Sapienza 大学的 C.M. Medaglia 和 A. Serbanati 在其所发表的论文 *An overview of privacy and security issues in the internet of things* 中曾指出，物联网终端在与云端进行信息通信互动传输过程中，容易遭受流量分析、窃取、嗅探等网络攻击，进而导致传输信息数据遭遇泄露、劫持、被篡改（干扰）、屏蔽等威胁。

物联网数据传输所使用的网络包含有线网络、无线网络、3G、4G、LTE、电力载波等多种异构网络，其所面临的安全问题也很复杂。算法破解、协议破解、中间人攻击等诸多攻击方式正在逐渐侵蚀物联网体系，Key、协议、核心算法、证书等破解情况的发生，将会导致核心业务逻辑和重要接口暴露，甚至还有更多不可预知的物联网系统性安全风险。但抽象来看，物联网数据通信传输的安全问题需要重点关注传输管道自身与传输流量内容这两方面。

正如前文所提，已经有黑客通过分析、破解智能平衡车、无人机等物联网设备的通信传输协议，实现了对物联网终端设备的入侵、劫持。网络通信协议自身的安全性向来都不是很强，某些设备所采用的自定义网络通信协议的安全性则更为堪忧。而在一些特殊物联网环境里，网络通信过程中所传输的信息数据仅采用很简单的加密办法，甚至没有采用任何安全加密手段，直接对信息进行明文传输。黑客只要破解

通信传输协议，就可以直接读取其中所传输的数据信息，并任意进行篡改、屏蔽等操作。

对于物联网的通信安全，首先需要加强网络通信协议自身的安全防护。考虑到通信协议本身就是由一行行代码所组成，针对代码部分的安全防护方法可以直接移植过来。也就是说，可以对通信协议实施加密操作，采用多层密钥加密传输，密钥之间动态切换，提供更加安全的保证。通过白盒加密技术再对加密密钥进行安全性保护，防止密钥的泄漏和破解。对通信协议代码实施高强度混淆，彻底“打乱”旧有程序逻辑思路，极大增加黑客分析、破解、调试、Hook、Dump 通信协议的难度，甚至在超过破解性价比临界值时迫使黑客放弃入侵攻击。

其次，要对数据通信传输管道里的数据流进行加密操作，杜绝明文传输。还要对流量里的数据进行安全过滤、安全认证，确保让正确的数据在通信传输管道里流通。对设备指纹、时间戳信息、身份验证、消息完整性等多种维度的安全性校验，可以进一步保证数据传输的唯一性和安全性。另外要注意，在特殊物联网传输环境下，要考虑进行网络加速操作，避免数据通信传输管道成为物联网体系正常运转的瓶颈。

第三，要加强通信管道安全防护软硬件的研发，重点放在高性能信道与网络密码设备、密码网关、安全 Web 网关、安全路由及交换设备、高性能网络隔离与交换系统、网络行为监控系统、统一威胁管理平台等方面。

物联融合的未来安全云平台

物联网是一个规模庞大的信息计算系统，这个系统需要一个强有力的平台提供计算和存储服务来支撑其应用需求，云平台能够对物联网终端所收集的数据信息进行综合、整理、分析、反馈等操作。

物联网中的应用都是数据密集型的，传感设备与云平台之间、用户与云平台之间和用户与传感设备之间时刻都在进行数据交互，一旦数据丢失和损坏都将造成难以预料的后果。如果说物联网终端相当于人的手脚、眼鼻口，网络通信传输管道相当于人的四肢躯干，那么云端就等同于人的大脑，其安全重要性可见一斑。物联网云端保存着所有终端搜集上来的信息数据，以及据此分析获得的新数据信息。这些信息就犹如存放在仓库里的黄金珠宝，时刻诱惑着黑客发起攻击。云端一个小小的业务逻辑漏洞，就可能会给黑客攻击大开方便之门。因此，云平台必须采取适当的安全策略来保证物联网中数据的完整性、保密性和不可抵赖性。云平台安全包括云存储安全、云计算安全、云应用安全。

云存储安全的主要目的是保证数据存储的完整性和保密性，常采用的安全机制包括数据隔离与交换、数据备份、数据检错纠错、文件系统安全性、访问控制和身份鉴别等。云存储安全通过数据隔离与交换、冗余备份数据，将数据存放在不同的数据中心，以保证个别存储设备的故障不影响整个存储系统的可用性；通过采用检错和纠错技术使系统迅速发现错误并找寻备份数据来完成数据存取访问，保证数据的正确读写；通过文件系统加密实现存储系统安全；通过访问控制和身份

鉴别技术有效地控制用户对存储资源的访问，将用户对存储系统的访问限制在一定的范围内，从而保证其他用户数据的安全性，防止越界访问。

云计算安全主要是保证云平台数据计算与运行环境的安全，特别是基于虚拟化技术的云计算安全。重点应考虑虚拟化软件和虚拟服务器安全，虚拟化软件安全是保证客户虚拟机在多租户环境下相互隔离的重要层次，必须严格限制任何未经授权的用户访问虚拟化软件层，限制对于 Hypervisor 和其他形式的虚拟化层次的物理和逻辑访问控制。虚拟化层的完整性和可用性对于保证云平台的完整性和可用性是最重要，也是最关键的。一个有漏洞的虚拟化软件会暴露所有的业务域给恶意的入侵者。虚拟服务器位于虚拟化软件之上，对于物理服务器的安全原理与实践也可以被运用到虚拟服务器上，同时需要兼顾虚拟服务器的特点，包括选择具有 TPM 安全模块的物理服务器、使用支持虚拟技术的 CPU、安装虚拟服务器时分配独立的硬盘分区、使用 VLAN 和不同的 IP 网段、在防火墙中为虚拟服务器做相应的安全设置等，以对它们进行保护和隔离，并与其他安全防范措施一起构成多层次防范体系。

云应用安全主要是面向用户提供一些安全手段来保证用户数据在传输、交换和使用过程中的安全性，防止用户数据被非法访问和泄露，常采用的安全机制包括存储加密、交换加密、身份认证与访问控制、接口安全和个人信息安全保护等。存储加密是在访问云入口时对数据进行加密，以保障传输和存储的安全性；交换加密是采用数字信封等技术手段，保证用户数据在交互过程中的安全性；身份认证与访问控制机制是允许授权用户在自己的权限范围内进行数据操作，从而防止非法用户对数据的访问；接口安全是根据物联网的应用需求不同而提供不同的应用接口，采用多接口模式和加密技术等通过接口安全保证应用程序对存储资源的安全访问；个人信息安全保护是采用数据自我销毁技术等建立在云服务器端对用户数据从创建到销毁全过程的隐私

保护机制。

针对云平台的安全产品、安全方案很多，也在逐渐成熟，不过对于物联网云平台而言，还需要更注重移动安全这个维度的安全防御，例如需要移动威胁感知平台来完善云平台安全情报体系，通过 SOC、M-SOC（Security Operation Center for Mobile）实现对物联网安全体系的整体管控，通过移动安全测评云平台实现对物联网云端应用、源码、服务器安全性的实时检验与监测。

SOC 并非一个新的概念，但在物联网时代，面对复杂的物联网安全体系，SOC 的作用在变得愈加凸显。SOC 作为安全体系的一个集中单元，会在整个组织和技术的高度处理各类安全问题。SOC 能够将安全防御孤岛连接起来，从安全情报、安全产品、安全运维到安全服务，SOC 可以使之不再割裂，提高整体安全防御效率，降低安全防御成本。SOC 由于自身特点，使其所处位置只能是在云端层面：其或会依托于云计算平台，作为云平台内部的一个模块组件，或者单独以安全管理云平台的形式并列于云端之侧。

物联网与业务之间的结合达到了一个前所未有的高度，那么在物联网安全体系里，SOC 将以业务为导向驱动，量化安全、展示安全、控制安全，实现安全管理技术化。通过 SOC 可以对物联网云端、终端、传输端进行逻辑层、物理层等多层面的安全检测，及时解决所发现的安全隐患，力争将危机消灭于萌芽之中。而借助 SOC 还能够洞悉物联网整体系统的安全态势，即时制定新安全防御策略，实施有效的安全防护动作，并实现对全网传统与新兴安全能力的整合，避免安全防护一盘散沙局面的出现。而 M-SOC 则能在物联网移动维度实现全生命周期的安全防护，有力补足了物联网安全体系可能出现的安全防护遗漏。

英国 Newcastle 大学的 Leusse 在其论文 *Self managed security cell, a security model for the Internet of Things and Services* 里提出了一种面向服务思想的安全架构，利用 Identity Brokerage、Usage&Access Management、SOA（Service-Oriented Architecture）Security Analysis、

SOA Security Autonomics 等模块来构建具有自组织能力的安全物联网模型。

物联网的安全触角实在太为广阔，覆盖了众多领域维度。从大的方面考虑，需要各 SOC 能够实现耦合，进行安全防御联动，共享安全情报信息，整体把控物联网安全。往小的层面看，由微边界联合起来的众多物联网终端微点，要能够逐步实现矩阵化，从松散的个体成为组织化、智能自适应化的严谨统一整体。以集体的力量有效对抗有组织的恶意攻击。

在物联网时代，不同行业的云平台之间势必将互相连通起来，物联网可以说就是各类云平台的整合。而在云平台整合的背后，则联动着不同行业、不同领域物联网安全管控平台的整合，物联网安全体系内部各个环节的整合，物联网微观环境里各个单元、模组的整合。只有将一切松散元素锻造成严密的统一整体，才能将物联网安全清晰地呈现在人们面前。

如何度量安全？在物联网时代里，或将做到这一点。

加上全生态环境安全协同，可让物联网安全变得高度可控！

协同一致的物联网安全生态

面对复杂多变的物联网体系，需要构筑足以将其完全容纳的物联网安全生态环境，这意味着，既需要“端－管－云”安全防御体系，还需要构建“大安全”生态系统。目前，我国物联网安全产业链正处于发展阶段，包括安全相关芯片、元器件、硬件设备制造、网络通信、软件和信息服务、系统集成、运营服务等方面，物联网安全产业发展面临的瓶颈和深层次问题依然突出：一是物联网安全标准有待完善，重要标准研制进度较慢，跨行业应用安全标准制定难度大；二是物联网安全产业生态竞争力不强，芯片、操作系统、安全云平台等核心基础能力依然薄弱，三是产业链上下游资源需协同发展，与物联网相关的云安全、大数据安全、个人信息安全等问题亟待解决。

物联网体系自身的特点决定了物联网安全必然会受到来自上下游相关生态环境的影响。某国际著名企业所遭受的恶意攻击，就是由一封从合作伙伴处发来的电子邮件所导致。在苹果 Xcode Ghost 病毒事件里，Xcode 是由苹果制作的开发 Mac OS 和 iOS 应用程序最快捷、普遍的开发工具，恶意攻击者在 Xcode 中植入了恶意代码，当应用开发者下载并使用被感染的 Xcode 开发程序时，恶意代码就会污染开发者端程序。这会使得即便未越狱的 iOS 用户从苹果官方 App Store 下载应用时也将面临各类安全威胁风险。

木桶定律对于物联网安全生态有着极为深刻的影响，最短的那块“安全防御木板”将不仅会降低物联网安全整体防御度，甚至可能引发严重的负面影响，导致一个或数个相关体系被恶意攻击所摧垮。在

物联网时代下，哪怕一个普通人也需要作为一个安全防护单元，使得以该普通人为主导的物联网生态体系也能够拥有足够的安全防护能力。

同时还要注意，虽然传统安全防护产品已经无法有效应对新型恶意攻击，但并不意味着在物联网安全体系里就不再需要传统安全防护产品。恰恰相反，在物联网的网络层等维度中，传统安全防护产品依然起着不可或缺的作用。在物联网的安全生态环境里，一条坚固的传统安全防线极为重要。

物联网成为互联网之后又一个产业竞争制高点，未来我国需在物联网安全产业生态构建方面从整机设备、核心芯片、操作系统、安全运营服务等板块入手加快产业链布局，构建基础设施泛在安全，让具有自主知识产权的操作系统与安全云平台一体化成为掌控生态主导权的重要手段，服务于智能制造、智能交通与车联网、智能家居、智能医疗、智能环保等重点领域。物联网安全产业生态的各环节需加强产业链上下游协同创新，将移动互联网安全、云安全和大数据安全融合创新到物联网安全产业生态体系中，推进产业转型升级，提升我国物联网安全产业的核心竞争力。

可视可度量的物联网安全管理

人们一直希望能够度量世间万物，但对某些事物却始终无法找到有效的度量方法，安全就包括其中。

在计算机时代，人们可以统计系统被感染了多少病毒，但却无法准确衡量病毒对系统造成了多大的损坏。近几年人们所热议的安全可视化，其背后也是在探寻可以对安全进行衡量的方法。人们希望能够看到“不可见的安全”，人们更希望能够对安全体系的强壮程度进行丈量。人们需要更为明确地知晓自己所构建的安全防线是合格、优秀还是满分，或者是处于不及格之下，需要对其中部分环节进行提升。

物联网世界里的安全更需要做到可度量，并据此找寻、设立适用于各领域的安全基线，二者相结合精准掌控物联网安全。

实际上，随着安全防护能力的细微化，度量安全的方法也在逐渐清晰起来。以移动应用安全为例，移动应用自身的源代码、库文件、密钥、软键盘、启动界面、交互短信、通信协议等都是其主要的防护节点。那么最为简单的移动应用安全度量就可以是：依据各个节点是否实施了安全防护、采用了怎样强度的安全防护技术进行评分，综合得出安全防御度分数。进而根据不同行业、不同业务对于防御节点数量及强度需求的不同，设立各自的安全基线。金融行业对于安全性要求很高，那么可能其安全基线分数要达到 90 分以上才算及格，超过 120 分才算优良。

对于物联网安全的度量，可从物联网安全的检测能力、防护能力、预警能力和响应能力方面评价物联网安全性能和有效性。在对物联网

安全检测能力方面，度量尺度可用置信度来衡量，置信度由查全率、查准率、碎片率、错误关联率等尺度组成，在物联网复杂的网络环境中，需要具备检测、挖掘、分析各种恶意攻击轨迹的能力，以有效地感知物联网的安全态势。一般攻击轨迹可分为已知攻击轨迹、检测到的攻击轨迹和正确检测到的攻击轨迹，没有被检测到的已知攻击轨迹是漏警，而不存在但却检测出的攻击轨迹则是虚警，提高查全率和查准率可提高物联网安全检测能力。在物联网安全防护能力方面，度量尺度可以用不一致率指标来衡量，其主要衡量所采取安全防护措施的质量情况，即正确使用安全防护措施的程度如何，也表明安全防护措施存在错误的关联或联系。在物联网安全预警能力方面，度量尺度可以用告警率来衡量，其主要衡量正确告警的情况，正确告警的次数占总核实告警次数的比率越高物联网安全预警能力越强。在物联网安全响应能力方面，度量尺度可用响应时间来衡量，其主要衡量从发现安全问题到做出决策或采取行动之前所花费的时间，其既是性能衡量标准，又是有效性的衡量标准，提高响应时间，继而可提高物联网安全响应能力。物联网安全有效性的度量尺度可以用满意度来衡量，其主要衡量决策者对所重点关注的物联网领域所采取安全措施的满意程度，满意度越高物联网安全的有效性越好。物联网安全性能和有效性的衡量不能依靠单个尺度，需要各衡量尺度的组合，才能充分评价物联网安全的性能和有效性。

网络摄像头很小，却能瞬间让数亿人“下线”断网；

老司机控制下的智能汽车，竟然还会突然“发疯”到处乱撞；

温馨的智能家庭，虚拟空间中的“窃贼”早已悄然潜入。

这是物联网世界里已经或者正在发生的真实事件！这一切都是黑客以及恶意攻击者们捣的鬼！

好消息是，安全研究人员已经想到了一些解决方法，供您参考。

典型物联网环境安全防御

● 网络摄像头背后的物联网安全危机

今年所发生的大规模物联网 DDoS 测试攻击，导致美国东部互联网全部“下线”。而其罪魁祸首之一竟然是国内某安防视频产品方案和技术提供商所生产的摄像模组，该摄像模组被许多网络摄像头、DVR 厂家采用，并于美国大量销售。该公司部分早期摄像模组产品的密码被写入到固件里，且很难进行修改。黑客发现了这一可乘之机，通过默认密码打开了大门，控制其成为物联网 DDoS 攻击的肉鸡。如此不经意的一个问题，竟然就让小小的网络摄像头发挥出如此“巨大的作用”！

由此可见，物联网繁多的各类终端里一个不起眼的小毛病一旦被黑客挖掘出来，加、乘上终端设备庞大的个体数量，所爆发出来的破坏力不容小觑。

而在安全研究人员的眼里，物联网终端安全防护的办法其实有很多。举例来说，对于可穿戴智能设备安全防护的关键节点包括（不限于）：防止对其内部程序代码的静态分析与运行时的动态调试；加密敏感存储数据，在运行时解密；保护可穿戴设备 SDK，避免拦截、篡改数据；加固应用程序，拒绝未经授权的更改；防止逆向工程、窃取知识产权，避免盗版侵权；实现一机一密，并利用白盒技术深度保护密码等。

● **智能网联车不可变成“智能撞翻车”**

自从特斯拉惊艳亮相之后，人们才发现原来汽车的世界还可以是这样，原来科幻电影里炫酷的未来交通工具也能够来到我们的身边。而其中最为兴奋的竟然是网络安全世界里的黑客们，各种花样玩转特斯拉。

但从智能网联车自身角度看安全能够发现，T-BOX、IVI、OBD、USB、充电接口、GPS、摄像头等更多的攻击入口，动力系统、转向系统、制动系统、车身控制系统、仪表盘等更多的被攻击点越来越多地暴露在人们视野里。智能汽车与外部的每个接口都可能被利用，每个控制单元都可能被攻击。

再从智能网联车的生态环境来看，与智能汽车有信息交互的外部组件如果被入侵，都可能引发智能汽车的信息安全事件、交通安全事故。例如智能汽车的充电桩、行车记录、智能标示牌等一旦被恶意攻击，“无人驾驶”失控将更为“频繁”。

无需认证、明文传输、通信流程伪造……智能网联车的生态环境中面临的潜在安全风险几乎无处不在。现实生活中，已经有厂商因为各类信息安全问题，开始召回存在安全隐患的智能汽车。

车联网是物联网的重要分支，作为车联网核心要素之一的智能汽车所暴露出来的安全问题，将直接影响到人们的生命安全。那么对于智能网联车的安全防御要能够做到：

· 从内到外：从车内部到整个外部生态环境安全；

· 从小到大：从芯片安全到云安全，对应各点提供保护；

· 从始到终：从安全设计到安全运营。

也就是要实现，从车内到外部的生态环境、从微小的芯片到云端平台、从智能汽车诞生之前到其生命的终结，全维度、全生命周期的安全能力覆盖。

对于智能网联车的安全防御可以参考如下原则：

· 架构全面性：采用端管云安全架构体系，考虑整个生态的

安全需求；

· 方案综合性：层次化、多样性的特点将更为突出，应根据风险分析合理实施纵深防护方案，部署适合的安全防护产品；

· 技术创新性：随着智能化、网联化与电动化的进一步发展，会出现更多新的攻击手段，需要超越原有理念，采纳新技术防护。

● 家庭里的那朵安全智能云

现在许多人的手上会有三部移动设备：智能手机、智能手表（智能手环）、平板电脑。而当人们回到家里后，需要联网的智能设备会增加为智能门锁、智能电视、智能空调、智能冰箱、智能洗衣机等。

物联网另外一个重要分支——智能家庭网络的雏形开始显露出来。

然而，绝大部分智能家居产品在设计、生产过程中都没有将安全性考虑进去，黑客对于智能家居产品的破解几乎是手到擒来。去年就频繁爆出各类智能家居产品存在安全漏洞、安全隐患，某国外品牌智能电视会将语音搜索功能产生的信息数据直接明文发送到网络，黑客通过网络嗅探就可以窃取到这些没有进行加密的用户信息。

那么对于智能家庭网络里的各类终端——智能家电的安全防护，要注意防止绕过、屏蔽身份认证机制；要防止通过互联网对智能家电进行侵入式的恶意控制；还需要对智能家电的控制应用 App 进行加壳保护，增强 App 安全度，避免其成为整体防御架构中的薄弱节点。

扩展到智能家庭网络，其安全防御策略要能够阻止未经授权对智能家居设备的开启、关闭等控制，要阻止智能家居设备控制电子密钥的非授权发送。更为深入则可以考虑通过白盒密码技术对存储在本地的电子密钥 / 证书进行保护，并保护通信协议及数据，防止针对性的音频、视频等信息数据被窃取。

结 束 语

对于国内物联网现状来说，技术创新不断，软硬件产品层出不穷，但却和安全关联不大。设计思路的狭隘、品牌利益为王的标杆、用户安全意识教育缺失、行业标准和选检尺度的不明朗均会造成日后安全大事件的发生，前方已经兵临城下。

然而无论物联网如何变化，“终端－传输管道－云端”这一本质架构形式将成为主要形式之一。所以，对于物联网的安全防御动作要紧扣其架构本质，保护好智能终端、通信数据、云服务器等环节，并将安全能力细微化、极大化、整体化，借助安全度量与安全基线，清晰物联网安全的整个体系，将安全效能最大化。

提出物联网安全方法论思考

探索物联网环境安全策略

揭露物联网安全本质

让安全可视可度量

信息安全 通信保密

Information Security and Communications Privacy

梆梆安全 BANGCLE

ISSN 1009-8054

02>

9 771009 805170