物联网 M2M 的安全分析及策略

晁世伟[1] 杨 元[2] 李静毅[3]
(重庆邮电大学通信学院 重庆 400039)[1] (重庆市电力公司 重庆 400014)[2]
(重庆邮电大学计算机学院 重庆 400039)[3]

摘 要 物联网 M2M 的先进理念引来了新一轮的"无线革命",也暴露出物联网的安全隐患。在此以 M2M 的前端传感器及设备、网络和末端 IT 系统三个部分为出发点,提出了从十三个方面来分析物联网所面临的安全隐患问题,并大胆提出了相应的解决策略。

关键词 物联网,M2M,物联网机器/感知节点,安全,攻击
中图法分类号 TP309 **文献标识码** A

Security Analysis and Strategy for M2M of IOT

CHAO Shi-wei[1] YANG Yuan[2] LI Jing-yi[3]
(School of Communication Chongqing University of Posts and Telecommunications, Chongqing 400039, China)[1]
(Chongqing Electric Power Company, Chongqing 400014, China)[2]
(School of Computer, Chongqing University of Posts and Telectommunications, Chongqing 400039, China)[3]

Abstract The advanced idea of M2M technology attracts one new round of "wireless revolutions", and also exposes the potential security hazard of Internet of Things. So, in this case, M2M's structure, consists of front-end sensors and equipment, networks, back-end IT systems, will become a starting point to analyze the possible potential security threats, those are Internet of Things faced, from thirteen parts which is to proposed in this paper, aggressively proposed their corresponding solutions and strategies.

Keywords Internet of things, M2M, Internet of thing machine/perception nodes, Security, Attack

1 前言

无处不在的计算和环境智能[1]的新技术领域不仅给我们带来了具有计算能力的物理环境,还扩展了周围物体设施的智能化。并且已经实现了从 Web2.0 的 Smart Place [2]到物体对象之间可以相互交流的智能对象的转变。其中物联网的 M2M 技术就是后者的前驱。然而 M2M 技术正演变成为一种用来监控和控制全球行业用户资产、机器和生产过程所带来的高性能、高效率、高利润的方法,同时具有可靠、节省成本等特点。无线 M2M 方案的无限潜力意味着整个市场将准备经历接下来几年的爆炸性的增长。

据法国 IDATE 调研数据显示,到 2010 年,全球将有超过 4000 亿台机器装设行动传输功能,让机器与机器进行数据传输,取代人力控制、操作的成本,整体市场规模将远远超过以个人为主的市场。而在国内,有专家预测 M2M 市场增长速度会高于国际市场 30%的增长率[3]。

2 物联网 M2M

物联网中最主要的核心部分就是机器之间的互联、互通;

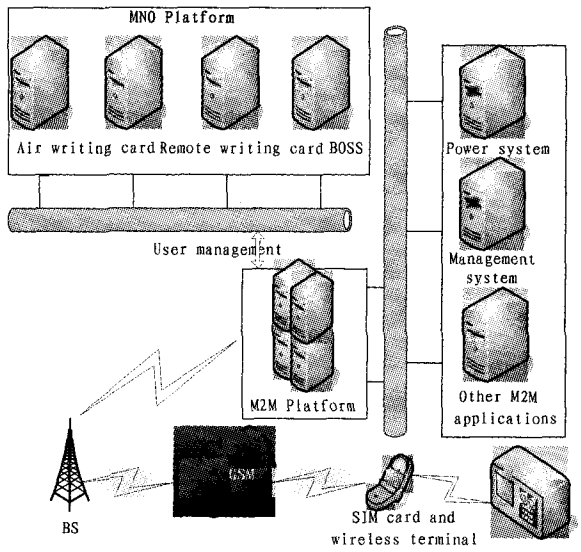

图 1 物联网 M2M 的系统结构框图

也就是通常说的 M2M(见图 1)。M2M 是所有增强机器设备

也就是通常说的 M2M(见图 1)。M2M 是所有增强机器设备

通信和网络能力技术的统称,它将机器之间的通信、机器控制

本文受信息内网应用服务安全监管策略及其关键技术研究基金资助。
晁世伟(1985—),男,硕士生,主要研究领域为信息安全,E-mail:cswdhy06@163.com;李静毅(1988—),女,硕士生,主要研究领域为信息安全。

通信、人机交互通信、移动互联通信等多种不同类型的通信技术有机地结合在一起，让机器、设备、应用处理过程与后台信息系统共享信息，并与操作者共享信息。M2M[4]这一概念来自英文“Machine to Machine”，即“机器对机器”的缩写，扩展的概念包括“Machine to Mobile ”——“机器对移动设备”、“Man to Machine”——“人对机器”等，主要是指通过无线网络传递信息和后端的服务器网络来实现机器对机器或者机器对移动设备或者人对机器的实时数据交换，也就是机器互联、互通。

3 M2M 存在的安全隐患及策略

物联网是一种虚拟网络与现实世界实时交互的新型系统，其发展的初级阶段是 M2M。M2M 由前端的传感器及设备、网络、末端的 IT 系统构成[5]。由此可知，在没有人机直接交互的情况下实现远程管理 M2M 设备和传输数据的信息安全问题是物联网 M2M 面临的最大的安全挑战。

下面分别从 3 个方面来分析物联网 M2M 存在的信息安全问题。

3.1 前端的传感器及设备部分的安全隐患及策略

前端传感器及设备通过内置的传感器获得数据，并通过 M2M 使设备或模块进行数据传输，实现多个传感器的联网服务。这样就会涉及到机器与节点连接和业务实现的安全问题。

3.1.1 物联网机器/感知节点的本地安全威胁及分析

由于物联网机器/感知节点[6]多数部署在无人监控的场景中，那么攻击者就可以轻易地接触到这些设备，从而对它们造成破坏或者通过本地操作进行非法操作。

M2M 终端设备与服务网之间的无线接口可能面临的威胁及分析：

(1)非授权访问数据

攻击者可以窃听无线链路上的用户数据、信令数据和控制数据，窃取暴露在公共场合中的信号，从而获取 M2M 用户密钥或控制数据等机密信息，非法访问 M2M 设备上的数据。

因此应设计健壮性好的设备与网络的双向认证机制以及相应的加密算法，使得攻击者无法窃听或非授权访问无线链路上的数据。

(2)对完整性的威胁及分析

攻击者可以修改、插入、重放或者删除无线链路上传输的合法的 M2M 用户数据或信令数据，对 M2M 用户交易信息造成破坏。

因此应该加强完整性保护机制，M2M 设备传输用户数据时需进行完整性加密保护。

(3)拒绝服务攻击

攻击者通过在物理层或协议层干扰用户数据、信令数据或控制数据在无线链路上的正确传输，实现无线链路上的拒绝服务攻击。

因此应设计健壮好的协议算法以对抗拒绝服务攻击，或设计追踪机制以快速确定攻击者的位置，减少攻击者对网络的破坏。

3.1.2 物联网业务的安全威胁及分析

由于物联网设备可能是采用先放置部署后连接网络的方式布置，而物联网节点又无人看守，因此如何对物联网设备进行远程签约信息和业务信息配置就成了难题。M2M 通信终端很少是有人直接参与管理的，因而存在许多针对 M2M 终端设备和签约信息的攻击。

(1)盗用 M2M 设备或签约信息攻击及分析

M2M 设备一般情况下是无专人看管的，这就不可避免地会有不法者破坏 M2M 设备，盗取 USIM 或 UICC 甚至 M2M 设备，从而窃取或篡改 M2M 设备中的用户签约信息，给被攻击用户造成一定的损失。

因此 M2M 设备应具备特殊的功能和相关的安全机制来防止签约信息被窃取，使合法 M2M 用户的损失降到最低，同时能够防止攻击者通过逻辑或物理方式进行攻击。

(2)破坏 M2M 设备或签约信息攻击及分析

攻击者可能直接破坏 M2M 设备或 UICC，造成签约信息或 M2M 设备丢失或者破坏，或者通过其他攻击方式造成签约信息丢失或者破坏。此外，攻击者还可以通过向 M2M 设备中添加恶意信息导致签约信息丢失或者破坏。

为防止签约信息与安全应用被非法修改或破坏，M2M 设备还应当保证在添加和修改签约信息时需要通过网络进行认证。

3.2 网络部分的安全隐患及策略

网络的职责是提供更全面的互联互通能力，提供连接的有效性和经济性，以及可靠的服务质量。由于物联网中节点数量庞大，且以集群方式存在，因此会导致在数据传播时，由于大量机器的数据发送使网络拥塞，产生拒绝服务攻击。

(1)非授权访问数据威胁及分析

攻击者可以进入服务网窃听用户数据、信令数据、控制数据以及没有经过授权访问存储在系统网络单元内的数据，甚至可以进行被动或主动的流量分析。

对于非授权访问数据的行为，应使用非人为可控的三方认证技术[7]，即合址认证或者设计好的设备与网络双向认证机制以及相应的加密算法，使得攻击者无法窃听或非授权访问服务网络上的数据。

(2)非授权访问服务威胁及分析

攻击者可能会冒充合法用户使用网络服务，也可能冒充服务网以利用合法用户的接入尝试获得网络服务，从而获得非授权的网络服务。

要防止非授权的访问服务，首先要保护 M2M 设备的签约信息不被盗用。其次，设计授权和相互认证机制[8]确保只有授权的 M2M 设备才能接入服务网络，同时要确保只有认证通过的服务网络才能为 M2M 用户提供服务。

(3)窃取、更改通信信息威胁及分析

攻击者常通过物理窃取、在线侦听、伪装成合法用户等手段来获取、修改、插入、删除或重放用户通信信息，如中间人攻击[9](Man—in—the—Middle Attack)，这种攻击可以在“拦截数据—修改数据—发送数据”[10]的过程中窃取或更改 M2M 设备间的通信信息，从而造成合法用户的损失。

通常，攻击者会想方设法获取通信中的数据，如采用在线

侦听、MITM[12]攻击等，因此 M2M 设备间通信的数据需要受到完整性和机密性保护，M2M 设备应具备相应的机制来完成这种功能。

(4)拒绝服务攻击威胁及分析

攻击者通过在物理层或协议层干扰用户数据、信令数据或控制数据的传输，来实现网络中的拒绝服务攻击；还可以通过假冒某一网络单元来阻止合法 M2M 用户的业务数据、信令数据或控制数据，从而使合法 M2M 用户无法使用正常的网络服务。

应设计健壮性好的协议算法抵制或减轻拒绝服务攻击，或设计追踪机制快速确定攻击者的位置[11]，减少攻击者对网络的破坏。

(5)病毒、恶意软件的攻击

攻击者可以通过恶意软件、木马程序或其他手段获取 M2M 上的应用软件、签约信息，然后在其他 M2M 设备上复制还原，从而冒用 M2M 用户的身份；还可以通过病毒或恶意软件更改、插入、删除用户的通信数据。

防病毒软件的应用会减轻病毒和恶意软件等对 M2M 设备的破坏，M2M 设备应能够定期更新防病毒软件。

(6)网络连接的安全分析

4 大类(有线长、短距离和无线长、短距离)网路相互连接组成的异构(heterogeneous)、多级(multi-hop)、分布式网络导致统一的安全体系难以实现“桥接”和过渡[13]。数据的传输被阻止，不能到达服务末端，攻击者就可以通过在线侦听或物理窃取用户数据、信令数据或控制数据，从而非法访问。

3.3 末端 IT 系统的安全隐患及策略

后端的 IT 系统的责任是提供更深入的智能化能力。它在形态上可以为网关、应用或中间件，它具有较高的安全性要求，可以实时或准实时地收集、分析传感器数据，增加商业智能。

(1)码号资源的安全管理

物联网系统的安全主要有 8 个尺度[14]：读取控制、隐私保护、用户认证、不可抵耐性、数据保密性、通讯层安全、数据完整性、随时可用性。其中“隐私权”和“可信度”(数据完整性和保密性)问题在物联网体系中尤其受关注。

因此在物联网中的每一个物体都分配一个独立的编码，以增加可信度和安全性。为了解决码号资源的安全管理，可使用机卡安全认证解决方案[15]。机卡安全认证解决方案利用了终端的 IMEI(International Mobile Equipment Identity 是国际移动设备身份码的缩写)号和 SIM 模块的 IMSI(国际移动用户识别码 international mobile subscriber identity)进行机卡绑定，同时通过 M2M 鉴权认证平台进行机卡互锁管理，平台定期下发更新密钥，这样就能防止盗卡、盗机现象的发生，确保了码号资源的安全性。

(2)更换运营商时的安全隐患

由于运营商间竞争的存在，在 M2M 用户选择新运营商后，其证书信息及密钥在运营商间进行交换时可能会面临一些不正当行为的威胁，造成用户交易信息泄露，给用户造成经济损失。

对于此种威胁，政府应制定相应的法规来规范运营商的行为，并充分利用签约合同来降低切换运营商时的风险。此外，运营商也应提供专门的进程来进行切换运营商时密钥等用户信息的传输，确保用户信息的安全。

结束语 M2M 已经渗透至日常生活的各个方面，并形成一定的产业规模。目前 M2M 广泛应用于电力、交通、工业控制、零售、公共事业管理、医疗、水利、石油等多个行业，可以实现车辆防盗、安全监测、自动售货、机械维修、公共交通管理等功能，包括异常重要的个人隐私和各行各业的信息安全，这更能说明对物联网 M2M 的安全机制研究的重要性和必要性。

参 考 文 献

[1] Weiser M. The Computer for the Twenty-First Century[J]. Scientific American, 1991, 265(3): 94-104

[2] Ahola J. Ambient Intelligence[J]. ERCIM News, 2001(47) http://www.ercim.org/publication/Ercim_News/enw47/intro.html, 2001

[3] International Telecommunication Union UIT[R]. ITU Internet Reports 2005: The Internet of Things. 2005

[4] Dai Guo-hua, Li Bao-rong, Liu Zhao-yuan. M2M Industry Development Status and Problems [P]. Guangzhou Research Institute of China Telecom Co., Ltd. 2008

[5] 3rd Generation Partnership Project(3GPP). (2007, Mar.). Study on facilitation of machine-to-machine communication in 3GPP systems[R]. 3GPP Tech. Rep. 22, 868, version 8.0.0[OL]. ftp.3gpp.org/Specs/archive/22_series/22, 868/22868-800.zip

[6] 朱红儒，齐曼鹏. 物联网面对的安全问题[J]. 中国移动研究院，2009

[7] Liu Xiao-peng. Internet of things in information security. 2010

[8] Leicher A, Kuntze N, Schmidt A U. Implementation of a trusted ticket system[C]// Proc. IFIP Int. Information Security Conf SEC2009. Boston, MA, to be published

[9] Brickell E, Camenisch I, Chen L. Direct anonymous attestation [C]// Proc. 11th ACM Conf. Computer and Communications Security. 2004: 132-145

[10] Camenisch J. Better privacy for trusted computing platforms[C]// Proc. 9th European Symp. Research in Computer Security(ESORICS'04). 2004: 73-88

[11] Jiao Wen-juan, Qi Man-peng, Zhu Hong-ru. M2M in security research[J]. Telecommunications Technology, 2009(6)

[12] Chaum. Security without identification: Transaction systems to make big brotheer obsolete[J]. Commun. ACM, 1985, 28(10): 1030-1044

[13] KoolSpan TrustChip Solution for OEMs[OL]. http://koolspan.com/oem/trustchip_hardware.htm

[14] Chaum. Security without identification: Transaction systems to make big brotheer obsolete[J]. Commun. ACM, 1985, 28(10): 1030-1044

[15] Shu Gu-wang, Huang Hai-dong. Trends of Internet of things M2M[J]. Data in China, 2010