2015 年 4 月

IBM 观点：物联网安全

“事物”的互联为企业开展创新、寻找商机营造了一个活跃的环境，但同时也带来了一系列的安全威胁和挑战。

IBM

引言

本文将全面介绍 IBM® 对物联网 (IoT) 安全和隐私的观点。在 2014 年 11 月发布的一份报告中，分析师预计，到 2020 年，物联网中的互联事物将达到 300 亿，而在 2013 年，这一数字还只有 990 万。[1] 如今，在企业和机构的运营以及我们的生活中，充斥着各种各样的事物和设备，比如恒温器、医疗设备、汽车和工业设备。这些事物之间的互联无处不在，为企业开展创新、寻找新的商机营造了一个活跃的环境。但是，这种逐渐膨胀的计算环境也带来了一系列的安全威胁和挑战。在这个万物互联的世界里，企业生成和使用的数据、为这些数据提供支持的系统和应用都已成为潜在恶意攻击的目标。潜在的攻击行为包括：获取隐私或机密数据；操纵或控制设备；或者当应用在物联网系统中使用和提供数据时，以错误方式服务或拒绝服务这些应用。

制造行业、能源行业、运输行业和经济体中的其他工业行业也在使用物联网系统，这些工业物联网系统面临的风险甚至更大。为了获得更广泛的洞察力和控制力，并开展基于条件的维护，工业事物开始联网，这使得它们非常容易受到安全攻击。一些发布的报告就曾经披露过监测控制和数据采集 (SCADA) 系统与工业控制系统 (ICS) 遭受了攻击。"在研究了网上公开的 60000 多个控制系统后，两名俄罗斯安全研究员找到了一些漏洞，通过这些漏洞，他们可以全面控制能源系统、化工系统和运输系统。"[2]

一个物联网系统中的设备（事物）会与其他设备、应用和服务进行通信，而这些设备、应用和服务使用的是各种各样的协议，并且会公开应用编程接口 (API)，以便访问互联网上的数据和服务。物联网系统中既有基本的单一传感器，也有更强大、更成熟的处理节点，前者直接联网或者通过某种简单的网关联网，后者则能自动进行处理。例如，一台互联汽车就是一台由不同的电子操纵子系统和传感器组成的复杂设备，这些子系统和传感器不仅能够自动进行处理，还能通过无线连接网络。

每个被保护的系统面临的风险状况都不同，因此它们对物联网安全的要求也不同。一个消费者 IoT 系统和一个复杂的任务关键型企业 IoT 系统，前者是用来评估和控制园林植物供水系统，后者是用于石油钻井或管线作业，其中包含与 IoT 互联的阀门和水泵，这两个系统的安全需求肯定截然不同。钻井和管线作业 IoT 系统中必须有安全关键型系统，才能保护企业、环境和人身安全。同样是忽视安全因素，钻井作业系统所面临的风险和付出的代价要远远高于家用花园供水系统。因此，对于这类系统，全面的安全措施、专业知识、分析、测试和管理必不可少。如果企业构建的 IoT 系统面临着极高的安全风险和复杂性，那么他们必须邀请经验丰富的主题专家来为系统的设计和操作提供指导。物联网安全性是一个热门话题，有许多企业和代表发表了他们的真知灼见。IBM 在 2014 年 6 月发布的一篇 IBV 研究[3] 报告中首次提到了安全性和物联网。其他实体也围绕这一话题发布了许多信息和观点，其中就包括开放式 Web 应用程序安全项目组织（OWASP，Open Web Application Security Project）[4] 近日发布的一篇文章。此外还有一些联盟组织也在研究物联网与安全性，比如工业互联网联盟 (IIC)[5]、Allseen Alliance[6] 和 builditsecure.ly[7]。

我们在考虑物联网系统（或任何一个 IT 环境）的安全性时，需要慎重考虑一个因素：物联网系统无法依靠每个互联设备的持续完整性，来确保整个系统的持续完整性。物联网系统的设计方案和安全功能都是建立在以下假设的基础上：某个设备的安全性可能会受到威胁（没有万无一失的安全措施），但是即使有几个设备受到威胁，整个系统仍然能安全地运转。

物联网系统架构

物联网系统有很多种配置方式。在有些物联网系统中，所有设备都是直接联网，每个设备负责其本地的安全。

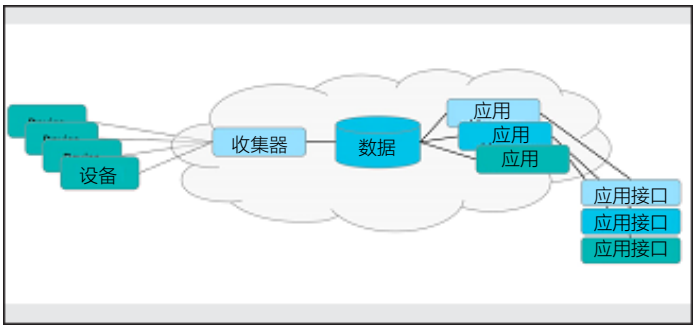

图 1：设备直接联网的物联网系统

在其他物联网系统中，设备可能在本地连接至一个汇聚节点，这个节点会充当中介或网关，从本地连接的设备中汇总数据。网关会筛选并智能地响应数据，发送数据或命令至互联网，或者接受来自互联网的数据或命令。网关设备能够将以前没有互联的设备、老设备或不安全的设备进行互联。它还支持多个设备共享一个共同的连接，进而提高运营效率。

网关设备可能还会作为外部互联设备的代理，管理本地互联设备的安全性。网关的作用非常关键，因为它管理着与下游设备的连接，必须保证下游设备的真实性。

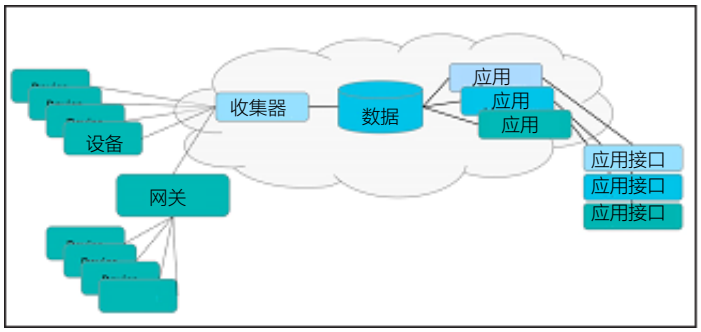

图 2：设备通过网关联网的物联网系统

比如，互联汽车中装有许多传感器和处理器，但这些设备本身就不安全，而且只连接了汽车的控制器局域网（CANbus）。这时就有一个子系统（通常是远程信息处理子系统或信息娱乐子系统）充当汽车与外部世界之间的通信网关。这个子系统会聚合其他汽车子系统中的数据，与互联网进行通信，并解读来自互联网的命令或数据，然后再通过本地 CANbus 将数据和命令重新分配给其他汽车子系统。在制造工厂等工业环境中，通过现有工业协议（Modbus、Profibus 或 DeviceNet）连接本地网关设备的设备比比皆是。本地网关可能会聚合和筛选数据，并在本地分析数据。它还能连接云端或后端服务器，从而将数据传输至一个更高级别的系统和分析软件中。

连接云端的设备可能并非一个单一的实体，而是包含多层互联网络节点。出于可扩展性、性能或容错的原因，支持这些设备的应用可能会分布在多个应用节点上，但是就互联设备而言，这些应用都是作为单一逻辑源/目标出现。

也有一些物联网系统是以点对点模式或网状模式进行通信。这些系统有一些需要特别考虑的独特的安全特点，还有一些风险、威胁和攻击需要解决。鉴于点对点操作环境的局限性，这些环境给企业带来了极大的挑战。这些设备运行时，功率、网络通信水平与计算能力、存储能力和存储容量都相对较低。它们可能会在连接与断开连接、以及不同的点对点设备集合之间进行切换。

物联网系统可能会与其他系统互联（比如后台系统、其他连接的物联网系统、政府/市政系统），也可能会连接互联网中各运营方所提供的各项服务。在考虑物联网系统的安全时，这个由设备、网络和应用系统构成的整个生态系统都必须包含在内。

我们还可以从互联事物的人类用户的角度来讨论安全性，这是一个截然不同的视角。下面，我们以一名普通消费者为例。这名消费者能够通过移动设备访问许多事物。移动设备成为了消费者观察万物互联世界的窗口，同时也是一个潜在的安全漏洞。

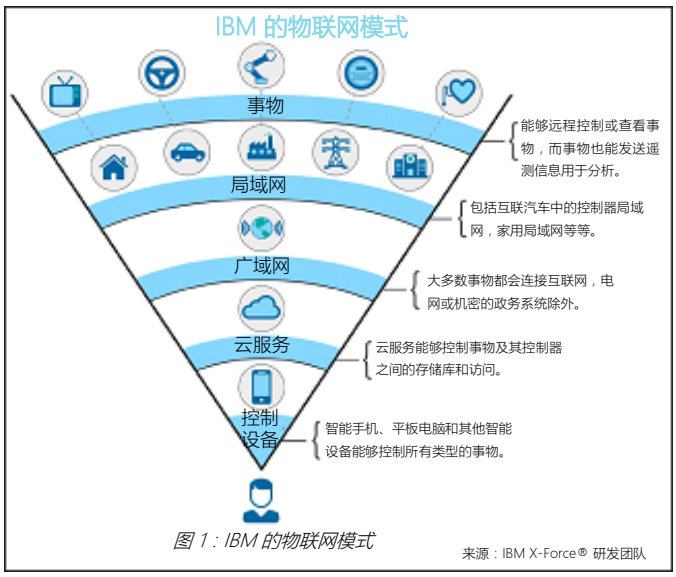

图 3：从人的角度看待物联网（来源：IBM X-Force 研发团队）[8]

前面我们已经说过，物联网系统面临着各种各样的风险、威胁和攻击。在图 4 中，我们在高级别系统架构图（图 2）上注明了这些攻击。有些威胁很常见，比如中间人攻击、应用漏洞和信息泄露。对应用或设备的拒绝服务攻击也是其中的一种威胁。此外还有一种威胁就是，非法设备或者被僵尸程序感染的设备对物联网系统中的其他系统发起拒绝服务攻击。

如今，市场上有许多保护措施保护系统免受攻击和防止漏洞被他人利用，其中很多措施甚至可以说是众人皆知。比如，操作系统完整性检查、身份验证/授权、异常检测，以及安全开发与交付。不同的物联网系统采用的是不同的保护措施，如图 4 所示。

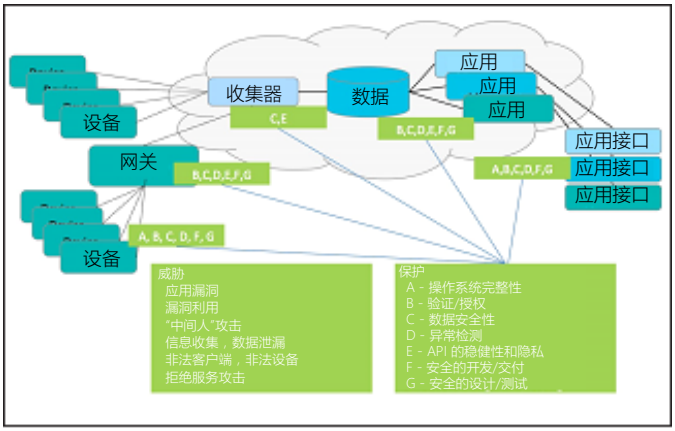

图 4：物联网系统及其威胁与保护措施

本文从两大角度，阐释了物联网系统安全管理方面的问题和技术：

- 事物的制造 - 设计和制造安全的物联网系统和设备
- 事物的运行 - 安全地运行部署的物联网系统

事物的制造 - 安全的设计和制造

安全性设计

要点：

- 根据安全工程原则，设计互联设备及其运行环境。
- 深度防御 – 在解决方案中设置多层防御系统。
- "失控"的设备成为了一个攻击面。
- 孤立的设备如今都变成了互联设备，这极大地拓宽了每个安全漏洞的影响范围。
- 必须确保设备能够进入故障自动保护模式，即使这会切断设备与物联网环境中其他事物的通信。

IBM 在安全技术领域拥有丰富的经验，推出了许多重大技术和先进的理念。在 IBM Secure Engineering Framework (SEF)[9] 中，IBM 发布了他们在软件保证和网路供应链安全领域的内部最佳实践。IBM 的 SEF 的适用范围非常广，不仅能用于软件应用开发，还适用于互联设备和物联网系统。

物联网设备的设计必须安全可靠，并且其默认安全性必须得到保障。我们必须从设备的设计阶段就开始考虑安全性问题，比如，分析设备的可能攻击面。在设计阶段，我们还必须对威胁进行建模，识别能够以哪种方式缓解哪些威胁。

同时，我们还必须从通信和运行特点的角度，考虑预期的和所需的设备运行条件。比如，如果能够从设备处理器发射的电磁辐射推理出正在执行的计算，那么攻击者就可以从中掌握该设备使用的安全程序。我们需要考虑这个外部运行特点，因为它会成为一个攻击点。为了消除这类潜在攻击，我们在设计设备时，可能需要考虑一些特殊技术。不然，我们就得定义允许的运行条件，注明该设备需要特殊的保护，以确保该设备附近没有任何 EMF 传感器。

物联网设备中必须嵌入安全通信功能。我们可以重复利用安全通信协议，包括 SSL/TLS 和 Diffie-Hellman 密钥交换等现有协议、经过测试的协议、经过分析的协议以及更新后的协议。我们也可以重复利用 Kerberos（一种有名的公钥/私钥对称加密算法）和安全哈希算法。设计团队必须确保使用的安全通信协议能够修复已知的漏洞（比如 Poodle、Heartbleed 和 FREAK），并及时地变更实施的安全通信协议。

随着设备功能的增加，设备生成、传输、接受、处理和使用的信息数量也越来越多。这种情况下，在设备中嵌入安全处理功能也变得越来越重要。因此，不论是对等设备，还是物联网环境中在其他位置运行的设备，这些设备都必须证明其唯一身份，并利用这一身份与合作伙伴建立安全的通信。

IBM 正携手设备制造商和处理器制造商，合作开发保护物联网设备生命周期的方法。在生命周期的起始阶段，我们会在物联网设备处理器中嵌入加密材料，并在制造处理器时在安全注册中心中识别处理器。在设备制造阶段，我们会在物联网设备中安装处理器，这时我们会在一个安全注册中心中注册这些设备。而在用户部署阶段，我们能够激活这些设备。通过安全注册中心，当设备处于非活动状态或停止使用时，我们可以移除该设备。这种安全注册服务提供了一个合适的安全编程接口，让处理器制造商、设备制造商和用户都能与注册中心进行安全的交互。

物联网开发团队必须遵守安全编码规则，确保其推出的环境不容易被侵入。如今市场上有许多安全编码规则资源。此外，他们还可以利用 IBM Security AppScan[10] 这类工具，来验证和实施安全编码规则。

开发团队可以在系统设计模型中增加一个安全视角，利用威胁建模[11]预测潜在的威胁向量，以及设计保护措施和缓解措施。他们可以考虑采用带安全视角和威胁建模配置的系统建模工具，比如 UML/SysML 设计工具 - IBM Rational® Rhapsody®[12]。

此外，开发团队需要避免对通过 API 的数据进行假设。相反，他们应该检查所有数据。对组件接口作出的错误假设，这是一个常见的安全漏洞。没有检查组件接口的数据会给设备带来风险，缓冲区溢出攻击和 SQL 注入攻击就是其中两个典型的风险。事实上，通过妥善地检查输入参数（检查适当的范围或者参数内容），我们就可以规避这两种风险。

面对飞速发展的环境，许多开发团队选择使用开源组件，来重复利用现有的软件，从而更快地交付核心功能。开源技术有助于加快开发速度，但是也是滋生漏洞的肥沃土壤。在记录在案的物联网设备安全漏洞实例中，许多漏洞产生的根源都是因为使用了有已知漏洞的开源组件，比如 Heartbleed/OpenSSL。由于这些漏洞被记录在案并且广泛存在，因此黑客们能够轻松地在设备上找到这些漏洞。企业应该仔细跟踪所有开源组件和版本依赖关系。IBM 的 X-Force Vulnerability Research Database[13] 和 National Vulnerability Database[14] 等数据库会定期发布和更新已知的漏洞。检测到安全风险时有办法管理和更新设备，这是物联网架构的一个关键要素。系统的漏洞源自系统更新的困难，因为这些漏洞还未被发现。通常，开源组件能够及时提供已知的补丁。但是这些补丁必须应用至开源组件部署的所有位置。

在许多环境中，防御性编码和威胁建模还不足以解决安全问题。开发人员还必须仔细记录对系统做出的所有变更，从而在出现安全问题时，能够彻底检查整个环境。在有些行业和企业，保留变更记录甚至是一项强制要求。通过使用正确的高级软件变更和配置管理环境或应用生命周期管理 (ALM) 工具，开发人员能够提高可追溯性和可审计性，更有效地应对软件故障或安全问题。IBM Rational Team Concert[15] 提供了一个跟踪变更的高级模型，帮助开发人员实现精细的变更检查和溯源。

安全设计的其中一环是定义、考虑并满足安全策略要求。在这个设计环节，开发人员需要定义一个合适的设备和整体物联网系统运行环境/条件。此外，开发人员还需要确定必要的执行机制，并开展检查，确保所需条件已经生效。

在设计设备的故障自动保护模式时，有一些特别注意事项。当互联设备发现自身、通信网络、与其通信的其他设备和系统受到威胁时，该互联设备必须依然能够安全地运行。在设计不同物联网系统的安全性时，最大的区别在于如何继续安全地运行。一个移动设备用户无法查看天气或股票价格，与一个工业水泵不能评估当前状况，进而无法确定所需的运转速度，保护河流下游人们的生命，这两者之间有很大的区别。

此外，在设计安全性时，我们还需要同时兼顾信息技术 (IT) 和运营技术 (OT) 元素。物联网系统的一部分是在一个相对受控的环境下运行，但是还有相当大一部分是在一个相对不受控的环境下运行，极端天气和对漏洞的攻击都会影响到该部分的物联网系统。这种情况下，设备的重置/更新更多地是通过自动化无线处理技术完成，因为现场调整很难实现。

现在，您可以看出保护系统安全无虞是一场多么艰难的持久战了吧。在物联网领域，我们一般更注重设备的漏洞和保护设备的需求。但是，我们也必须放眼全局，记住设备通常只是多层架构系统的一部分。物联网设备极易受到攻击，因为我们通常能在实际受控环境之外访问这些设备。即使采取了最周密的保护措施，我们也无法保证所有设备能始终保持灾备状态且不受威胁。我们无法 100% 地保证个人设备的安全性。鉴于一个或多个设备受到威胁在所难免，因此，物联网系统设计师必须作出这样一个假设：设备可能会受到威胁。但是即使有设备受到了威胁，物联网系统依然得运行，但同时又要尽量隔离和移除受威胁设备带来的漏洞。比如，一个设备在被物理地移除（被偷或被强行侵入）后又被进行了逆向工程，这个设备无疑会受到威胁。为了解决这类攻击，您可能需要付出高昂的代价，比如采用基于硬件的加密技术和烧入数字证书/密钥。但是，您依然无法根除这类攻击。因此，在设计和测试物联网系统时，您需要考虑并运行设备受到威胁的场景。这样，物联网系统就能一边识别、隔离和报告受威胁的设备，一边保证系统的其余部分继续运行。

隐私性设计

要点：

- 利用数据分离、数据隔离、数据修订和数据转换技术，移除个人身份信息。
- 在某些情况下，独特的设备标识符也可以看做个人身份标识符。
- 在通信和数据存储中，使用单独的暂时性标识符。避免关联独特的设备标识符和个人身份标识符。

在事物之间流动的数据，以及事物或其控制设备中存储的数据通常都很敏感。驾驶员可能会将他们的移动手机接入车载咨询娱乐系统中，这样，咨询娱乐系统就能访问他们的背景信息、电子邮件和短信。如果手机上装有财务应用，那么汽车甚至能访问驾驶员的信用卡信息。如果没有妥善的保护措施，驾驶员访问家庭自动化系统和工业控制系统的凭证都有可能暴露。

利用从设备中收集的信息，我们可以知道人员/事物的身份、地点、时间以及从事的作业/任务/行动。如此详细地了解这个世界的动态，这在以前是不可能做到的。这种情况下，人们开始担心以下问题：这些数据将被如何处理？哪些人可以访问这些数据？哪些人和企业有权利使用这些数据？这些顾虑完全合情合理。

多年来，计算行业致力于处理医疗记录和财务记录领域的个人身份信息 (PII)。数据隐私并非新概念，真正新鲜的其实是信息的规模和这些信息提供的细节。IBM InfoSphere Guardium[16] 和 IBM InfoSphere Optim[17] 解决方案针对数据隐私的处理专门提供了功能。这些工具能够集中控制以下事务：实时数据安全性和监控，精细的数据库审核，自动化合规性报告，数据层面的访问控制，数据库漏洞管理，敏感数据的自动发现，以及按需的静态和动态数据屏蔽。

企业在构建物联网解决方案时，需要考虑数据隐私问题。不论是构建用于访问信息的数据模型，还是构建面向合作伙伴、用户和消费者的外部接口，企业必须始终提出有关数据类型、数据格式和数据粒度的问题，并得出有关隐私性的答案。

当数据从设备流向数据收集系统时，我们必须对信息加以保护。在数据中心中，我们必须将 PII 与其他数据元素分离开来，确保信息不会传播至整个环境中。在此之前，人们就已经开始考虑并解决信息的隐私和隔离问题。比如，您可以考虑使用多级安全 (MLS) 等技术，防止对源自个人非标识数据间关联的信息或推断知识发生非授权访问。

值得注意的是，我们在使用多个数据集的信息时，可能可以从这些信息中推断出 PII，即使 PII 并未保存在这些数据集中。在医疗记录和财务记录领域，人们已经考虑并解决了这些问题。我们可以借鉴他们的经验，应用于物联网系统中。

物联网带来了新的代理业务模式，并且也支持您访问从传感器和设备中收集的信息。您可以通过一个编程接口（比如 RESTful 服务接口）,访问这些数据。该编程接口会定义以参数形式提供的数据元素，以及反馈的输入数据。在构建每一个接口时，我们必须评估其可能泄露的 PII。比如，在请求获取可穿戴设备用户数据、以便跟踪他们的日常健身锻炼时，设备的名称也可能被无意地暴露出来。根据命名习惯，我们又可能可以从这些泄露的信息反推出用户的名字，比如"Jane Doe 的 Fitbit®"。在这些场景中，我们就需要采取特殊的保护措施，防止信息的无意泄露。比如我们可以采取以下安全措施：仅反馈聚合信息（一个足够大的样本集的平均值和方差），将能够鉴别个人或设备的信息进行转变或一般化处理。

数据保存策略是数据隐私领域另一个需要考量的问题。随着我们收集的信息越来越多，我们可能会在未来用到其中的一些信息，并且这种几率越来越高。为了避免出现这种情况，我们可以采用以下方法：制定一个良好的数据保存和清理策略，积极地清除不再需要的信息。在符合法律规定的前提下积极地删除信息，这样做的理由有很多。

安全性测试

要点：

- 利用测试其他软件系统的安全性测试技术，测试物联网设备。
- 利用代码分析、正面黑客攻击和其他技术，测试设备和设备端代码。
- 不利环境测试不仅包括实体不利环境，还应该包括不利的通信和网络环境。
- 如果验证测试显示代码正确，则受攻击面会缩小。

安全漏洞测试是物联网实施项目中不可或缺的有机组成部分。软件系统测试中常用的安全性测试技术也能被用于测试物联网设备和基础架构。

在实施任意物联网项目时，我们必须根据设计规范，执行一系列测试，以便验证功能运行情况。这些测试包括：验证传感器设备中的安全机制和服务；以及验证与这些传感器设备进行通信的基础架构。

我们可以分阶段进行测试：

- 开展单元测试，验证解决方案的每个组件能否独立地发挥设计的作用。
- 开展功能验证测试，验证集成式解决方案的运行是否符合书面设计规范。
- 开展系统验证测试，验证整个解决方案环境内组件的集成和运行情况。

我们可以在所有测试阶段开展安全性测试。测试期间，我们可以使用自动化测试工具，比如 IBM Rational® Software Analyzer[18] 和 IBM Security AppScan[19]。我们还可以囊括采用正面黑客攻击技术的安全性测试。目前市面上有很多测试技术能帮助我们验证系统的安全性。我们必须反复测试软件能够抵抗攻击，因为即使在产品或解决方案面世后，都还会出现新的攻击。除了在开发阶段和质量保证阶段开展测试外，我们还应该在生产阶段测试物联网系统。既然设备会受到实际运行条件极限的影响，那么我们就应该根据计算条件的极限，相应地调整这些设备。这些条件包括抵抗拒绝服务攻击和阻塞类型的攻击。其攻击形式如下：攻击者通过向设备发送海量信息，试图迷惑设备，或者使设备过载或瘫痪。

如果可能的话，解决方案还应该通过外部分析和测试，包括通用标准 (Common Criteria) [20] 中规定的认证。IBM X-Force 提供了渗透测试所需的资源。IBM X-Force 致力于研究和监控最新的互联网威胁趋势，为 IBM 客户开发安全内容，为客户和公众提供建议，帮助他们更有效地应对新兴的威胁和重大的威胁。

持续交付模式

要点：

- 在完成设备的生产、交付和部署后，我们依然会发现问题和漏洞。
- 我们需要更新正在使用的设备端代码。
- 针对设备端代码，规划并利用持续交付技术。
- 在确定更新的应用/发布/启动时间时，我们需要考虑一些特殊的因素。

敏捷和开发运维 (DevOps) 是软件行业常用的方法，这是有一定道理的。借助这些方法，软件企业能够尽早向客户交付有用的功能，更快地收集用户的反馈意见，并更快地调整和更新这些功能。软件产品的交付更多地表现为一个持续的交付流程，而非偶尔的产品发布、迁移规划和软件转换。随着基于服务的环境的问世，产品和功能能够以服务的形式进行交付。这种情况下，频繁地更新"正处于生产中"的产品成为了一种新常态。

基于服务的环境利弊皆有。但是，当功能的更新和交付成为了一个持续的流程，最终成为一个"非事件"，我们就能利用软件的部署和交付流程，更好地应对从交付产品中发现的相关安全问题。

所有形式的安全措施都很重要：预防、检测、反应和处理。过去我们采用产品发布、补丁和修复等机制作出反应和处理。而持续交付模式能够更轻松地作出反应和处理。开发软件时，使用的敏捷和 DevOps 方法中的技术也能够用于物联网系统的开发和交付。但是这里有一个重要的区别就是：运行的代码和需要更新的代码并非存储在受控的数据中心或服务器环境中。事实上，这些代码运行于现场、路由器、网关、传感器和其他设备中。这些设备可能是移动设备或者固定设备，可能经常联网或者偶尔联网，其存储和计算能力也各有不同。但是，这些设备中依然有运行的代码；在部署到现场后，设备依然会暴露出一些问题或漏洞。鉴于没有 100% 可靠的预防措施，因此，我们需要以无线方式更新系统，解决发现的问题。

一旦针对设备中运行的代码构建了一个持续交付模式，企业就能更快速、更轻松地向客户交付功能，并频繁地发布更新和附加功能。这种模式需要验证通过无线方式收到的更新，包括使用的代码签名和验证技术。尽管它们并非新兴技术，但我们依然需要将这些技术应用于系统/设备的开发和部署领域。

在以无线方式更新现场设备时，我们需要解决一些独特的挑战。尤其设备的更新不能中断设备的运行。不然设备就必须有充足的逻辑，能够推迟更新的处理/应用，直至设备的位置、时间和环境适合应用更新。此外，设备还必须有一个故障自动保护退回机制，包括通过检查运行的系统，撤销运行不当的变更。

许多设备都将开源软件当做设备运行代码的一部分。设备制造商应该保留一份开源组件使用清单，一旦发现其中某个组件出现了漏洞，他们能够立即为设备所有者/运营商提供更新。此外，设备制造商还必须与设备所有者/运营商建立通信流程，确保一旦发现漏洞，他们能快速做出反应。目前已经有一些渠道用于发布和响应这些漏洞，包括 US-CERT[21] 和 Common Vulnerability and Exposures[22] 格式的漏洞。

确保制造和交付的完整性

要点：

- 设备的交付涵盖一整个供应链。
- 遵循现有指导原则，保护设备制造供应链。

一个可靠的供应链应该关注如何有效管理设计、制造、运输、订单履行、进出口、知识产权管理、支持和维护。IBM 引领全球的供应链安全领域，同时也是电子行业供应商行为准则组织的创始成员。此外，IBM 还参与编制了一个供应链安全的 Open Group[23] 标准。

一个可靠的供应链应该确保供应商遵循以下指导准则：

- 遵守既定的供应商行为和安全准则。
- 定期进行评估。
- 如发现违规，立即采取纠正措施。
- 确保组件的稳健性、稳定性、性能和安全性。
- 确保妥善地控制对软件和固件开发库和文件的访问。
- 通过记录所有已交付组件的来源，提供来源证书。

安全风险评估是供应商评估流程的重要一环，其目的是确定整个供应商风险的所有组成部分，包括产品风险、流程风险和业务风险。风险特征的确定有助于评估安全风险级别。风险缓解战略可以加入评估流程中。

保护制造和交付流程需要我们保护流程、步骤和供应链。保护制造流程还需要我们确保生产环境的实体安全性，因为设备和系统都是在这个环境中生产出来的。请务必确保这些系统的生产环境的安全性。转配/生产线受到感染或威胁后，就可能导致物联网设备出现漏洞。内置漏洞的电子设备例子有很多。由于制造系统本身受到了感染或威胁，导致这些设备在制造过程中就被注入了漏洞。

IBM 全球业务咨询服务部能帮助许多行业优化、审核和保护供应链。

事物的运营 - 安全运营强化设备

要点：

- 深度防御 – 在解决方案中设置多层防御系统。
- 通过隔离受威胁的子系统，保证整个解决方案仍然可用。

设备开发、测试和生产团队可以竭尽所能预防设备出现问题，但是过去的经验告诉我们，不论采取多少防护措施，设备总还是会有漏洞或者被攻击。通过部署深度防御技术，我们能够成功抵御攻击。深度防御技术的形式有很多种，比如数据中心的防火墙，或者家用路由器中的信息包过滤技术。设置多层防御系统后，这种深度防御技术将变得更为巩固，我们也可以利用该技术，隔离受到威胁的设备或系统。

为了加强设备，或者更确切地说，为了加强设备运行的环境，我们可以利用网关和路由器，将可能存在漏洞的设备从网络中隔离出来。每个网关和路由器都能够隔离其两端的设备。比如，针对位于网关另一端的受威胁设备，我们应该通过网关，隔离该设备发出的信息/数据/杂音。对于在网关或路由器后运行的设备，网关或路由器能够屏蔽这些设备的大多数潜在的网络通信。

网关或路由器还能够攻击这些环境中的某一个点。与网关和路由器保护的设备及帮助它们传输信息的设备一样，网关和路由器也要满足加强型持续交付模式和无线更新的需求。

网关和路由器也能利用传感器提供的数据反馈，成为一个网络监控点，监控设备与基于服务的应用之间的通信情况。

制定一个策略，来治理对设备的访问，并定义适当访问和不当访问（包括入站式访问和出站式访问），同时对该策略进行更新，这种方法非常有用。您不妨考虑采用一款终端设备管理解决方案，比如，IBM Unified Endpoint Management [24]，这类解决方案能够控制设备安全策略。终端设备管理系统可能无法在小型或者低能耗的嵌入式设备上运行。因此，应尽可能地将整个系统的终端设备都纳入到管理范围之内。并确保您的网关上至少有一个终端设备管理解决方案。

确保通信渠道安全无虞

要点：

- 我们必须确保设备与系统之间的通信渠道安全无虞。
- 网络类型和网络连接可能并不可靠。
- 遵循现有的与每个所用协议有关的指导原则。
- 一般采用 SSL/TLS 保护 IP 通信。

物联网系统采用了很多种网络通信机制。这些机制包括使用低能耗、小范围方法（如 Bluetooth、Bluetooth Low Energy、6LoPAN 和 Zigbee 等）的局域网；使用 WiFi 的局域网；以及使用 2G、3G 和 4GLTE 的广域网。

一个设备在实体环境中移动时，接入的网络的安全级别各有不同。同样的，不同网络模式提供的保护等级差别也很大。但是，物联网系统必须能够通过各种网络机制，建立安全的通信。

物联网系统中的通信通常分为两种：一种是通过 TCP 网络连接开展的基于 HTTP（REST 类型的调用）的通信；另一种则是在 IP 网络堆栈上开展的某些形式的基于事件的通信。基于事件的通信模式包括 DDS、CoAP 和 MQTT 格式。基于事件的通信模式通常会用 UDP 模式而非 TCP 模式，来减少网络引发的连接或数据传输延迟。

不论是基于 HTTP 的模式，还是基于事件的模式，它们都是使用 SSL/TLS 来建立受保护的通信。这种模式结合了多种加密算法，来建立一个安全的通信渠道。这样，设备、网关和云托管系统中的大多数逻辑都能够采用一个安全的通信渠道，并专注于提供设备或应用的功能。

审核并分析使用模式

要点：

- 预防措施不能解决所有问题。
- 通过检测才能作出反应和处理。
- 利用现有的日志分析技术，识别并响应异常情况。

计算行业不可能预测甚至防止一个系统可能受到的所有攻击。因此，检测、响应和处理攻击场景的重要性一点也不亚于在设备、 实施和部署系统时将安全性铭记在心。同样的，计算行业的许多现有功能也能够应用 于物联网环境中。

管理计算环境时，我们需要监控系统行为，检测需要特别注意的场景，并针对这些场景作出响应。我们需要考虑实时响应和近乎实时的响应、长期分析和报告。同时，我们还要检测主动攻击，并响应这些攻击。这些场景的起因可能是非法设备、来自外部的拒绝服务攻击，或者对该环境中运行的某个设备或某组设备的持续攻击。通过主动监控系统的使用模式，我们便可识别异常行为，进而采取适当的相应措施。部署监控工具来监控系统还只是第一步。您还必须查看和响应各个场景，而非只是监控和记录事件。IBM Security QRadar® SIEM[25] （安全信息和事件管理，简称 SIEM）等工具中就具有此类审核和分析功能。

有些潜在威胁可能会持续一段很长的时间。这种情况下，我们就必须观察系统行为，了解通常或预期的行为模式。通过主动监控系统，我们能够确定某些事件是否是异常事件。通过使用异常检测技术，当设备运行/使用/发出的信息与其正常运行行为不符时，我们就能立即发现这些可能受到威胁的设备。IBM Operations™ Analytics - Log Analysis[26] 等工具能够为您提供所需功能，帮助您长时间监控系统环境，确定系统运行是否与预期行为相符。

我们必须主动监控系统中发生的事件，包括通过网关、在设备、云端和数据中心托管计算服务中移动的事件。我们还需要制定相关策略，来审核整个系统的运行。这种审核更像是对监控者的监控，旨在保护系统免受内部攻击。有了一个主动审核流程，攻击或破坏系统就得在多方合作的情况下才能发起。通过增加系统审核的人数或层级，我们能够进一步提高保护级别。系统会例行记录所有访问尝试。并且这些日志要保存一段时间，以便我们在了解某个攻击和潜在泄露程度时，能够进行取证。

不断更新安全环境

要点：

- 安全环境应该包括以下方面：验证、授权、审核、管理、加密/解密、密钥管理和完整性检查。
- 结合利用多种技术和流程，确保环境安全无虞。
- 与数据中心、云端或其他受控环境中运行的系统相比，设备运行的环境的受控程度更低。

物联网应用安全环境的构建和维护，与企业所有计算系统的安全计算环境息息相关，并且前者还依赖于后者。此外，验证、授权（访问控制）、审核和管理等方面的要素同样如此。当我们与用户、群组、移动设备和终端设备交互时，设备数量比过去要多几个数量级。终端设备与企业的工作人员密切相关。在物联网世界中，我们需要考虑许多终端设备和各种各样的安全支持功能。

除了用户和设备注册、验证和访问控制外，我们还需要管理加密和解密机制中的密钥，这些机制是用于验证、通信和数据存储。通过密钥管理（包括物联网设备）流程，我们能够保护信息在源头到终点的流动，不论信息是处于流动状态还是静止状态。我们也可以利用物联网设备的可信平台模块 (TPM) 中的烧入私钥数据，执行密钥管理。可信计算组织 (TCG)[27] 已经制定并改进了有关 TPM 设备的规范。

借助 IBM Identity Management[28] 解决方案的功能，包括在使用 IBM Bluemix[29] 时使用 IBM Identity，我们能够针对与开发的物联网解决方案有关的用户/群组定义，不断更新安全环境。IBM IoT Foundation[30] 提供支持设备注册和生命周期的功能。这种功能中就有一些用于维持一个安全环境的基本功能，从而保护设备和通过这些设备进行通信的应用。其中就包括前文提到的安全设备注册功能。

利用 IBM Security Key Lifecycle Manager[31] 的功能，我们能够洞悉加密密钥管理和分配所需的核心功能集。尽管该产品主要在金融服务环境中使用，但是这些功能的初衷是将密钥管理融入设备级别的加密服务中。以 OASIS 密钥管理互操作性协议 (KMIP) [32] 为基础，我们可以将密钥管理扩展至分布式网络环境中的各种设备中。第一个采用这种方法的设备是 IBM 加密磁盘驱动器。KMIP 协议将被设计得尽可能的简洁。此外，KMIP 协议还能帮助您实施和支持各种网络设备和计算设备。

除了管理身份和加密密钥信息外，我们还需要管理和维护环境中的所有设备。比如，我们需要定期更新设备、网关、路由器和其他基础设施，运用所有安全补丁和修复程序。过去，我们需要大量手动作业来与设备、网关或路由器直接交互，以便执行固件或软件的升级、修复或迁移。未来设备数量会越来越多，人们对更新频率的期望也会越来越高。这种情况下，这些工作将逐渐从积极的人工参与模式转向自动化的无线更新处理模式。届时，只有在处理异常情况时才需要人工干预，而不需要人工处理每次更新。这意味着，我们将提高监控和报告级别，更有效地监控和报告所有涉及的网关、路由器和设备库存的更新处理状态和进度。

鉴于互联设备的价格会随着时间发生变动，因此，我们没有必要一直更新所有设备，或者保护每个设备免受所有攻击。这种情况下，我们应该采取一种性价比最高的管理方式，那就是不考虑失去价值的设备，并设置网关，忽略/筛除该设备发出的信息。此外，设备制造商还可以考虑在设备中增加一个自毁功能。设备仍将以设备自动保护模式或最小运营断开模式运行，但是不会接入网络，从而保护自身及其余环境。尽管可能会丢失一部分设备提供的传感器信息，但是攻击者也没法通过设备（设备无法打补丁/修复漏洞）攻击整个环境。

正如前文所说的，与管理其他联网技术设备一样，物联网设备制造商在管理更新的安全环境时，需要预测并响应安全事故报告。

与计算环境的其他部分一样，我们必须考虑并解决整个环境中登录/密码信息的主动管理和更新问题。比如，我们需要考虑如何主动管理物联网设备中嵌入的登录/密码信息。其中涉及的领域包括：密钥生命周期管理、身份管理、无线更新、设备注册和生命周期管理。同时，我们要考虑的利益相关方也有很多：设备制造商、设备采购商/所有者/管理者，以及设备用户。此外，我们还要考虑一些潜在的第三方：网络通信服务提供商、设备服务和支持承包商。

构建一个可信的维护生态系统

要点：

- 遵循现有的指导原则，构建并维护一个安全的环境。
- 构建一个全面的事故响应流程。

如果我们想运营一个安全的物联网系统，就需要负责运营物联网环境的人员注意他们的行为是否安全、妥当。如需了解更多信息，请查看保护供应链章节，供应链包括运营环境时所用的承包商。为了维持系统的安全性和完整性，我们需要遵守恰当的维护步骤。

为了处理安全事故报告，我们需要构建一个定义清晰且经过明确沟通的事故响应流程。借助该流程，在事故被发现和确认后，我们将有一个条理分明的补救计划来消除漏洞；其他可能被漏洞波及的组件所有者也将得到通知，从而执行补救计划。通过重复使用组件和构建解决方案，事故响应流程能够确保快速识别并补救所有可能被漏洞影响的组件。

未来，整个物联网系统的实体安全依然是一个问题。物联网设备本身的性质决定了它们的运行条件非常苛刻、困难，并且物联网设备会直面很多实体因素，面对各种各样的攻击。它们会在一个“失控”的环境下运行，会快速移动，会受到很多极端条件的影响。尽管对大型高科技电子部署项目来说，这是一个全新的领域，但是事实上这并不是什么新兴事物。军事应用、车载系统、航空电子设备、传感器，以及迄今为止为了保护移动设备构建的所有事物已经为我们指引了方向，我们可以从这些设备身上，发现值得借鉴的适当的实践。

总结

物联网技术的安全性与其他大型计算基础架构的安全性之间既有不同之处，也有相似之处。它们面临同样的问题，并利用同样的技术解决这些问题，包括验证（设备、系统/应用和用户），授权、审核、管理、加密/解密、数据完整性和密钥管理等技术。同时，新的挑战也在涌现：计算设备类型和功能的种类更多；运营的全球环境相对不受控；需要保护的攻击面也更多。

物联网安全领域面临新的挑战。但是通过利用经过多年优化的研发技术，我们能够克服这些挑战，前提是我们对这些技术进行扩展，以满足物联网的独特要求。

贡献者

《IBM 观点：物联网安全》是全体 IBM 员工精诚合作的成果。在此，衷心感谢以下人员为本篇《IBM 观点》发表所付出的关注和贡献。

Timothy Hahn	杰出工程师，IBM Analytics – 物联网
Sky Matthews	首席技术官，IBM Analytics – 物联网
Lisa Wood	总监，IBM Analytics – 物联网
John Cohn	同事，IBM Corporate Technical Strategy
Shmulik Regev	高级技术人员，IBM Security
Jim Fletcher	杰出工程师，IBM Analytics – 物联网
Eric Libow	杰出工程师，IBM Analytics – 物联网
Chris Poulin	研究策略师，IBM X-Force
Katsumi Ohnishi	杰出工程师，IBM Security

有关更多信息

如欲了解有关 IBM Internet of Things 的更多信息，敬请访问：http://www.ibm.com/software/info/internet-of-things/

参考文件

1 IDC."Worldwide and Regional Internet of Things 2014-2020 Forecast Update by Technology Split". 文档号 #252330. 发布日期：2014 年 11 月. http://www.idc.com/getdoc.jsp?containerId=252330

2 Storm、Darlene. " Hackers exploit SCADA holes to take full control of critical infrastructure". 发布日期：2014 年 1 月 .Computerworld.http://www.computerworld.com/article/2475789/cybercrime-hacking/hackers-exploit-scada-holes-to-take-full-control-of-critical- infrastructure.html

3 IBM IBV Driving Security. http://www-935.ibm.com/services/us/gbs/thoughtleadership/automotivesecurity/

4 开放式 Web 应用程序安全项目组织 (OWASP) 物联网十大问题. http://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

5 IIC Reference Architecture. http://www.iiconsortium.org/ and IIC Security Working Group Reference Guide – http://www.iiconsortium.org/wc-security.htm

6 Allseen Alliance. https://allseenalliance.org/

7 BuildItSecure.Ly. http://builditsecure.ly

8 X-Force Research and Development."IBM X-Force Threat Intelligence Quarterly 4Q 2014". 文档号 #WGL03062USEN. 发布日期：2014 年 11 月. http://www.ibm.com/security/xforce/downloads. html

9 IBM Secure Engineering Framework. http://www.redbooks.ibm.com/abstracts/redp4641.html

10,19 IBM Security AppScan®. http://www.ibm.com/software/products/en/appscan-source

11 Threat Modeling.http://en.wikipedia.org/wiki/Threat_model

12 IBM Rational® Rhapsody®. http://www.ibm.com/software/products/en/ratirhapfami

13 X-Force Vulnerability Research Database. https://xforce.iss.net/

14 National Vulnerability Database. http://nvd.nist.gov/

15 IBM Rational Team Concert. http://www.ibm.com/software/products/en/rtc

16 IBM Infosphere Guardium Data Security.http://www.ibm.com/ software/data/guardium/

17 IBM Infosphere Optim Data Privacy. http://www.ibm.com/software/data/optim/

18 IBM Rational® Software Analyzer. http://www.ibm.com/software/products/en/ratisoftanalfami

20 通用标准. http://www.commoncriteriaportal.org

21 US-Cert. http://www.us-cert.gov/

22 Common Vulnerability Exposures.http://cve.mitre.org/

23 Open Group – Supply Chain Security.http://www.opengroup.org/news/press/open-group-releases-global-technology-supply- chain- security-standard

24 IBM Unified Endpoint Management.http://www.ibm.com/software/tivoli/unified-endpoint-management/

25 IBM Security QRadar® SIEM.http://www.ibm.com/software/products/en/qradar-siem

26 IBM Operations™ Analytics – Log Analysis.http://www.ibm.com/software/products/en/ibm-operations-analytics-log-analysis

27 Trusted Computing Group. http://www.trustedcomputinggroup.org/

28 IBM Identity and Access Manage. http://www.ibm.com/software/products/en/identity-access-manager

29 IBM Bluemix. http://www.bluemix.net

30 IBM IoT Foundation. http://internetofthings.ibmcloud.com

31 IBM Security Key Lifecycle Manager. http://www.ibm.com/software/products/en/key-lifecycle-manager

32 OASIS Key Management Interoperability Protocal (KMIP).http://www.oasis-open.org/committees/kmip/

© Copyright IBM Corporation 2015

IBM Corporation Software
Group Route 100
Somers, NY 10589

美国印刷
2015 年 4 月

IBM、IBM 徽标、ibm.com、AppScan、QRadar、Rational、Rhapsody 及 X-Force 是 International Business Machines Corporation 在世界各地司法辖区的注册商标。其他产品和服务名称可能是 IBM 或其他公司的商标。Web 站点 ibm.com/legal/copytrade.shtml 上的"Copyright and trademark information"部分中包含了 IBM 商标的最新列表。

Fitbit 是 Fitbit, Inc. 的注册商标和服务标记。

本文档截至最初公布日期为最新版本，IBM 可随时对其进行修改。IBM 并不一定在开展业务的所有国家或地区提供所有这些产品或服务。

本文档内的信息"按现状"提供，不附有任何种类的（无论是明示的还是默示的）保证，包括不附有关于适销性、适用于某种特定用途的任何保证以及非侵权的任何保证或条件。IBM 产品根据其提供时所依据协议的条款和条件获得保证。

客户应负责确保与适用法律和法规的合规性。IBM 并不提供法务建议，亦不承诺或保证其服务或产品可确保符合任何法律或法规。有关 IBM 未来发展方向及意图的声明如有变更或撤销，恕不另行通知，且仅用于说明目标之用。

良好的安全实践声明：IT 系统安全涉及通过对来自贵企业内外部的非法访问进行阻止、检测和响应来保护系统和信息。非法访问会导致信息变更、损毁或滥用，或导致对您的系统的破坏或滥用，包括用于对他人的攻击。没有任何 IT 系统或产品可被视为完全安全，也没有单一产品或安全措施可完全有效地阻止非法访问。IBM 系统和产品设计为全面的安全方法的一部分，该方法必然涉及其他操作程序并可能需要其它系统、产品或服务，以达到最大效力。IBM 不保证任何系统和产品可免受任何一方的恶意或非法行为的影响。

请回收利用

RAW14382-CNZH-00