ICS 35.020
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1267—2015

公安物联网感知层信息安全技术导则

Technical guidelines for sensing layer information security of internet of things of public security

2015-07-16 发布　　2015-07-16 实施

中华人民共和国公安部　　发布

前　言

本标准按照 GB/T 1.1—2009 给出的规范起草。

本标准由公安部第一研究所提出。

本标准由公安部计算机与信息处理标准化技术委员会归口。

本标准起草单位：公安部第一研究所、公安部第三研究所。

本标准主要起草人：范红、李程远、邵华、胡志昂、张洪斌、李海涛、张冬芳、韩煜、杜大海、王冠、周东平、金丽娜、齐力、赵会敏、杨明、刘鑫、唐前进、李娜。

公安物联网感知层信息安全技术导则

1 范围

本标准规定了公安物联网感知层信息安全通用技术要求。

本标准适用于指导公安物联网感知层信息安全设计。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

GB/T 25069—2010 信息安全技术 术语

GB/T 25070—2010 信息安全技术 信息系统等级保护安全设计技术要求

GA/T 1266—2015 公安物联网术语

3 术语和定义

GB/T 25069—2010、GA/T 1266—2015 界定的以及下列术语和定义适用于本文件。

3.1

感知节点设备 sensor node device

连接在公安物联网中并完成感知操作过程的一个或一组装置。

示例：摄像机、RFID 标签及 RFID 阅读器。

[GA/T 1266—2015，定义 2.3]

3.2

感知操作 sensing operation

感知节点设备对感知对象进行数据读取或状态控制的过程。

[GA/T 1266—2015，定义 2.5]

4 感知层安全体系

感知层安全体系结构如图 1 所示，感知层安全体系包括：

a) 感知操作安全。指感知节点设备和感知对象在进行感知操作过程中的安全要求。感知操作方式分为单向读取、双向读取、单向控制和双向控制四类：

1) 单向读取指感知节点设备向感知对象单方面获取信息数据的感知操作过程；

2) 双向读取指感知节点设备与感知对象间交互获取信息数据的感知操作过程；

3) 单向控制指感知节点设备对感知对象发送控制指令使其状态发生改变的感知操作过程；

4) 双向控制指感知节点设备与感知对象间相互发送控制指令使对方改变状态的感知操作过程。

b) 数据处理安全。指感知节点设备通过感知操作获取感知数据后，在设备内部对数据进行运算处理过程中的安全要求。

c) 数据存储安全。指感知节点设备对感知数据在处理过程中或处理后进行缓存时的安全要求。
d) 感知节点设备通信安全。指感知节点设备间在进行网络通信过程中的安全要求。
e) 感知节点设备安全。指感知节点设备的用户身份鉴别、访问控制、安全审计和备份与恢复等安全要求。
f) 感知安全监管。指部署在物联网系统中负责物联网感知层系统管理、策略下发、审计以及安全保障的系统模块。

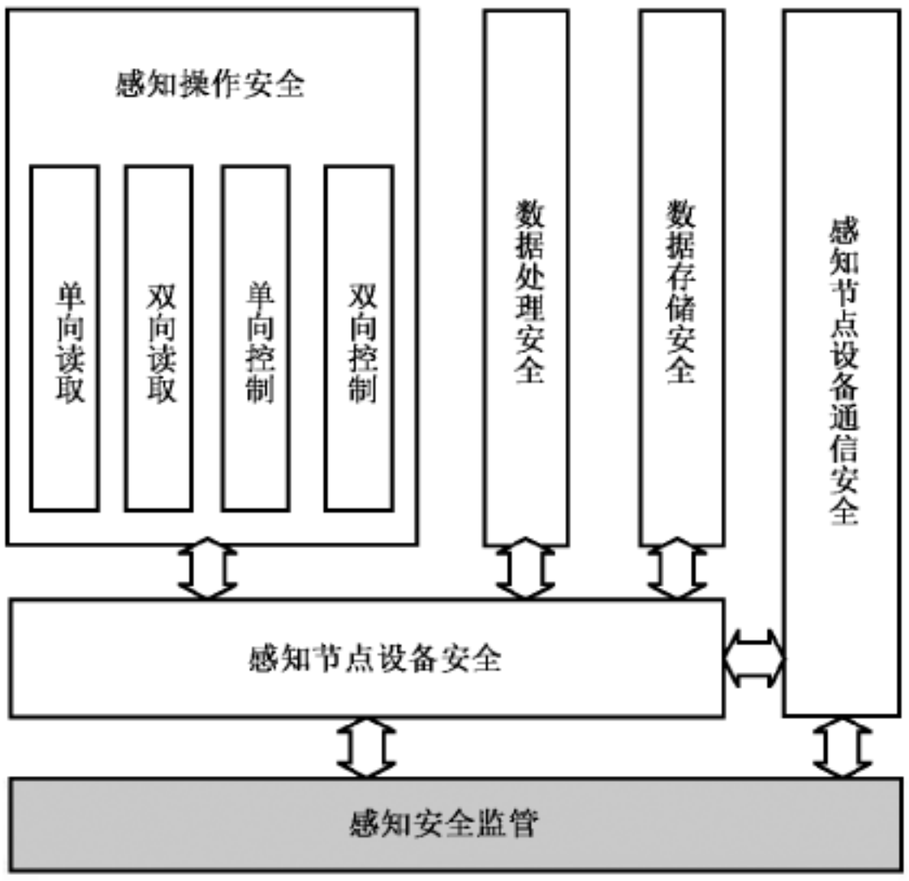

图 1 感知层安全体系结构

5 感知操作安全

5.1 感知操作安全技术要素

感知操作安全技术要素主要为数据保密性、数据完整性、数据新鲜性、设备认证、访问控制、抗干扰6个方面。感知操作的安全技术要素如表1所示。

表 1 感知操作安全技术要素

安全技术要素	单向读取	双向读取	单向控制	双向控制
数据保密性	—	★	★	★
数据完整性	★	★	★	★
数据新鲜性	—	★	★	★
设备认证	—	★	★	★
访问控制	—	—	★	★
抗干扰	★	★	★	★
注：“★”表示包含本行与第1列对应的安全技术要素，“—”表示不包含对应的安全技术要素。				

5.2 单向读取安全技术要求

5.2.1 数据完整性

宜对所读取数据进行完整性验证，可采用具有完整性校验机制的空中接口通信协议。

5.2.2 抗干扰

宜采用报警机制，限定干扰阈值，若超过阈值则实施报警。

5.3 双向读取安全技术要求

5.3.1 数据保密性

宜为交互数据提供数据加密，可采用具有链路加密功能的空中接口通信协议。

5.3.2 数据完整性

宜对所交互数据进行完整性验证，可采用具有完整性校验机制的空中接口通信协议。

5.3.3 数据新鲜性

宜采用适当的安全机制提供抵御重放攻击的能力，可采用时间戳或序列号的方式。

5.3.4 设备认证

在感知节点设备与感知对象进行数据交互之前，感知节点设备应对感知对象进行合法认证，可采用密码技术支持的双向认证机制。

5.3.5 抗干扰

宜采用适当的抗干扰机制提供抵御无线信号干扰的能力，可采用电磁/无线电屏蔽等机制。

5.4 单向控制安全技术要求

5.4.1 数据保密性

宜为单向控制指令提供数据加密，可采用具有链路加密功能的空中接口通信协议。

5.4.2 数据完整性

宜对单向控制指令进行完整性验证，可采用具有完整性校验机制的空中接口通信协议。

5.4.3 数据新鲜性

宜采用适当的安全机制提供抵御重放攻击的能力，可采用时间戳或序列号的方式。

5.4.4 设备认证

在感知节点设备对感知对象进行控制操作之前，感知对象应对感知节点设备进行合法认证，可采用密码技术支持的单向认证机制。

5.4.5 访问控制

宜限定合法感知节点设备所能进行控制操作的范围，可采用维护感知节点设备访问控制策略列表

的方式。

5.4.6 抗干扰

宜采用适当的抗干扰机制提供抵御无线信号干扰的能力，可采用无线序列跳频等机制。

5.5 双向控制安全技术要求

5.5.1 数据保密性

宜为双向控制指令提供数据加密，可采用具有链路加密功能的空中接口通信协议。

5.5.2 数据完整性

宜对双向控制指令进行完整性验证，可采用具有完整性校验机制的空中接口通信协议。

5.5.3 数据新鲜性

宜采用适当的安全机制提供抵御重放攻击的能力，可采用时间戳或序列号的方式。

5.5.4 设备认证

在感知节点设备与感知对象进行交互控制操作之前，感知节点设备与感知对象间应进行双向合法性认证，可采用密码技术支持的双向认证机制。

5.5.5 访问控制

宜限定合法感知节点设备所能进行控制操作的范围，可采用维护感知节点设备访问控制策略列表的方式。

5.5.6 抗干扰

宜采用适当的抗干扰机制提供抵御无线信号干扰的能力，可采用无线序列跳频等机制。

6 数据存储安全

6.1 数据保密性

宜对感知节点设备的设备信息、密钥、安全参数和重要数据等关键信息进行保护。可依据数据的重要程度、节点计算能力、存储能力进行不同强度的加密算法保护。

6.2 数据完整性

在感知节点设备计算能力、存储容量的可用范围内，宜采用数字签名算法或散列算法确保数据的完整性。

6.3 数据的备份与恢复

宜根据数据的重要性及其对系统运行的影响，制定不同等级的数据备份和恢复策略，备份策略指明备份数据的放置场所、文件命名规则、介质替换频率和数据运输方法。

7 数据处理安全

7.1 数据保密性

在感知节点设备计算能力、存储容量的可用范围内，宜采用密码算法保护处理过程中的数据保密性。

7.2 数据完整性

在感知节点设备计算能力、存储容量的可用范围内，宜采用数字签名算法或散列算法保护处理过程中的数据完整性。

8 感知节点设备通信安全

8.1 数据保密性

宜采用适用于存储及计算能力有限的感知节点设备且含有密码算法的网络通信协议，实现通信数据传输的保密性保护。

8.2 数据完整性

宜采用适用于存储及计算能力有限的感知节点设备且包含完整性校验机制的网络通信协议，实现通信数据传输的完整性保护，使感知节点设备能够检验网络通信数据的完整性。

8.3 设备入网标识与认证

对参与通信的设备设置网络标识，并在系统整个生存周期中保证标识的唯一性，以在网络中识别设备身份。宜采用密码等技术支持的认证机制，在每次进行网络连接时认证设备身份。

8.4 抗干扰

宜采用干扰监测机制与扩频或跳频机制相结合的方式，通过频率跳转、降低工作占空比、切换通信模式等方法防御网络通信干扰。

9 感知节点设备安全

9.1 用户身份鉴别

宜支持用户身份标识和身份鉴别。在每一个用户注册到感知节点设备时，应采用用户名或用户标识符标识用户身份，并确保在感知节点设备整个生存周期用户标识的唯一性；在每次用户登录感知节点设备时，应采用感知节点设备管理的或受感知监控中心控制的鉴别机制进行用户身份鉴别，并对鉴别数据进行保密性和完整性保护。

9.2 访问控制

宜采用感知节点设备管理或受感知监控中心控制的安全策略，对用户进行访问控制，控制用户访问资源的范围。

9.3 安全审计

应提供安全审计机制，审计用户、设备运行和数据处理相关的安全事件，审计记录包括时间、类型和结果。审计机制应提供审计记录查询、分类和存储保护，并可由感知监控中心管理。

9.4 节点备份与恢复

宜采用双节点或多节点备份与恢复机制，将备用节点部署在网络中，在需要时向备份节点传输配置信息，并激活备份节点检测机制，在节点发生故障时，自动执行故障处理操作。如重新启动设备。

10 感知安全监管

10.1 策略管理

10.1.1 功能要求

应对安全策略进行集中管理，为感知节点设备提供统一标识和身份认证，支持感知节点设备备份与恢复统一管理。

10.1.2 策略管理

策略管理功能包括：

a) 存储；

b) 查询；

c) 导入/导出；

d) 审核/修订。

10.2 审计管理

10.2.1 审计范围

应实现感知层中感知操作行为、感知节点设备运行和数据处理、感知节点设备网络通信过程的安全审计，且审计记录应包括时间、类型和结果。

10.2.2 审计管理

审计管理应符合 GB/T 25070—2010 中 7.3.4.3 的要求。

参 考 文 献

[1] ISO 14443 Contactless card standards 非接触式 IC 卡标准协议

[2] IEEE 802.15 Enabling wireless sensors with ieee 802.15.4 stdsp1150

[3] 3GPP TR 3.868 Security Aspects of Machine-Type Communications 机器类型通信安全问题研究

[4] Draft-ietf-roll-security-Framework-07 A Security Framework for Routing over Low Power and Lossy Network 低功耗易损网络路由安全架构

[5] 传感器网络 信息安全 通用技术规范(征求意见稿)

[6] ISO/IEC 29192-1:2012 Information technology—Security techniques—Lightweight cryptography—Part 1: General

中华人民共和国公共安全
行业标准

公安物联网感知层信息安全技术导则

GA/T 1267—2015

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址:www.gb168.cn
服务热线:400-168-0010
010-68522006

2015年11月第一版

*

书号:155066·2-29083

GA/T 1267-2015