2015 年 4 月

IBM 观点：物联网安全

“事物”的互连互通营造了一种活跃的环境，有利于开展创新和寻求商机，同时也带来了一系列安全挑战和威胁。

IBM

引言

本文将全面介绍 IBM® 关于物联网 (IoT) 系统安全和隐私的观点。根据 2014 年 11 月发布的一份报告，分析师预计，到 2020 年，物联网中的互连设备将达到 300 亿台，而 2013 年这一数字仅为 990 万。[1] 如今，在我们的生活环境、商业环境和企业环境中，互连设备无处不在，例如恒温器、医疗设备、汽车和工业设备。这些互连设备营造了一个活跃的环境，有利于企业开展创新、寻找商机。与此同时，这种日渐膨胀的计算环境也带了一系列安全问题和威胁。在这个万物互连互通的世界中，设备生成和使用的数据、为这些数据提供支持的系统和应用都有可能沦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 IoT 系统中使用和提供数据时，以错误的方式服务或拒绝服务应用。

制造业、能源业、运输业及其他工业经济领域也在使用物联网系统，这些工业 IoT 系统面临的挑战甚至更为严峻。工业设备的联网可使其获得更广泛的可视性、控制力和状态维护能力，但也同样让它们易受安全攻击。有关监视控制与数据采集 (SCADA) 系统和工业控制系统 (ICS) 系统遭受攻击的报告已多次公布。“在研究了 60,000 多个网上公开的控制系统后，两位俄罗斯安全研究人员发现了一些安全漏洞，通过这些漏洞，他们可以全面控制能源系统、化学系统和运输系统。”[2]

IoT 系统由大量设备（装置）构成，这些设备可与其他设备、应用和服务进行通信，而这些其他设备、应用和服务使用各种不同协议，并且会利用应用程序编程接口 (API)，访问整个互联网上的数据和服务。物联网设备多种多样，既有基本的单个传感器，也有更成熟、更强大的处理节点，前者直接联网或通过某种简单的网关联网，而后者则会自动进行处理。例如，一台互连车辆便是一个复杂的设备，其中包含各种不同的电子子系统和传感器，这些系统和传感器不仅可以自动进行处理，还能通过无线连接网络。

每个系统面临的风险状况不同，因此 IoT 安全防护需求也各不相同。例如，一个消费者 IoT 系统与一个复杂的任务关键型企业级 IoT 系统，前者用于评估和控制园艺植物供水系统，后者用于石油钻井或管线作业，其中包含与 IoT 互连的阀门和水泵，两者的安全需求必然有所不同。

钻井和管线作业必须采用安全关键型系统，以便保护企业、环境和人身安全。面对相同的安全威胁，钻井作业受损所带来的风险和代价远远高于家用花园供水系统。因此，对于这类系统，综合安全措施、专业知识、分析、测试和管理必不可少。如果企业在构建 IoT 系统时面临着极高的安全风险和复杂性问题，那么便需要聘请经验丰富的主题专家就此类系统的设计和运作提供指导。IoT 安全性是一个热门话题，许多人员和组织纷纷就此发表观点和看法。在 2014 年 6 月发布的一篇 IBV 调研报告[3] 中，IBM 首次提及了安全性与物联网。其他实体也发布了同类信息和观点，其中就包括开放式 Web 应用程序安全项目组织 (OWASP)4 近期发布的一篇文档；此外，相继跟进这一话题还有一些联盟组织，例如工业互联网联盟 (IIC)[5]、Allseen Alliance[6] 和 builditsecure.ly[7]。

IoT 系统（或任何 IT 环境）安全性的关键点在于，系统无法依靠保持每一台互连设备的恒久完整性来确保整个系统的持续完整性。IoT 系统的设计方案和安全功能都建基于以下这个假设之上：总会有一个或多个设备受损（任何安全措施均无法做到万无一失），但整个系统仍能安全运行。

物联网系统架构

IoT 系统配置方式多种多样。在某些 IoT 系统中，所有设备均直接联网，每个设备对自身的本地安全负责。

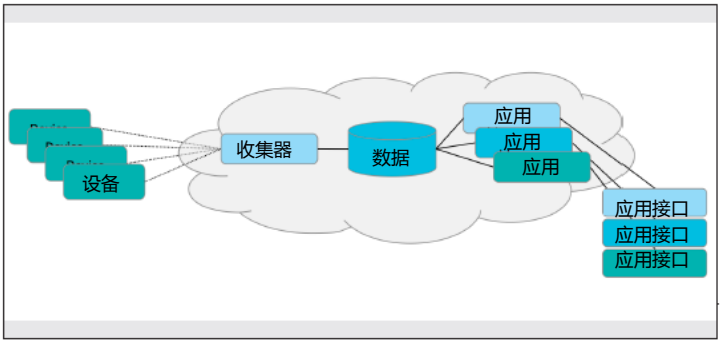

图 1：设备直接联网的 IoT 系统

在其他一些 IoT 系统中，设备很可能在本地连接至一个聚合节点，聚合节点将充当中介或网关，从本地互连设备汇总数据。网关会过滤数据并智能地对其做出响应，从互联网收发数据或命令。网关设备用于连接之前没有互连的设备、旧设备及不安全设备。另外，它还支持多个设备共享一个共同的连接，进而提高运行效率。

网关设备还可以作为连接外部世界的其他设备的代理，代表本地连接设备负责管理安全性。网关是安全系统的重要组成元素，因为它管理着与下游设备的连接，而且必须确保下游设备的真实性。

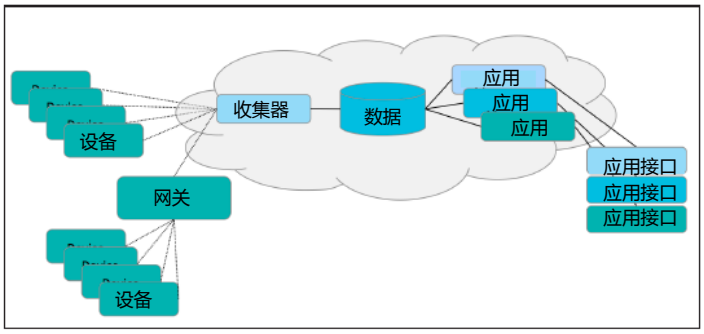

图 2：设备通过网关联网的 IoT 系统

例如，互联汽车包含大量传感器和处理器，这些设备本身并不安全，而且仅与汽车的控制器局域网 (CANbus) 相连。这时就需要一个子系统（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。该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，这个子系统通过本地 CANbus 将数据和命令重新分发至其他汽车子系统。在制造工厂等工业环境中，设备通过现有工业协议（如 Modbus、Profibus 或 DeviceNet）连接本地网关设备的情况比比皆是。本地网关可汇总数据、过滤数据并在本地分析数据。同时，它还能连接云端或后端服务器，将数据向上传播至更高级别的系统和分析软件中。

连接云端的设备可能不是单一实体，而是包含多层互连网络节点。由于扩展性、性能或容错原因，支持这些设备的应用很可能分散于多个硬件节点上，但从互连设备的角度而言，这些应用却与单一逻辑源/目标并无二致。

还有一些 IoT 系统采用点到点模型或网状模型开展通信。在这些系统中，不仅要考量独特的安全特性，还要衡量需要应对的风险、威胁和攻击。鉴于点到点运行环境的种种限制，此类环境会带来严峻挑战。

这些设备往往运行功率较低、网络通信水平低下，而且计算、存储和记忆能力相对较差。设备不但可能会在断开状态与连接状态之间自由切换，还能在不同的点到点设备集合之间自如转换。

IoT 系统可能会与其他系统互连，如后台系统、其他联动 IoT 系统、政府或政务系统，也可能会与互联网中其他各方提供的服务相连。在考量 IoT 系统安全时，必须将由设备、网络和应用系统构成的整个生态系统考虑在内。

我们还可以从互连设备的人类用户角度来看待安全问题，在本示例中我们以一名普通消费者为例。这名消费者可以通过移动设备访问很多内容。移动设备成为消费者通向互连互通世界的窗口，同时也是一个潜在的安全漏洞。

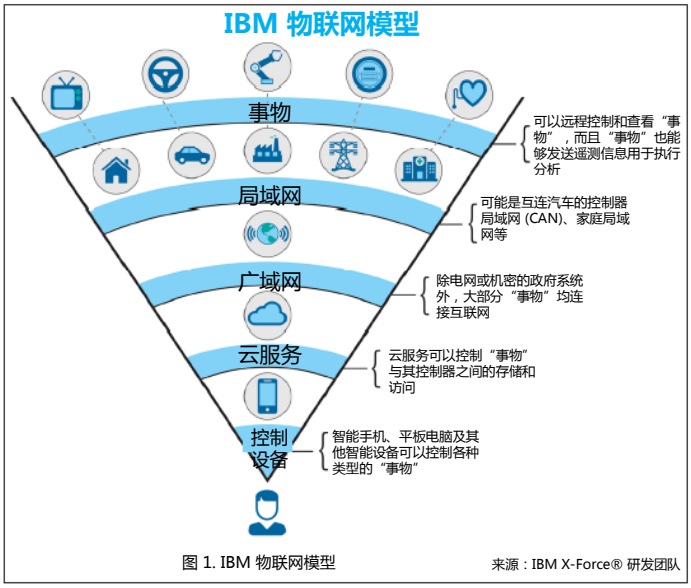

图 1. IBM 物联网模型　　来源：IBM X-Force® 研发团队

图 3：从人类角度看物联网（来源：X-Force 研发团队）[8]

如上文所述，IoT 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。

有些威胁广为人知，如中间人攻击、应用漏洞和信息泄露。拒绝服务攻击（无论应用还是设备）也是一种威胁。特别是由非法设备或受僵尸程序感染的设备对 IoT 环境中其他系统发起的拒绝服务攻击。

应对攻击和漏洞的防护措施数量庞大，而且很多防护方法广为人知。比如，操作系统完整性检查、身份验证/授权、异常检测及安全开发和交付。如图 4 所示，不同的 IoT 系统会采用不同的保护措施。

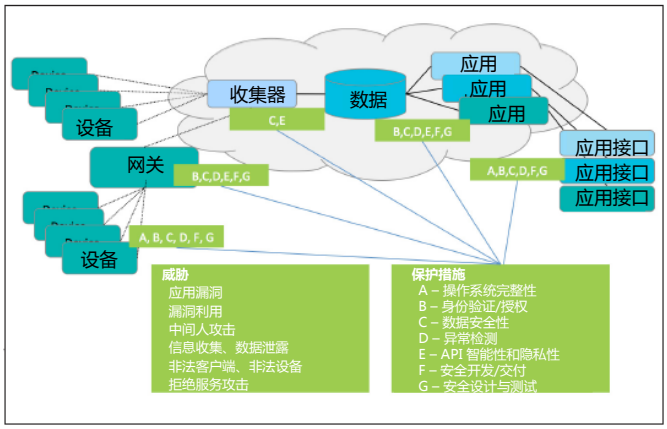

图 4：IoT 系统及其威胁和保护措施

本文从两个角度出发，阐释了 IoT 系统安全管理方面的问题和技术：

- 设备制造者 - 设计和制造安全的物联网系统和设备
- 设备运行者 - 安全地运行部署的 IoT 系统

设备制造者 - 安全地设计与制造

为安全而设计

关键要点：

- 根据安全工程原则，设计互连设备及其运行环境。
- 深层防御 - 在解决方案中设置多层防御机制。
- 设备处于网络中，现已成为一个攻击面。
- 过去彼此孤立的设备如今都变成了互连设备，这大大拓宽了每个安全漏洞的潜在影响范围。
- 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环境中其他设备的通信。

IBM 在安全技术领域拥有丰富的经验，推出了许多重大技术，并提出了许多先进理念。在 IBM Secure Engineering Framework (SEF)[9] 中，IBM 发布了面向软件保证和网络供应链安全的内部最佳实践。IBM SEF 的应用范围十分广泛，不仅可以用于软件应用程序开发，还适用于互连设备与 IoT 系统。

IoT 设备的设计必须安全可靠，而且默认安全性必须得到保障。从设备设计阶段开始严把安全关，同时分析设备的潜在攻击面。另外，在设计过程中，还要实施威胁建模，辨别哪些威胁可以缓解以及如何缓解那些威胁。

同时，务必从通信和运行特点的角度出发，综合考虑预期和必要的设备运行条件。例如，如果可以利用设备处理器发射的电磁辐射 (EMF) 推理出正在执行的计算，那么攻击者就可以从中了解设备所使用的安全机制。这种外部运行特点就是一个需要考虑的攻击点。为消除此类潜在攻击，在设备设计过程中，我们可能需要使用一些特殊包装技术。我们也可以定义允许的运行条件，标明设备需要特殊保护，以确保设备周围没有任何 EMF 传感器。

IoT 设备必须嵌入安全通信功能。我们可以重复利用通信协议，包括 SSL/TLS 和 Diffie-Hellman 密钥交换等经过测试、分析和更新的协议。我们也可以重复利用 Kerberos（一种知名的对称式公钥/私钥加密算法）和安全哈希算法。各团队必须确保所用的安全通信协议能够修复已知漏洞（如 Poodle、Heartbleed 和 FREAK），并及时变更所实施的协议。

随着设备功能的增加，设备生成、传输、接收、处理和使用的信息数量也随之增加。在这种情况下，在设备中嵌入安全处理功能的重要意义也大幅提升。设备必需能够证明其唯一身份，并运用这一身份与其他设备建立安全通信，无论是在环境中其他位置运行的对等设备，还是对等服务。

IBM 正在与设备和处理器制造商开展合作，共同开发保护 IoT 设备生命周期的方法。在生命周期的起始阶段，我们首先将加密材料嵌入 IoT 设备中的处理器，并在制造处理器时向安全注册中心确认这些处理器。然后，设备制造期间会将处理器安装到 IoT 设备中，此时就会向安全注册中心注册这些设备。随后，在用户部署阶段，我们会激活这些设备。当设备脱离活动状态或停止运行时，安全注册中心允许移除或淘汰这些设备。安全注册中心服务提供了一个适当的安全编程接口 (API)，处理器制造商、设备制造商及用户都能安全地与注册中心进行交互作用。

IoT 开发团队必须遵循安全编码规则，确保其推出的环境不易遭到入侵。如今，市场上存在多种安全编码规则。此外，用于验证和实施安全编码规则的工具（如 IBM Security AppScan[10]）同样层出不穷。

开发团队可在系统设计模型中增加一个安全视角，运用威胁建模 [11] 预测潜在威胁载体，并设计保护措施和缓解方案。开发团队

可以考虑运用带有安全视角和威胁建模功能的系统建模工具，如 IBM Rational® Rhapsody®[12]（一种 UML/SysML 设计工具）。

此外，开发团队需要避免对通过 API 的数据做出想当然的假设，而应检查所有数据。对组件接口所做的错误假设是一种常见的安全漏洞。未检查组件接口数据会引发两类常见风险：缓冲区溢出攻击和 SQL 注入攻击。通过妥善地检查输入数据，不管是检查适当的范围，还是参数内容，都可以避免上述两类攻击风险。

在当今瞬息万变的环境中，很多开发团队选择使用开源组件，以便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，但同时也为漏洞创造了滋生温床。据记载，在 IoT 设备中发现的大量安全漏洞中，许多漏洞皆因使用了带有已知漏洞的开源组件，比如 Heartbleed/OpenSSL。由于这些漏洞已被记录在案并广泛存在，黑客能够轻松地在设备上找到这些漏洞。广大组织应严格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漏洞· 无论对于任何 IoT 架构，在检测到安全漏洞后，有办法管理和更新设备都是关键要素。奋力更新系统必然会引发系统漏洞，因为这些漏洞都尚未被发现。通常，开源组件能够积极提供补丁程序。但是在公开发布后，这些补丁程序必须应用至开源技术所有的部署位置。

在很多环境中，实行防御性编码和开展威胁建模不过是杯水车薪。开放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。某些行业和组织可能会强制保留变更记录。通过运用适当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，有助于提高可追溯性和可审计性，从而更有效地应对软件故障或安全漏洞。IBM Rational Team Concert[15] 可以提供一个跟踪变更的精密模型，帮助实现精细的变更审查和跟踪。

在安全性设计过程中，必需确保制定、考量及满足安全策略要求。这个设计环节包括为设备和整个 IoT 系统定义一个合适的运行环境/条件。另外，还要确定必要的执行机制，并开展检查，确保所需条件均已到位。

在设计设备的故障自动保护模式时，需要特别注意一些事项。互连设备必须能够持续安全运行，即使在设备本身、通信网络或者与之通信的其他设备和系统遭到威胁的情况下也不例外。在设计不同 IoT 系统的安全性时，最大的区别在于如何确保持续安全运行。例如，一个移动设备用户无法检查天气或股票价格，与一个工业水泵无法评估当前状况，继而无法确定所需运行速度以保护下游居民安全，这两者之间存在显著差异。

此外，安全性设计还必须考量信息技术 (IT) 和运营技术 (OT) 元素。部分 IoT 系统是在相对受控的条件下运行，但是还有相当大的部分是在一个受控程度较低的环境下运行，这类环境极易受极端天气状况的影响而且容易受到攻击。在这种情况下，设备重置/更新更多地依赖于无人参与无线处理技术，因为即使在最佳条件下也很难实施现场调整。

显而易见，保障系统安全是一场艰难的持久战。在物联网中，我们理所当然地将目光投向设备漏洞和设备保护需求。但是，绝不能忽视大局 - 要记住设备往往隶属于更大的“多层架构系统”。IoT 设备尤其容易受到攻击，因为此类设备常常接收到来自实际受控环境之外的访问。即使采取了最周密的保护措施，我们也无法确保所有设备持续保持灾备状态且丝毫不受威胁。人们根本无法完全保证单个设备的安全性。鉴于一个或多个设备受到威胁在所难免，因此，IoT 系统设计师必须假设设备可能会受到威胁。在一个或多个设备受损的情况下，系统依然能够继续正常运行，同时又尽力隔离和消除受损设备所带来的漏洞。例如，设备在进行物理移除（被盗或被入侵）后又实施了逆向工程时，可能会受损。为应对这类攻击，您可能会使用代价高昂的基于硬件的加密和固化数字证书/密钥。

但是，依然无法消除这类攻击。因此，在设计和测试系统的过程中，必须考虑并运行设备遭受攻击的场景。此流程可确保系统能够识别、隔离及报告受损设备，同时保证系统的其余部分依然正常运行。

为隐私而设计

关键要点：

- 运用数据分离、隔离、修订和数据转换技术，移除个人身份信息。
- 在某些情况下，可将独特的设备标识符视为个人身份标识符。
- 在通信和数据存储中，使用单独的短暂标识符。杜绝独特的设备标识符和个人信息标识符之间的关联。

通常，在事物之间流动的数据以及事物或其控制设备上存储的数据都十分敏感。驾驶员可能会将移动手机与车载资讯娱乐系统相连接，这时，系统就能访问驾驶员的联系信息、电子邮件和短信。如果手机上安装了财务应用，那么汽车甚至能够访问驾驶员的信用卡信息。若未妥善保护，驾驶员访问住宅自动化系统和工业控制系统的凭据也可能会暴露。

从设备中收集的信息可用于确定谁或者什么，在哪里，什么时间，做过什么事（操作/任务/行为）。如此详细地了解世界的动态变化，这达到了前所未有的水平。在这种情况下，人们开始担心：这些数据被如何处理？哪些人员有权访问这些数据？哪些人员和企业可以使用这些数据？人们的这些顾虑也是情理之中的事情。

多年来，计算行业一直在竭力处理医疗记录和财务记录领域的个人可识别信息 (PII)。数据隐私并非新理念，但信息规模之大及信息内容之详细却是从未出现过。IBM InfoSphere Guardium[16] 和 IBM InfoSphere Optim[17] 解决方案提供了针对数据隐私的特定功能。这些工具可集中控制：实时数据安全性和监控、精细的数据库审计、自动化合规报告、数据级访问控制、数据库漏洞管理、敏感数据的自动发现以及按需静态和动态屏蔽。

在构建 IoT 解决方案的过程中，企业需要充分考虑数据隐私问题。从用于存储信息的数据模型到面向合作伙伴、用户和消费者的外部接口，企业必须始终关注数据性质、数据格式和数据粒度问题，并找到隐私性相关问题的答案。

当信息从设备流向数据收集系统时，我们必须对相关信息提供保护。在数据中心内部，应将 PII 与其他数据元素分离开来，避免这些信息弥漫整个环境。过去，人们一直都在努力思考和解决信息隐私和隔离问题。例如，有人考虑运用多级安全防护（MLS）等技术，防止对信息进行未授权访问，或者防止对个人非标识数据间关联的推断知识进行未经授权的访问。

值得注意的是，运用多个数据集的信息可以推断出 PII，即使这些数据集中未存储 PII。在医疗记录和财务记录管理领域，人们已经考虑和解决了这些问题，相关实践经验也可以应用于 IoT 系统中。

另外，物联网带来了新的代理业务模式，也支持访问从传感器和设备收集而来的信息。通常，通过编程接口（如 RESTful 服务接口），便可以访问这些数据。编程接口会定义以参数形式提供的数据元素和返回的输出数据。每个接口必须经过评估，确定 PII 潜在泄露风险。例如，在查询可穿戴设备的用户数据，以便跟踪用户的日常健身锻炼时，可能会无意泄露设备的名称。根据命名习惯，通过这些泄露的信息，很可能可以推断出用户的名字，如 Jane Doe 的 Fitbit®。在此类情况下，我们就需要采取特殊保护措施，防止信息的无意泄露。例如，我们可以采取以下保护措施：仅返回聚合信息（一个足够大的样本集的平均值和方差），将能够识别个人或设备的信息进行转化或一般化处理。

在数据隐私方面，另一个需要考虑的问题是数据保留策略。随着我们收集的信息越来越多，有些信息在未来只会极少用到的情况也日益增加。

为避免这种情形，一种方法是部署有效的数据保留和清理策略，积极地清除不再需要的信息。只要符合法规要求，人们有充分的理由来积极地删除信息。

安全性测试

关键要点：

- 向设备及任何其他软件系统应用安全测试技术。
- 利用代码分析、正面黑客攻击及其他技术，测试设备和设备端代码。
- 不利环境测试不仅涵盖物理不利环境，还包括不利的通信和网络环境。
- 倘若经测试验证，代码准确无误，攻击面必将会缩小。

在物联网实施中，安全漏洞测试是不可或缺的有机组成部分。软件系统测试中常用的安全测试技术也可用于测试 IoT 设备和基础架构。

所有 IoT 项目必须经过一系列测试，从而根据设计规范验证功能运作情况。这些测试包括：验证传感器设备中的安全机制和服务，以及验证与这些设备开展通信的基础架构。

我们可以分阶段开展测试：

- 单元测试，用于验证解决方案组件可否单独发挥设计的作用。
- 功能验证测试，用于验证复合解决方案的运行是否符合书面设计规范。
- 系统验证测试，用于验证整体解决方案环境中组件的集成性和运行状况。

所有测试阶段均可开展安全性测试。安全性测试可以借助自动化测试工具开展，如 IBM Rational® Software Analyzer[18] 和 IBM Security AppScan[19]。另外，也可运用采用正面黑客攻击技术的安全性测试。很多不同测试技术均可用于验证系统是否安全可靠。反复测试攻击抵抗能力至关重要，因为在产品和解决方案面世后，都可能会出现新的攻击。除在开发和质量保证阶段开展测试以外，还建议在生产过程中测试 IoT 系统。

设备会受到物理运行条件限制的影响，因此应该根据计算条件的限制，相应地调整这些设备。这些条件包括抵御拒绝服务攻击和干扰式攻击。在这类攻击中，攻击者会向设备发送大量信息，企图迷惑设备或使设备过载或瘫痪。

在适当的情况下，解决方案还需要经过外部分析和测试，包括通用标准 [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 可以研究和监控最新的互联网威胁趋势，面向 IBM 客户开发安全内容，并向客户和公众提出相关建议，帮助应对新兴威胁和重大威胁。

持续交付模式

关键要点：

- 在完成设备的生产、交付和部署之后，依然会发现各种问题和漏洞。
- 必需对正在使用中的设备端代码进行更新。
- 针对设备端代码，规划并利用持续交付技术。
- 在确定应用/发布/启动更新的时间时，必须考虑一些特殊因素。

敏捷和开发运营 (DevOps) 方法在软件行业十分流行，这是有一定道理的。借助这些方法企业可以及早向客户交付有用的功能、更快地收集用户反馈，以及更迅速地调整和更新这些功能。软件产品的交付更多地是一种持续的交付流程，而不是偶尔的产品发布、迁移规划及软件转换。随着基于服务的环境的出现，产品和功能能够以服务的形式予以交付，频繁更新“生产中”的产品便成为了一种新常态。

这种环境有利有弊。但是，功能的更新和交付成为了一个持续流程，并最终成为了一个“非事件”，人们便可以利用软件的部署和交付流程，应对交付产品中发现的相关安全问题。

形式多样的安全措施至关重要：预防、检测、反应和处理。过去，人们利用产品发布、补丁和修复等机制作出反应和处理，而现在，持续交付模式可以帮助更轻松地作出反应和处理。敏捷和

DevOps 方法中使用的很多技术同样可以用于 IoT 系统开发和交付。但是存在一个重要的区别：运行的代码和需要更新的代码并非存储于受控的数据中心或服务器环境中。这些代码运行于现场、路由器、网关、传感器及其他设备中。这些设备可能是移动设备，也可能是固定设备，可能始终保持联网状态，也可能偶尔联网，并且存储和计算能力也各不相同。不过，这些设备中依然有运行的代码，而且必然存在问题或漏洞，这在现场部署产品后将暴露无遗。鉴于不存在 100% 可靠的预防措施，因而必需通过无线方式 (OTA) 更新系统，从而解决发现的各类问题。

企业越早面向设备上运行的代码构建一个持续交付模式，就能越早越快地向客户交付功能，并频繁更新及添加功能。这种模式需要验证通过无线方式接收的更新，包括使用的代码签名和验证技术。这类技术并非新技术，但依然需要将其应用于系统/设备开发和部署领域。

在通过无线方式更新现场设备时，我们会面临一些独特的挑战，尤其是设备必须在更新时保持正常运行。不然，设备需要具备足够的逻辑，以便推迟更新的处理/应用，直至设备所处的位置、时间和环境适于应用更新为止。此外，设备必须具备故障自动保护退出机制，包括检查运行中的系统，撤销运行不稳定的变更。

很多设备都将开源软件作为设备运行代码的一部分。设备制造商应保留一份所用开源组件清单，以便在某个组件中出现漏洞时，能够快速向设备所有者/操作者提供更新。同时，设备制造商还必须与设备所有者/操作者建立通信流程，确保在发现漏洞时能够迅速做出响应。目前已有一些发布和应对此类漏洞的渠道，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

关键要点：

- 设备的交付综合覆盖整个供应链。
- 遵循现有指导原则，保护设备制造供应链。

一个可靠的供应链必须专注于如何有效管理设计、制造、运输、订单履行、进出口、知识产权管理、支持和维护。IBM 引领全球供应链安全性风潮，同时也是电子行业供应商行为守则组织 (Electronic Industry Supplier Code of Conduct) 的创始成员。此外，IBM 还参与制定了有关供应链安全的 Open Group[23] 标准。

一个可信的供应链应确保供应商遵循以下指导原则：

- 遵守明确的供应商行为守则和安全原则。
- 定期进行评估。
- 一经发现违规，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。
- 确保对软件和固件开发库和文件实施妥善的访问控制。
- 通过记录所有已交付组件的来源，提供来源认证。

安全风险评估是供应商评估流程的一个重要环节，其目的在于确定整个供应商风险的各个组成部分，包括产品风险、流程风险和业务风险。确定风险特征，可以帮助评估安全风险级别。风险缓解战略可纳入评估流程中。

保护制造和交付流程就是要保护流程、程序和供应链。保护制造流程也就是要保护生产环境的实际安全性，因为设备和系统都是在生产环境中生产出来的。一定要确保这些系统的生产环境的安全性。装配/生产线受到感染或威胁后，就可能会造成 IoT 设备出现漏洞。电子设备包含嵌入漏洞的例子不胜枚举。由于制造系统本身受到感染或受损，导致这些设备在制造时便带有嵌入式漏洞。

IBM 全球企业咨询服务部可以帮助众多行业优化、审计和保护供应链。

设备操作 - 安全运营强化设备

关键要点：

- 深层防御 - 在解决方案中设置多层防御机制。
- 设法隔离受损子系统，确保整个解决方案始终保持正常运行。

设备开发、测试和制造团队会全力预防设备出现故障，但历史表明，无论防护措施多么完善，设备总是会出现漏洞以及遭受攻击。抵御攻击的一种成功手段是采用深层防御技术。深层防御技术表现形式多种多样，包括数据中心的防火墙，以及家用路由器中的信息包过滤技术。设置多重防护不仅可以增加防御深度，还能用于隔离受损设备或系统。

为加强设备，或者更确切地说，是加强设备的运行环境，我们可以使用网关和路由器，将可能易受攻击的设备与网络的其他部分隔离开来。每个路由器和网关均可用于实现两端隔离。例如，对于网关另一侧的受损设备，人们可以利用网关隔离该设备发出的信息/数据/噪音。另外，对于在网关或路由器保护下运行的设备，网关或路由器还可用于阻止这些设备的大部分潜在网络通信。

在这些环境中，网关或路由器也是攻击目标。与网关和路由器保护的设备以及帮助它们传输信息的设备一样，网关和路由器也要遵循同样的加强型持续交付和无线更新的要求。

此外，网关和路由器也可以运用传感器数据反馈，充当网络的监控点，监控设备与基于服务的应用之间的通信状况。

如能制定和更新监管设备访问权限的策略，并定义适当和不当访问（入站访问或出站访问），势必会有所帮助。您可以考虑采用端点管理解决方案，掌控设备安全策略，如 IBM Unified Endpoint Management[24]。端点管理系统可能不适用于在小型或低功率的嵌入设备上运行，因而，应尽量将整个系统的端点设备都纳入管理范围之中。务必确保至少在网关中部署端点管理解决方案。

保护通信渠道

关键要点：

- 必须保障设备与系统之间通信渠道的安全。
- 网络类型和连接可能不足凭信。
- 遵守与每个现用协议相关的指导原则。
- 一般采用 SSL/TLS 保护 IP 通信。

IoT 系统会采用一系列不同的网络通信机制。这些机制包括采用低功率、小范围方法的局域网，如 Bluetooth、Bluetooth Low Energy (BTLE)、6LoPAN、Zigbee 等方法；也包括使用 WiFi 的局域网；以及使用 2G、3G 和 4GLTE 的广域网。

不同网络模型所提供的保护级别大相径庭，设备在穿越物理环境时可能得到的网络安全保护也各不相同。IoT 系统必须始终能够通过各种网络机制，建立安全的通信。

归根结底，IoT 系统中的通信通常分为两种：一种是通过 TCP 网络连接开展基于 HTTP（REST 式调用）的通信；另一种是通过 IP 网络堆栈实施某种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采用 UDP 模式（而非 TCP 模式），减少网络引发的连接或数据传输延迟。

不管是基于 HTTP 的模式，还是基于事件的模式，两者都会运用 SSL/TLS 来建立受保护的通信。此模式会综合运用加密算

法，建立安全的通信渠道。这样一来，设备、网关和云托管系统中运行的大部分逻辑都能建立安全的通信渠道，并专注于提供设备或应用功能。

审计和分析使用模式

关键要点：

- 预防措施并不能解决所有问题。
- 需要进行检测，以便做出反应和处理。
- 运用现有的日志分析技术，识别并响应异常情况。

在计算行业中，根本不可能预测乃至预防系统可能遭受的所有攻击。设计、实施和部署系统的过程中应充分考量安全性，但检测、响应和处理各种攻击场景同样至关重要。另外，计算行业的很多现有功能也可应用于 IoT 环境。

在管理计算环境时，必需监控系统行为、检测需要重点关注的场景，并响应相关场景。不仅要做出近实时响应，还需考虑实施长期分析和报告。此外，还亟需检测主动攻击，并对这些攻击做出响应。这些场景的起因可能是外部非法设备、来自内部的拒绝服务攻击，也可能是对环境中运行的一个或一组设备开展的持续攻击。通过主动监控系统使用模式，可以发现异常行为，进而采取相应的响应措施。部署系统监控工具后，只有在积极运用这些监控工具的情况下，才会高效发挥其作用。您必须监控和应对各种场景，而不单单是监控和记录事件。IBM Security QRadar® SIEM[25]（安全信息与事件管理）等工具便可提供此类审计和分析功能。

有些潜在威胁可能会持续很长一段时间。在这种情况下，我们必须观察系统行为，掌握常见或预期行为模式。必须主动监控系统，以便确定某些事件是否存在异常。如果设备运行/使用/发出的信息有悖于正常运行行为，那么可以通过异常检测技术，便可发现可能受到攻击的设备。IBM Operations™ Analytics - Log Analysis[26] 等工具可以提供长期监控环境所需的功能，从而确定系统是否与预期行为相符。

监控系统中发生的事件十分重要，包括通过网关、在设备、云端和数据中心托管计算服务中发生的事件。同时，还必需部署策略，审计整个系统的运行状况。此类审计更像是对监控者的监控，旨在防范内部攻击。建立主动审计流程后，若想攻击或破坏系统，必需多方串谋合作才能得逞。通过增加系统审计的人数或层级，可以提高保护级别。系统会定期记录所有访问尝试，并且这些日志会保留一段合理时间，一旦日后需要了解攻击和潜在泄露程度，便可进行取证。

不断更新安全环境

关键要点：

- 安全环境防护包含若干层面：身份验证、授权、审计、管理、加密/解密、密钥管理和完整性检查。
- 综合运用技术和流程，确保环境始终安全。
- 与数据中心、云端或其他受控环境中运行的系统相比，设备运行环境的控制程度更低。

安全的 IoT 应用环境的创建和维护，与组织所有计算系统的安全计算环境息息相关，并且依赖于后者。身份验证、授权（访问控制）、审计和管理等元素也是如此。另外还面临一项挑战：当与用户、群组、移动设备及端点进行互动时，所用设备的数量较过去高出若干数量级。端点设备与组织的工作人员相互关联。在 IoT 世界中，人们需要考量许多端点，以及各种安全支持功能。

除用户和设备注册、身份验证和访问控制以外，还必需管理用于建立身份验证、通信和数据存储加密与解密机制的密钥。密钥管理一直延伸至 IoT 设备，旨在保护信息安全地从源头流至终点，不论信息处于流动状态还是静止状态。利用 IoT 设备内可信平台模块 (TPM) 中的内置私钥数据，可以帮助实施密钥管理。可信计算组织 (TCG)[27] 已经制定并改进了有关 TPM 设备的规范。

IBM Identity Management[28] 解决方案的功能，包括在使用 IBM Bluemix[29] 时运用 IBM Identity，可以帮助针对与开发的 IoT 解决方案相关的用户/群组定义，不断更新安全环境。此外，IBM IoT Foundation[30] 提供支持设备注册和生命周期的功能，这些功能是维持安全环境所需的基础功能，可以保护设备以及通过设备进行通信的应用。其中包括上文所提到的安全设备注册功能。

人们可利用 IBM Security Key Lifecycle Manager[31] 功能，深入认识加密密钥管理和分配所需的核心功能集。尽管该产品主要应用于金融服务环境，但这些功能旨在将密钥管理融入设备级加密服务中。鉴于基于 OASIS 密钥管理互操作性协议 (KMIP)[32]，密钥管理可扩展至分布式网络环境中运行的各类设备。IBM 加密磁盘驱动器便是采用这种模式的首个设备。KMIP 协议的设计尽量保持简洁。KMIP 协议可以在各种网络设备和计算设备中实施并提供支持。

除管理身份和加密密钥信息以外，还必须管理和维护环境中的所有设备。必须定期更新设备、网关、路由器及其他基础架构，从而应用各种安全补丁和修复程序。过去，人们必需进行大量人工干预才能直接与设备、网关或路由器进行交互，以便执行固件或软件升级、修复或迁移。未来，鉴于设备数量和预期更新频率持续增加，这项工作将从主动人工干预转变为自动无线更新处理模式。

到时，只有在处理异常情况时才需要人工干预，而不是人工处理每次更新。这意味着，企业的监控和报告能力将会更上一层面，更有效地监控和报告网关、路由器和设备库存的更新处理状态和进度。

鉴于随着时间推移，互连设备的价格会不断变化，因此，没有必要一直更新所有设备，或者保护每一台设备免受所有攻击。相反，在这种情况下，最经济高效的管理方法是不再考量相关设备，并配置网关，忽略/过滤设备发出的信息。此外，设备制造商应考虑添加“自毁开关”型功能。在故障自动保护模式或最低运营断开模式下，设备仍能正常运行，但不会再接入网络，从而保护自身和其余环境部分的安全。尽管设备发出的传感器信息可能会丢失，但这可以保护系统免受潜在攻击，设备无法修补/修复也就是消除了一个漏洞。

我们在这份报告的前文中曾指出，若要不断更新安全环境，就需要设备制造商参与并响应安全事件报告，这一点与其他联网计算设备并无二致。

与计算环境中的其他任何部分一样，我们必须考虑在整个环境中解决登录/密码信息的积极管理和更新问题。其中就涉及到积极管理可能嵌入 IoT 设备的这一类信息。这包括以下层面：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，还要考量与互连设备有关的多个利益相关方：设备制造商、设备采购者/所有者/管理者以及设备用户。此外，还需要考虑潜在的第三方，例如网络通信提供商、设备服务和支持承包商。

打造值得信赖的维护生态系统

关键要点：

- 遵循现有指导原则，创建和维护安全环境。
- 制定综合全面的事件响应流程。

为运行安全的 IoT 系统，必需监督环境运营负责人，确保他们开展安全适当的活动。有关详细信息，请参见供应链保护部分，供应链包括运营环境时所聘请的承包商。必须遵循适当的维护程序，从而保持系统的安全性和完整性。

为处理安全事件报告，我们必须制定明确清晰并经过沟通的事件响应流程。该流程必须确保在发现并确认事件后，具备弥补漏洞的结构化补救计划。另外，这项流程还必须确保向可能受漏洞影响的其他组件所有者通报情况，以便他们执行补救计划。通过重复使用组件与构建解决方案，事件响应流程必须能够确保快速辨别并补救所有可能受影响的组件。

整体 IoT 系统的实际安全性仍将是一项重大挑战。就其本质而言，IoT 设备的运营环境必然十分严苛，并且会面临大量物理元素，以及各类攻击。这些设备在网络环境中运行，会不时快速移动，而且还会受到极端条件的影响。尽管对于大规模高科技电子部署项目来说，这是一个全新的领域，但其实并非什么新鲜事物。军事应用、车载系统、机载航空电子设备和传感器以及目前为保护移动设备而创建的各种系统均为我们指明了方向，为我们带来了各种值得借鉴的实践。

总结

物联网技术的安全性与其他大规模计算基础架构的安全性既有不同之处，也有相似之处。两者面临的问题相似，并且用于解决问题的技术也十分相似，包括身份验证（设备、系统/应用和用户）、授权、审计、管理、加密/解密、数据完整性和密钥管理等技术。同时，还面临着一些新的挑战 - 计算设备的类型和功能更为多样、运行环境的控制度更低，而且需要保护的攻击面更多。

IoT 安全方面的挑战不断涌现。但是，我们可以运用经多年优化的研发技术成果，应对这些挑战，并对这些技术实施必要扩展，以便满足物联网的独特需求。

贡献者

《IBM 观点：物联网 (IoT) 安全》是全体 IBM 人员精诚合作的成果。在此感谢下列人员为本白皮书的发表所付出的努力和贡献。

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

了解更多信息

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

参考文献

1 IDC, ” Worldwide and Regional Internet of Things 2014-2020 Forecast Update by Technology Split,” 文档编号：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。《计算机世界》。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) 十大 IoT 问题。http://www.owasp.org/index.php/OWASP_Internet_of_Things_Top_Ten_Project

5 IIC 参考架构。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 季度威胁情报（2014 年第四季度）” ；文档编号：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 Common Criteria. 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/

IBM Corporation Software
Group Route 100
Somers, NY 10589

美国印刷
2015 年 4 月

请回收利用

RAW14382-CNZH-00