ICS 35.040
L 80

中华人民共和国国家标准

GB/T —XXXX

信息安全技术
物联网感知层网关安全技术要求

Network security technology- Security technology requirements of gateway in sensing layer of the internet of things,

（征求意见稿）

（本稿完成日期：2016-12-16）

-XX-XX 发布　　XXXX-XX-XX

中华人民共和国国家质量监督检验检疫总局
中国国家标准化管理委员会　发布

目　次

前　言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由网神信息技术(北京)股份有限公司提出。

本标准由全国信息安全标准化技术委员会归口。

本标准起草单位：网神信息技术(北京)股份有限公司、北京奇安信科技有限公司、北京奇虎科技有限公司、北京工业大学、工业和信息化部电子工业标准化研究所、中国信息安全认证中心、北京博大光通国际半导体技术有限公司。

本标准主要起草人：谭晓生、王刚、李健、孙凌、乔思远、李鸿培、张翀斌、武传坤、张剑、范科峰、龚洁中、廖原。

信息安全技术 物联网感知层网关安全技术要求

1 引言

物联网感知层网关安全技术要求旨在对物联网感知网络与其他通信网络之间、不同类型的感知网络之间、以及不同安全等级的感知网络之间的网关安全技术进行规范、指导和建议，建立轻量级、一体化的防护技术体系。

2 范围

本标准规定了物联网感知层网关安全功能要求和安全保证要求。

本标准适用于物联网感知层网关安全技术的研究及安全设备的研发。

3 术语和定义

下列术语和定义适用于本标准

3.1

物联网 internet of things

通过感知设备，按照约定的协议，进行物与物之间的信息交换和通信，实现智能化识别、定位、跟踪、监控和管理功能的信息通信系统。

3.2

对象 object

与物联网应用有关、用户感兴趣的物理实体。

3.3

物联网感知层网关

物联网感知层网关作为物联网的重要组成部分，它实现了感知网络与通信网络、不同类型感知网络之间的协议转换、互联和设备管理功能。

3.4

感知层 sensing layer

实现对对象的信息采集、汇聚、处理和控制的功能层。

3.5

域 domain

具有特定目的的实体集合。

3.6

物联网参考模型 IoT reference model

物联网中抽象化的概念、公理、关联组成的最小集合，用以描述物联网逻辑功能、接口关系等，它是形成网络体系结构的模型。

3.7

物联网参考体系结构 IoT reference architecture

对物联网系统整体结构、层次划分和不同部分之间协作关系的描述

3.8

物联网安全 security for IoT

凭借物联网技术及应用，形成抵御外来干扰或破坏的能力。

3.9

隐私保护 privacy protection

为保护隐私而采取的措施。

3.10

物联网安全管理 IoT security management

为保护物联网中人身、信息、设备的保密性、安整性、可用性以及核查性、真实性、抗抵赖性及可靠性等，对物联网系统所选择并施加的管理、操作和技术等方面的控制。

3.11

标识 identification

通过使用属性、标识符等来识别一个实体的过程。

3.12

标识符 identifier

用于描述实体的身份以及属性的一系列数字、字母、符号或者它们的任何组合形式。

3.13

标识符解析 identifier resolution

将标识符翻译成与其相关联的信息的过程。

3.14

数据 data

信息的可再解释的形式化表示

3.15

信息 information

关于客体（如事实、事件、事物、过程或思想,包括概念）的知识,在一定的场合中具有特定的意义。

4 缩略语

下列术语和定义适用于本标准。

RFID 射频识别（Radio Frequency Identification）

IoT 物联网（internt of things）

WI-FI 无线网(WIreless-FIdelity)

5 安全功能要求

5.1 物联网感知层网关安全技术要求组成

应包括专用于物联网网关的强认证安全功能，具体可参考防火墙、入侵检测、安全审计等多项网关技术的融合，从保障感知层网络出入端具备强安全性的技术角度，对物联网的整体安全起到支撑作用。

5.2 物联网感知层通讯支持

应支持至少一种广域网通信技术和短距离通信技术，例如：以太网、射频、串口、移动互联网、3G/4G、电力通信网等常用物联网感知层通讯方式，及 ZigBee、RFID、蓝牙、Wi-Fi、微波通信、载波通信、光纤通信、音频电缆等（但不限于）主流通讯方式中的信息采集协议。

5.3 安全环境

5.3.1 物理安全

应确保物联网感知层网关所涉及信息资源的处理，被限定在一些可控制的访问设备内，并防止未授权的物理访问。所有与实施安全策略相关的硬件和软件应受到保护，使其免于未授权的物理修改。同时，网关应对未授权的射频、无线、有限连接请求具备拒绝服务的能力。

5.3.2 人员安全

授权管理员应不具敌意，应遵守所有的管理员规则。

5.3.3 技术安全

应包括专用于物联网网关的防火墙技术、入侵检测技术和安全审计技术。

5.4 设备属性安全

5.4.1 结构安全

应采用独立主机形式或纯软件形式，达到相应行业设备系统的基本安全要求。

5.4.2 安全属性的定义

对于每一个授权管理员、构成系统的信息传输与控制部件和主机，应为其提供一套唯一的、为了执行功能策略所必需的安全属性。

5.4.3 安全功能属性

应具备对安全属性访问的授权与拒绝功能，且对授权管理员提供主机属性默认值和初始化功能，并仅向授权管理员提供设置、修改、查询安全功能参数和相应关系的能力。

5.4.4 身份鉴别

5.4.4.1 鉴别数据初始化

应根据规定的鉴别机制，提供授权管理员鉴别数据的初始化功能，并确保仅允许授权管理员使用这些功能。

5.4.4.2 鉴别时机

在所有授权管理员请求执行的任何操作之前，应确保对每个授权管理员进行身份鉴别。

5.4.4.3 最少反馈

当进行鉴别时，安全功能仅向用户提供身份验证的需求信息。

5.4.4.4 鉴别失败处理

在经过一定次数的鉴别失败以后，安全功能应能终止登录尝试的主机继续建立会话。最多失败次数仅由授权管理员设定。

5.4.4.5 超时重鉴别

应具有登录超时锁定或注销功能。在设定的时间段内没有任何操作的情况下，终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

5.4.4.6 多鉴别机制

安全功能应提供两种以上的鉴别机制以支持对用户的多重鉴别。

5.4.5 数据保护

应保护储存的鉴别数据和安全策略不受未授权查阅、修改或删除。

5.4.6 运行状态监测

应能够实时监测设备内外网主机维持自身功能正常运转的状态参数，比如CPU使用率、内存占用率、存储空间、电源状态等。

5.4.7 标识

开发者应为系统的不同版本提供唯一的标识，并且每个版本应当使用它们的唯一标识作为标签。

5.4.8 客体重用

在为不同安全域上的主机连接进行资源分配时，应保证不提供以前连接的任何信息内容。

5.5 访问控制

5.5.1 访问控制类型

访问控制的安全策略应包含，具体技术要求如下：

a) 基于数据包关键词的访问控制；
b) 基于安全域、群组的访问控制；
c) 满足环境、功能等特定控制形式需求的访问控制。

5.5.2 黑名单与白名单机制

用户可根据需要进行选择：

a) 相对开放的网络架构建议采用黑名单机制；
b) 相对封闭的网络架构建议采用白名单机制。

5.5.3 包过滤

应具备具体技术要求如下：

a) 应支持自定义机制，除非明确允许，否则就禁止；
b) 应支持协议转换，至少支持常用物联网传输协议与TCP/IP协议的转换；

5.5.4 包过滤的系统安全策略

应具备具体技术要求如下：

a) 应包含基于ID的访问控制；
b) 应包含基于源IP地址、目的IP地址的访问控制；
c) 应包含基于源端口、目的端口的访问控制；
d) 应包含基于协议类型的访问控制。

5.5.5 协议解析与转换

应具备具体技术要求如下：

a) 应支持物联网常用传输协议之一：RFID （ISO14433 TYPE A 等），Zigbee，802.11x，IEC61850 等；
b) 应支持物联网协议与互联网 TCP/IP 协议的转换；
c) 应实现基于转换后的标准协议制定访问规则，过滤规则和验证规则；

d) 应包含基于数据包关键词的访问控制的系统安全策略；
e) 应包含基于安全域、群组等进行的访问控制的系统安全策略。

5.6 入侵检测

5.6.1 强制访问控制

应能根据应用构建一个强访问控制模型，安全功能应能识别用户和应用数据的敏感标记，根据标记执行强制访问控制策略。

5.6.2 访问授权与拒绝

入侵检测应具备访问授权与拒绝的功能，具体技术要求如下：

a) 应执行默认禁止原则；
b) 应根据主体（发送方）和客体（接收方）的安全属性值提供明确的访问保障能力和拒绝访问能力；
c) 应能控制传输的服务类型；
d) 应能对传输数据进行内容过滤，只有用户明确允许的数据才能传输。

5.6.3 区分安全管理角色

入侵检测安全功能：

a) 应明确将安全相关的管理功能与其他功能区分开；
b) 应具备安装、配置和管理入侵检测安全功能本身所需的基本功能，具体包括：增加和删除主体（发送信息的主机）和客体（接受信息的主机），查阅安全属性，分配、修改和撤销安全属性，查阅和管理审计数据；
c) 应把执行与安全相关的管理功能的能力限定为一种安全管理职责，该职责具有一套特别授权的功能和响应的责任；
d) 应能把授权执行管理功能的授权管理员与使用隔离部件的所有其他个人或系统分开；
e) 应仅允许授权管理员承担安全管理职责；
f) 应在提出一个明确的请求以后，才会让授权管理员承担安全管理职责。

5.6.4 完整性保证

应通过技术手段保证传输信息的完整性，应考虑轻量级设备的处理能力，保障可用性。

5.6.5 管理功能

应向授权管理员提供如下管理功能：

a) 设置和更新与安全相关的数据；
b) 配置策略备份和恢复的能力，备份能力应有自动工具的支持；
c) 若支持远程管理，则应能限制可进行远程管理的地址，并且能够通过加密来保护远程管理对话。

5.6.6 设备冗余

应具备基于链路状态检测的设备冗余功能，当主入侵检测模块直接连接的链路发生故障而无法正常工作时，以备入侵检测模块应及时发现并接管主访问控制模块和入侵检测模块进行工作。

5.7 安全审计

5.7.1 审计数据生成

应能对下列可审计事件生成审计记录：

a) 审计功能的启动和关闭；
b) 任何对审计记录进行操作的尝试，包括关闭审计功能或子系统，以及受影响客体的标识；
c) 任何读取、修改、破坏审计记录的尝试；
d) 所有对访问授权与拒绝规则覆盖的主体执行操作的请求，以及受影响客体的标识；
e) 修改安全属性的所有尝试，以及修改后安全属性的新值；
f) 所有使用安全功能中鉴别数据管理机制的请求；
g) 所有访问鉴别数据的请求，以及访问请求的目标；
h) 任何对鉴别机制的使用；
i) 所有使用标识机制的尝试；
j) 所有对安全功能配置参数的修改（设置和更新），无论成功与否，以及配置参数的新值；
k) 因鉴别尝试不成功的次数超出了设定的限制。

对于每一个审计记录，安全功能应至少记录以下信息：事件发生的日期和时间，事件的类型，主体身份和成功或失败事件。

5.7.2 用户身份关联

应能将每个可审计事件与引起该事件的用户身份相关联。

5.7.3 审计记录管理

应使授权管理员能创建、存档和清空审计记录。

5.7.4 常用格式

应使存储于永久性审计记录中的所有审计数据为常用格式，并标明格式类型。

5.7.5 限制审计记录访问

应仅允许授权管理员访问审计记录。

5.7.6 可选择查阅审计

应提供能按主体 ID（标识符）、客体 ID、日期、时间以及这些参数的逻辑组合等参数对审计数据进行查找和排序的审计查阅工具。

5.7.7 防止审计数据丢失

应满足下列要求：

a) 应把生成的审计记录储存于一个永久性的审计记录中，并应限制由于故障和攻击造成的审计事件丢失的数量；
b) 一旦审计存储容量达到事先规定的警戒值，应能发出警告信息，并保证在产品审计员所采取的审计行为以外，防止其他可审计行为的出现。
c) 对因故障或存储耗竭而导致审计数据丢失的最大审计存储容量，访问控制和入侵检测功能的开发者应提供相应的分析结果。

5.8 安全保障要求

5.8.1 配置管理

5.8.1.1 配置管理自动化

应具备配置管理系统功能，并提供配置管理计划：

a) 配置管理系统应确保只有已授权开发及管理人员才能对系统实现进行修改，并支持系统基本配置项的生成；

b) 配置管理计划应描述在配置管理系统中使用的工具软件。

5.8.1.2 配置管理能力

开发者及使用者应能够使用配置管理系统并提供配置管理文档，以及为不同版本提供唯一的标识：

a) 配置管理系统应对所有的配置项给出唯一的标识，并保证只有经过授权才能修改配置项，还应支持访问控制和入侵检测技术基本配置项的生成。

b) 配置管理文档应包括配置清单、配置管理计划以及接受计划。配置清单用来描述组成各部分的配置项。在配置管理计划中，应描述配置管理系统是如何使用的。实施的配置管理应与配置管理计划相一致。在接受计划中，应描述对修改过或新建的配置项进行接受的程序。

c) 配置管理文档应描述对配置项给出唯一标识的方法，并提供所有配置项得到有效地维护的证据。

5.8.1.3 配置管理范围

应提供配置管理文档，该文档应说明配置管理系统至少能跟踪：产品实现表示、设计文档、测试文档、用户文档、管理员文档、配置管理文档和安全缺陷，并描述配置管理系统是如何跟踪配置项的。

5.8.2 指导性文档

5.8.2.1 管理员指南

应提供系统管理管理指南，管理指南应说明以下内容：

a) 明确可以使用的管理功能和接口；

b) 怎样安全地管理各安全模块；

c) 在安全处理环境中应进行控制的功能和权限；

d) 所有对与安全操作有关的用户行为的假设；

e) 所有受管理控制的安全参数，如果可能，应指明安全值；

f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制的实体的安全特性进行的改变；

g) 所有与系统管理操作有关的 IT 环境的安全要求；

h) 管理指南应与为评估而提供的其他所有文档保持一致。

5.8.2.2 用户指南

应提供用户指南，该用户指南应说明以下内容：

a) 非管理用户可使用的安全功能和接口；

b) 系统提供给用户的安全功能和接口的用法；

c) 在安全处理环境控制的范围内，用户可获取的所有功能和权限；

d) 安全操作中用户所应承担的职责；

e) 与用户有关的 IT 环境的所有安全要求；
f) 用户指南应与为评估而提供的其他所有文档保持一致。

5.8.2.3 操作指南文档

应提供操作指南文档，该确定对系统的所有可能的操作方式（包括失败和操作失误后的操作）、它们的后果以及对于保持安全操作的意义。指南性文档中还应列出所有目标环境的假设以及所有外部安全措施（包括外部程序的、物理的或人员的控制）的要求。指南性文档应是完备的、清晰的、一致的、合理的。在分析文档中，应阐明指南性文档是完备的。

5.8.2.4 脆弱性评定文档

应从用户可能破坏安全策略的角度出发，对系统安全内容进行分析并提供文档。对被确定的脆弱性，应明确记录采取的措施。 对每一条脆弱性，应有证据显示在使用系统时，该脆弱性不能被利用。在文档中，还需证明经过标识脆弱性的系统部分可以抵御明显的穿透性攻击。

5.8.3 测试要求

5.8.3.1 范围

应提供测试覆盖的分析结果，表明测试文档中所标识的测试与安全功能设计中所描述的安全功能是对应的，且该对应是完备的。

5.8.3.2 测试深度

应提供测试深度的分析，在深度分析中，应说明测试文档中所标识的对安全功能的测试，足以表明该安全功能和高层设计是一致的。

5.8.3.3 功能测试

应进行安全功能测试，并将结果文档化，并提供测试文档，具体测试条件、测试计划、测试过程、预期的测试结果和实际测试结果应满足如下要求：

a) 测试条件应标识最低测试环境要求，包括对关键协议、算法、应用的支持；
b) 测试计划应标识出要测试的安全功能，并描述测试的目标；
c) 测试过程应标识出要执行的测试内容，并描述每个安全功能的测试概况，这些概况包括对其它测试结果的顺序依赖性；
d) 预期的测试结果应清晰表明测试成功后的预期输出；
e) 实际测试结果应清晰表明每个被测试的安全功能能按照规定进行运作。

5.8.3.4 独立性测试

开发商应提供用于适合测试的产品，且提供的测试集合应与其自测产品功能时使用的测试集合相一致。

5.8.4 生命周期支持

5.8.4.1 开发安全

应提供开发安全文件，该文件应描述在系统开发环境中，为了保护其设计和实现的机密性和完整性，在物理上、程序上、人员上以及其他方面所采取的必要的安全措施。开发安全文件还应提供在系统开发和维护过程中执行安全措施的证据。

5.8.4.2 生命周期模型

应提供生命周期定义文档，该文档应描述用于开发和维护各系统模型。为了对各系统的开发和维护进行必要控制，该模型应提供相应的支持。

5.8.4.3 工具和技术

应明确标识出用于开发或辅助系统安全的各项工具，并对所涉及的各项工具中已选择的依赖实现的情况进行文档化。应明确定义所以工具在实现中每个语句的含义，以及所有基于实现的选项的含义。

参考文献

[1] GB 17859,计算机信息系统安全保护划分准则[S],1999.
[2] GB/T 18336.3,信息技术 安全技术 信息技术安全性评估准则[S],2008.
[3] GB/T 20281,信息安全技术 防火墙技术要求和测试评价方法[S],2006.