物联网系统安全检测与检查方法研究

李海涛　李程远　范　红
(公安部第一研究所　北京　100048)

[摘　要] 随着物联网技术得到广泛应用,物联网系统面临着多方面的安全威胁。因此,物联网系统安全检测与检查需求迫切。本文从系统安全检测、风险评估和集成化安全管理三个方面对物联网系统的安全检测、检查方法进行研究。
[关键词] 物联网系统 安全检测 风险评估 安全检查
[中图分类号] TN918

Research on Security Test and Check Method of IoT System

Li Hai-tao　Li Cheng-yuan　Fan Hong
(The First Research Institute of the Ministry of Public Security　Beijing　100048)

[**Abstract**] With the wide application on the internet of things (IoTs) technology, the IoT systems are confronted with various security threats. There are eager demands on Security test and check of IoT System. In this paper, we have researched on Security test and check method of IoT System from system security test, risk assessment and integration security management.
[**Keywords**] internet of things system; security test; risk assessment; security check

1　引言

目前在全球市场的数据统计分析上看,物联网成为未来 10 年发展迅猛的行业。据美国市场研究公司 Forester 预测,到 2020 年,世界上“物物互连”的应用业务,跟人与人之间通信的业务相比,前者是后者的 30 倍,仅在智能电网和机场入侵检测系统方面的市场就有上千亿美元。因此“物联网”必将成为下一个万亿美元级的信息技术产业。

从经济发展角度看,各国齐头并进,相继推出物联网区域战略规划。当前,世界各国的物联网基本都处于技术研究与试验阶段,美、日、韩、欧盟等都正投入巨资深入研究探索物联网关键技术。

物联网是互联网在现实世界的延伸。随着应用的不断扩展,物联网一旦发生安全问题,极有可能在现实世界造成电力中断、金融瘫痪、社会混乱等严重危害公共安全的事件,甚至将危及国家安全。由于物联网感知节点和传输设备具有能量低、计算能力差、运行环境恶劣、通信协议庞杂等特点,使得传统安全技术无法直接应用于物联网,由此引发众物联网特有的安全问题。

物联网安全问题如果得不到有效解决,将严重阻碍物联网产业发展。目前物联网安全技术和安全状况缺乏有效的检测和评价手段,已有的物联网应用急需对其安全性能的检测和技术支持。所以,对物联网安全检测与检查方法的研究是解决物联网安全问题必不可少的关键工作。

2　物联网系统面临的安全威胁

从安全测评的角度来看,物联网系统的结构可以分为三层,即智能感知层、接入传输层和业务应用层。物联网面临的安全威胁也来自这三个层次。

由于网络环境的不确定性,感知节点面临着多方面的威胁,感知节点本身就是用于监测和控制各种感知设备。节点对各种检测对象进行监测,从而提供感知设备传输的数据信息来监控网络系统的运行情况。这些智能传感器节点是暴露在攻击者面前的,最容易被攻击。因

此，与传统的 IP 网络比较，所有的监控措施、安全防范策略不仅面临着更复杂的网络环境，而且还有更高的实时性要求。物联网系统面临的主要威胁有几个方面。

（1）安全隐私 射频识别技术被广泛用于物联网系统中，RFID 标签可能被嵌入到任何物体中，例如人们的生活和生产用品。但是这些物品的拥有者不一定能够了解相关情况，会导致该对象的拥有者被随意地扫描、定位和追踪。

（2）伪造攻击 与传统 IP 网络相比，传感设备和电子标签都是裸露在攻击者面前的。与此同时，接入传输网络中有一部分是无线网络，窜扰问题在传感网络和无线网络中是普遍存在的，而无线安全研究方面也显得非常棘手。因此，在网络中这些方面面临的伪造节点攻击很大程度上威胁着传感器节点的安全，从而影响整个物联网安全。

（3）恶意代码攻击 恶意代码在接入传输层和传感层中都可以找到很多可以攻击的突破口。对攻击者而言只要进入到网络，通过传输网络进行病毒传播就变得轻车熟路，而且具有较强的隐蔽性，这一点与有线网络相比就更加难以防御。例如类似蠕虫这样的恶意代码，本身又不需要寄生文件，在这种环境中检测发现和清除恶意代码的难度是非常大的。

（4）拒绝服务攻击 这种被熟悉的攻击方式，一般发生在感知层与接入传输层衔接位置的概率是非常大的。由于物联网中感知节点数量庞大，而且多数是以集群的方式存在，因此信息在网络中传输时，海量的感知节点信息传递转发请求会导致网络拥塞，产生拒绝服务攻击的效果。

（5）信息安全 感知节点一般都具有功能单一、信息处理能力低的特点。因此，感知节点不可能具有高强度的安全防范措施。同时因为感知层节点的多样化，采集的数据、传输的信息也就不会有统一的格式，所以提供统一的安全防范策略和安全体系架构是很难做到的。

（6）接入传输层和业务应用层的安全隐患 在物联网系统的接入传输层和业务应用层除了面临传统有线网络的所有安全威胁的同时，还因为物联网在感知层所采集数据格式的不统一，来自不同类型感知节点的数据信息是无法想象的、并且是多源异构数据，所以接入层和业务应用层的安全问题也就更加繁杂。

通过对各行业物联网建设方面的调查发现，当前已有的物联网应用对其安全性能的检测和技术支持需求十分迫切，例如移动系统与行业网的接入安全性评估和检测、社会公共安全的视频采集系统的接入安全检测、基于 RFID 和车牌识别的智能车辆管控系统安全性评估等检测业务都是亟待解决的问题。由此看出，物联网安全检测和检查方法研究需求迫切。

为了把物联网系统安全风险降到最低，应该做到系统建设与检测检查同步进行，且检测检查过程中要技术与管理并重。本文将从物联网系统安全检测、物联网系统风险评估和物联网集成化安全管理三个方面进行检测、检查的方法研究。

3 物联网系统安全检测

安全检测是以系统检测方式对物联网系统三层架构的各个层面进行安全符合性和有效性检测。

（1）智能感知层应该对访问控制策略配置、身份认证策略配置、数据完整性保护策略配置、数据保密性保护策略配置、感知节点抗攻击性、安全审计策略配置和物理安全进行符合性测试。

（2）接入传输层检测应该对 AKA 机制的一致性或兼容性、跨域认证和跨网络认证、视频传输协议转换前后的安全性；传统认证和数据交换安全、无线认证网关安全、无线传输协议、身份认证安全等进行符合性和有效性检测。

（3）业务应用层应该对数据库安全、应用系统和网站安全、应用系统稳定性、业务连续性以及应用模拟等进行符合性和有效性检测。

下面从物联网系统检测规则和检测工具两个方面研究物联网系统安全检测方法。

物联网系统检测规则由三个部分组成分别是智能感知层规则、接入传输层规则和业务应用层规则。

（1）智能感知层规则主要包括访问控制、身份认证、数据完整性保护、数据保密性保护、抗攻击、安全审计以及物理安全等安全规则。

（2）接入传输层规则包括数字接入系统中接入业务可管理性、可控性、信息保密性、完整性和可用性的规则要求，视频接入系统实现外部视频资源单向传输至内网，视频控制信令和数据的会话终止于应用服务区，包含对视频信令格式进行检查及内容过滤、合法的协议和数据通过、视频数据和视频控制信令安全传输等方面的规则，无线接入系统接入内网，需要与内网的各种信息系统交互信息，包含敏感信息、数据完整性保护、数据保密性保护、抗攻击、安全审计以及物理安全等方面的规则。

(3)业务应用层规则一般包括访问控制、用户身份鉴别、资源控制、安全漏洞、安全审计以及数据备份等安全规则。

检测工具是包含物联网系统安全检测中所有测试工具、测试样本数据的集合。检测工具根据其应用范围可以划分为三类。

(1)智能感知层检测工具:主要包括对感知操作安全项目进行检测所用到的软硬件工具和测试样本数据;感知数据处理安全检测工具包括对感知数据处理安全项目进行检测所用到的工具;感知数据存储安全检测工具主要包括感知数据存储安全项目进行检测所用到的工具和测试样本数据;感知节点设备安全检测工具主要包括漏洞扫描工具、自动化攻击工具以及自身所建立的漏洞补丁知识库,根据被测设备的操作系统、功能组件,查询漏洞补丁知识库,可以发现漏洞扫描类工具无法直接探测的隐藏漏洞。

(2)接入传输层检测工具:主要包括脆弱性扫描与管理工具、网络协议分析工具、主机配置检测工具、网络边界检测工具等。

(3)业务应用层检测工具:主要包括 Web 应用系统及网站安全检测工具、数据库脆弱性检测工具和网络终端安全检测工具等。

4 物联网系统风险评估

物联网系统风险评估主要针对物联网智能感知层、接入传输层和业务应用层中所包含的各个组成部分。开展物联网系统风险评估工作,需要构建物联网系统风险评估平台,对物联网可能遭受到的威胁和脆弱性进行安全分析,然后根据安全事件的可能性以及安全事件造成的损失计算出风险值、对安全事件进行风险等级定级,最后结合安全事件所涉及的资产价值来判断安全事件一旦发生对物联网系统造成的影响。

下面从物联网系统风险评估知识库和风险评估工具两方面来研究物联网系统风险评估方法。

风险评估知识库应该包含威胁库、脆弱性库、风险分析方法和评估案例等。物联网系统风险评估服务威胁库包括智能感知层威胁库、接入传输层威胁库和业务应用层威胁库:智能感知层威胁有 RFID 安全隐私、RFID 标签复制、传感网安全路由、感知节点逐跳加密安全等;接入传输层威胁有海量数据融合信息窃取、海量数据传输安全、三网融合面临的新威胁等;业务应用层威胁有位置信息泄露、数据融合后机密信息泄露、应用系统漏洞等。脆弱性库,脆弱性识别时的数据应来自于资产的所有者、使用者,以及相关业务领域和软硬件方面的专业人员等。风险分析方法主要包括系统层次分析方法、基于概率论和数理统计的方法、模糊数学方法,这些方法或是在识别风险的基础上,进一步分析已识别风险,提高风险结果可信度,或是融入风险评估过程中,使评估过程更科学、更合理。

如果物联网系统风险评估案例库建立实际风险评估案例,能够给出风险分析方法、风险分析过程。系统整体风险评估结果就能一目了然,也为物联网系统风险评估工作提供参考案例。

根据在风险评估过程中的主要任务和作用原理的不同,风险评估工具可以分成风险评估与管理工具、系统基础平台风险评估工具和风险评估辅助工具三类。

(1)风险评估与管理工具应该是一套集成风险评估各类知识和判定依据的管理信息系统,以规范风险评估的过程和操作方法,或者用于收集评估所需要的数据和资料,基于专家总结的经验,对输人输出进行自动化的模型分析。

(2)系统基础平台风险评估工具主要用于对信息系统的主要部件(如操作系统、数据库系统、网络设备等)的脆弱性进行分析,或实施基于脆弱性的攻击。

(3)风险评估辅助工具则实现对数据的采集、现状分析和趋势分析等单项功能,为风险评估各要素的赋值、定级提供依据。

5 物联网集成化安全管理检查

目前监管体系对不同的物联网系统的防护管理要求存在没有差异和缺乏针对性等问题。因此,物联网集成化安全管理势在必行。根据物联网的技术特点,针对物联网面临的安全威胁,应该构建和完善物联网的监管体系,从防范阻止、检测发现、应急处置、审计追查和集中管控五个方面,对物联网系统感知层、接入传输层和业务应用层进行安全防护管理。

(1)防范阻止主要指物联网系统应该具有安全防护和阻止信息安全威胁影响的措施,从而有效防范本文中提到的安全威胁。从物联网的体系结构而言,物联网除了面对 TCP/IP 网络、无线网络和移动通信网络等传统网络安全问题之外,还存在着大量自身的特殊安全问题。因此数据完整性和保密性保护、身份认证、访问控

制、安全审计等方面的安全措施必不可少。

(2)检测发现主要是指物联网系统应该能够检测发现物联网系统存在安全隐患，其中包括感知层检测、接入传输层检测和业务应用层检测，在感知层应能检测发现感知设备伪造攻击。由于感知设备是“裸露”在攻击者面前的，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，甚至通过本地操作更换机器的软硬件。接入传输层应包括边界接入系统、视频接入系统和无线接入系统三类接入传输系统的安全管理要求。业务应用层应能检测发现业务应用中的安全隐患，因为TCP/IP网络的所有安全隐患都同样适用于物联网。同时应能针对物联网感知层、接入传输层、业务应用层三个层次进行风险威胁分析，形成反映物联网系统安全态势的总体视图。因为安全系统从隐患到影响是一个态势变化的过程，因此对物联网系统态势的分析与威胁防范同样重要。

(3)应急处置主要是指应该能够具有高效指导系统维护人员开展应急处置工作的措施，应制定物联网信息安全应急预案，并结合实际工作情况，对物联网信息安全应急预案做出相应修订。应明确现场总指挥、副总指挥、应急指挥中心以及各应急行动小组在应急救援整个过程中所担负的职责。应明确完成应急救援任务应该包含的所有应急程序，以及对各应急程序能否安全可靠地完成对应的某项应急救援任务进行确认。应急预案应具备实用性、可操作性、完整性和可读性的特点。

(4)审计追查主要是指应该能够为安全管理人员提供物联网系统安全事件倒查的措施，包括日志采集、查询、分析和追查。其中采集应能对分布在感知层、接入传输层和业务应用层各个部分的用户和管理员操作日志进行采集。查询应能对物联网信息系统日志进行查询，包括常规查询、条件查询和权限控制查询。分析应能根据统计需求，对物联网信息系统日志进行统计分析。追查应能根据追查安全事件需求，为安全管理人员提供安全事(案)件的倒查手段。

(5)集中管控主要是指应该能够为物联网系统自身安全管理和控制提供技术手段。它们包括集中监控、策略管理、运行监控、异常和用户监控，其中集中监控应能通过监控中心对物联网系统进行集中管控，包括系统安全管理和监控。策略管理应能对感知层、接入传输层和业务应用层的安全策略进行集中管理，支持管理感知节点的备份与恢复。运行管控应能对感知层终端运行情况进行监控，对物联网系统运行情况进行监控。异常和用户监控应能对业务应用层异常进行监控，能对系统用户的操作进行监控。

6 结束语

随着物联网产业的迅猛发展，信息安全问题也面临着新的挑战，所以安全作为物联网领域的核心问题，没有完善的安全保护和测评措施，物联网就无法被广泛地应用，这就会对物联网优势的发挥产生严重的影响。

本文在分析了物联网系统面临安全威胁的基础上。根据物联网技术特点，针对面临的安全威胁，从物联网系统安全检测、物联网系统风险评估和物联网集成化安全管理三个方面进行检测和检查的研究。从而进一步明确在物联网的建设中，物联网应用不仅要投入巨资深入研究系统构建技术，还需要做到安全保障与物联网建设齐头并进，避免先应用后安全的被动局面，增强物联网主动保障能力，提高物联网安全检测能力，扩大安全检测和检查应用范围，为推进我国物联网安全检测标准化进程提供保障，使得物联网安全检测工作更加专业化、规范化和常态化。

参考文献

[1] 丁超, 杨立君, 吴蒙. IoT/CPS的安全体系结构及关键技术.中兴通讯技术,2011,01(17).

[2] 李向军.物联网安全及解决措施.农业网络信息,2010,12.

[3] 戴铁君.物联网安全问题与其解决措施.科技风, 2011,02.

[4] 汪金鹏, 胡国华. 物联网安全性能分析与应用. 科技信息, 2010,33.

[5] 姚远. 基于中间件的物联网安全模型. 电脑知识与技术, 2011,01(07).

[6] 肖毅.物联网安全管理技术研究.通信技术. 2011, 01(44).

[7] 蒲石,陈周国祝世雄.震网病毒分析与防范[J].信息网络安全,2012,(02):40-43.

[8] 武鸿浩.CUDA并行计算技术在情报信息研判中的应用 [J].信息网络安全,2012,(02):58-59.

[9] 王勇.随机函数及其在密码学中的应用研究[J].信息网络安全,2012,(03):17-18.

[10] 丁丽萍.Android操作系统的安全性分析[J].信息网络安全,2012,(03):23-26.

作者简介:

李海涛(1980-),男,公安部第一研究所,博士,信息安全工程师;主要研究方向和关注领域:信息安全、物联网安全检测、风险评估、等级保护。