ICS 35.020
A 90

中华人民共和国国家标准

GB/T 35318—2017

公安物联网感知终端安全防护技术要求

Security protection technology requirements for sensing terminals of IoTPS

2017-12-29 发布　　2017-12-29 实施

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。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中华人民共和国公安部提出并归口。

本标准起草单位：公安部第三研究所、公安部第一研究所、公安部安全防范报警系统质量监督检验测试中心、无锡物联网产业研究院、工业和信息化部电子工业标准化研究院、华为技术有限公司、浙江宇视科技有限公司、上海辰锐信息科技公司、国家计算机网络应急技术处理协调中心。

本标准主要起草人：杨明、齐力、唐前进、陶源、巩思亮、张洪斌、陆洪波、张艳、李旋、陈书义、龚洁中、沈国华、廖双龙、陈家明、王晖。

公安物联网感知终端安全防护技术要求

1 范围

本标准规定了公安物联网感知终端所涉及的硬件安全、软件安全和数据安全等安全防护技术要求。

本标准适用于公安物联网感知终端产品的软、硬件设计和研发等。

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 4208 外壳防护等级(IP 代码)

GB/T 17799.1—2017 电磁兼容 通用标准 居住、商业和轻工业环境中的抗扰度

GB/T 25069 信息安全技术 术语

GB/T 28181 公共安全视频监控联网系统信息传输、交换、控制技术要求

GB/T 28925 信息技术 射频识别 2.45 GHz 空中接口协议

GB/T 29768 信息技术 射频识别 800/900 MHz 空中接口协议

GA 267 计算机信息系统雷电电磁脉冲安全防护规范

GA/T 1266 公安物联网术语

3 术语和定义

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

3.1

公安物联网感知终端 sensing terminal of IoTPS

部署在公安物联网感知层中，能够通过有线、无线方式发起或终结通信的感知节点设备。

3.2

安全增强软件 enhanced security software

在操作系统中，实现实体认证、访问控制、数据安全和安全日志/审计等功能的程序。

3.3

数据时效性 timeliness of data

保证数据发送和接收的时间有效性，确保数据的传输没有被重放。

3.4

安全功能硬件 security function hardware

可独立进行密钥生成，加解密计算和随机数生成等操作的，并能保护密钥、参数等密码材料安全存储的独立的处理器和存储单元。

4 缩略语

下列缩略语适用于本文件。

ID:身份标识号码(Identity)

IoTPS:公安物联网(Internet of Things of Public Security)

IP:互联网协议(Internet Protocol)

5 公安物联网感知终端安全防护概述

5.1 感知终端安全防护技术架构

公安物联网感知终端(以下简称“感知终端”)安全防护技术架构由硬件安全、软件安全、数据安全、产品开发与发布安全和管理安全构成。见图1。

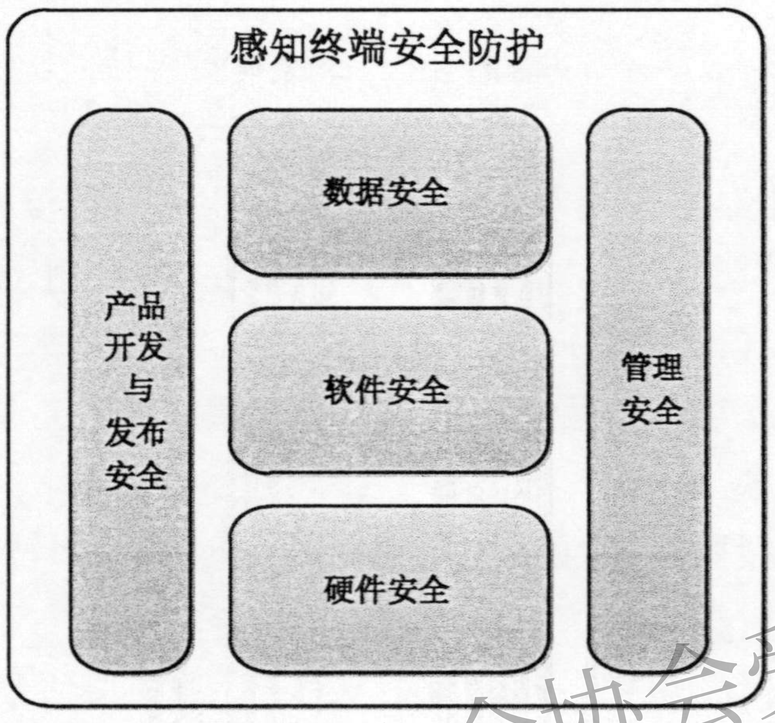

图1 感知终端安全防护技术架构图

5.2 感知终端类型

感知终端常见类型有:

a) 有线IP类带操作系统型;

b) 无线IP类带操作系统型;

c) 有线IP类无操作系统型;

d) 无线IP类无操作系统型;

e) 有线非IP类型;

f) 无线非IP类型。

注:以上“无操作系统”是指不采用已知的操作系统,通过直接编写硬件驱动和IP协议栈的方式形成的终端可执行程序。

6 感知终端通用安全技术要求

6.1 硬件安全

6.1.1 外观及结构要求

感知终端应满足以下外观及结构的防护要求:

a) 外观完好且不易被破坏,金属件无锈蚀;

b) 表面的标记和字符清晰可辨,设备名称、型号、制造厂名和编号等标志齐全;

c) 根据部署的工作环境条件,其防护等级及其细则满足GB/T 4208的相应要求;

d) 具备雷电防护措施，对于部署于室外环境的中、大型终端的防雷电保护满足 GA 267 的相应要求。

6.1.2 终端标识要求

感知终端应具备应用系统可识别、防篡改和防擦除的唯一 ID 标识。

6.1.3 电路设计要求

6.1.3.1 电磁兼容要求

感知终端应能根据工作条件和环境，符合 GB/T 17799.1—2017 中相应的表 1、表 2、表 3 和表 4 中限值的静电放电、射频电磁场、快速瞬变脉冲群、浪涌、射频共模、电压中断和电压暂降等抗扰度测试要求。

6.1.3.2 外设和通信接口要求

感知终端满足以下外设和通信接口安全要求：

a) 应具备外设和通信接口的电路自检功能，自检异常时应自动报警或停止工作；
b) 应使用文字或图案标记来说明外设和通信接口用途，外设和通信接口的使用应符合相关应用安全规定；
c) 宜去除板载软件调试接口或将接口封闭在产品外壳内。

6.1.4 安全功能硬件要求

感知终端宜具备安全功能硬件并支持运行国家密码局规定密码算法。

6.2 软件安全

感知终端满足以下通用软件安全要求：

a) 应支持读取唯一 ID 识别码、设备信息或信息摘要的功能；
b) 应具备通信协议过滤功能，应支持限定应用的通信协议，按协议格式进行数据过滤，并限定数据段长度；
c) 宜具备对安全事件的日志和审计功能。

6.3 数据安全

6.3.1 感知数据安全

感知终端感知数据的通信安全应满足：

a) 射频识别通信符合 GB/T 29768 和 GB/T 28925 中相应安全要求；
b) 视频通信符合 GB/T 28181 中相应安全要求；
c) 其他感知类型具备数据校验功能并保证时效性。

6.3.2 数据传输安全

感知终端与公安物联网应用系统的数据传输应满足以下传输安全要求：

a) 具备数据校验功能；
b) 具备时间戳数据保护功能，满足数据时效性要求。

6.3.3 数据存储安全

感知终端应保障存储数据的完整性，并对敏感信息数据进行加密。

6.4 感知终端连接网关要求

当感知终端与物联网网关的连接时，感知终端宜具备实体认证、数据加密和完整性保障功能。

6.5 产品开发与发布安全

感知终端产品开发与发布安全应满足以下要求：

a) 提供安全功能设计、开发和测试文档；

b) 提供产品的版本标识；

c) 提供产品的安全功能说明，及其使用、维护和升级方法。

6.6 管理安全

6.6.1 身份管理

感知终端应支持身份管理功能。

6.6.2 日志/审计

感知终端应对安全事件进行日志审计，内容应包括日期/时间、事件类型、内容描述、结果等。

7 有线 IP 类带操作系统型补充要求

7.1 软件安全

7.1.1 软件安全功能要求

7.1.1.1 接入认证

感知终端应支持唯一 ID 识别、终端信息数字摘要及媒体接入控制(MAC)地址绑定方式的接入认证。

7.1.1.2 访问控制

感知终端的访问控制满足以下安全要求：

a) 应使用统一的用户管理和授权，宜采用基于属性或角色的访问控制模型来控制用户的访问权限，应使用访问控制列表(ACL)来进行授权用户对终端资源的访问控制；

b) 应保障授权用户仅可访问被授权的终端资源，并能阻止非授权的终端资源访问操作。

7.1.1.3 入侵防护

感知终端的入侵防护满足以下安全要求：

a) 安装经过安全认证的恶意代码扫描软件，支持对恶意代码入侵报警和处理；

b) 恶意代码入侵报警，生成日志信息，并通过向应用服务器发送数据形式，通知终端管理员；

c) 宜对正常通信指令的异常行为进行检测和报警，并宜具备相应的保护措施，生成日志信息，并通过向应用服务器发送数据形式，通知终端管理员。

7.1.2 软件安全保障要求

7.1.2.1 操作系统

感知终端的软件操作系统满足以下安全要求：

a) 使用装有安全增强软件的操作系统；

b) 操作系统应提供对各个进程及其使用资源的查阅和控制功能；
c) 操作系统应支持外设接口和通信端口的参数设置和管理功能，应限制未授权的接口和端口的使用，并限定动态侦听端口的范围；
d) 操作系统应能实时检测到外接硬件设备的接入，当发现外接设备连接之后，应及时通知预先指定的处理软件；
e) 操作系统应有定期补丁计划，宜使用授权的升级补丁为操作系统升级；
f) 仅允许安装经过授权的应用软件或升级程序；
g) 对应用软件的完整性、安全性和来源的合法性进行验证。

7.1.2.2 数据库软件

感知终端的数据库软件满足以下安全要求：

a) 数据库口令应避免使用数据库厂商提供的缺省值，数据库若存在多个默认账户，应将不使用的账户禁用或删除；
b) 应使用单独的操作系统帐号来运行数据库。对数据库帐户授予权限应进行划分，所有数据库账户应授予其操作范围的最小权限；对于有监听功能的数据库应设置监听器密码或者设置为本地操作系统验证；
c) 数据库中的敏感信息文件应控制访问权限，只能被数据库进程运行账户和数据库管理员(DBA)账户读写。

7.1.2.3 应用软件

应用软件的源代码宜经过防病毒扫描测试，并进行完整性校验。

7.1.2.4 安全增强软件

感知终端的安全增强软件应满足开机自启动、宜防止卸载、防止被进程服务停止等要求。

7.1.2.5 网页服务软件

感知终端的网页服务软件满足以下安全要求：

a) 所有浏览器侧产生的数据，在感知终端上进行校验，输出到客户端前先进行超文本标记语言(HTML)编码；
b) 宜具备对跨站脚本攻击(XSS)、跨站请求伪造(CSRF)、命令注入等漏洞的防护措施。

7.2 数据安全

7.2.1 感知数据安全

感知终端感知数据的通信安全应支持数据异常监测，一旦发现感知数据出现明显偏差或丢失关键信息，应采取预先设定的应对安全措施。

7.2.2 数据传输安全

感知终端宜支持数据加密传输。

7.3 管理安全

7.3.1 用户和权限管理

感知终端应满足以下安全要求：

a) 为多个用户包括管理员用户建立账号、口令等登录信息；

b) 支持管理员用户登录鉴别功能，支持用户的本地登录和/或远程登录；
c) 为不同的管理员用户提供不同的访问权限，访问权限包括查阅、配置不同终端功能的属性和应用软件的执行权限；
d) 禁止非授权用户查询、配置终端功能属性和应用软件的执行权限。

7.3.2 用户身份鉴别

感知终端应满足以下安全要求：

a) 用户身份鉴别机制应包括“口令”认证方式，鉴别在每次访问终端时执行；
b) 具备用户鉴别失败处理措施，在经过一定次数的鉴别失败以后，该账号被锁定并保存报警日志和发出报警信息，经过一段由应用规定的时间后才可解锁；
c) 具备用户登录超时自动退出的功能。在设定的时间内没有任何操作的情况下将终止会话，再次进行身份鉴别才能进行新的操作。超时时间具备不为“0”的默认值，并由特定权限的管理员设置。

7.3.3 口令安全

感知终端用户鉴别口令应满足以下安全要求：

a) 口令具备一定的复杂度，长度不少于 6 个字符，至少包含字母大小写、数字、特殊字符的组合；
b) 用户(管理员用户除外)仅可以修改自身帐号的口令，用户修改口令前验证旧口令；
c) 不应使用默认口令。

7.3.4 日志/审计

感知终端支持对定义周期日志的自动覆盖，宜对以下范围内容进行日志/审计：

a) 接入认证、入侵检测、故障、报警等事件；
b) 终端软件安装、卸载、升级等事件；
c) 敏感信息标识的感知数据信息的创建、删除、修改等事件；
d) 管理员用户的登录和注销、更改口令、对其他用户的锁定和解锁等事件。

8 无线 IP 类带操作系统型补充要求

8.1 硬件安全

感知终端的安全功能硬件应满足以下安全要求：

a) 具备唯一 ID 标识、数字证书、密钥的安全存储和管理功能；
b) 支持鉴别用户的安全加密模块、用户标识与终端 ID 的绑定使用。

8.2 软件安全

8.2.1 软件安全功能要求

8.2.1.1 接入认证

感知终端满足以下接入认证安全要求：

a) 应支持建立安全通信链路的双向身份认证；
b) 宜具备通信端口及协议的认证机制。

8.2.1.2 访问控制

同 7.1.1.2 的规定。

8.2.1.3 入侵防护

同 7.1.1.3 的规定。

8.2.2 软件安全保障要求

同 7.1.2 的规定。

8.3 数据安全

8.3.1 感知数据安全

同 7.2.1 的规定。

8.3.2 数据传输安全

感知终端应支持数据加密传输。

8.3.3 数据存储安全

感知终端应保障存储在终端内的公安物联网业务数据的安全，满足以下安全要求：

a) 数字证书信息、实体认证密钥、数据通信密钥存储在安全功能硬件中的专用区域，该区域实行访问控制；

b) 管理员用户口令、安全日志/审计信息等数据存储在专用区域，该区域实行访问控制，数据加密并保障其完整性；

c) 在终端上备份的数据进行加密存储并保障其完整性。

8.4 管理安全

同 7.3 的规定。

9 有线 IP 类无操作系统型补充要求

9.1 软件安全

感知终端软件应满足以下安全要求：

a) 存储在具有授权访问机制保护的存储器内；

b) 对运行程序的内存区间与通信控制协议数据的读取区间进行有效隔离；

c) 排除已知病毒和木马类恶意代码。

9.2 数据安全

同 7.2 的规定。

9.3 管理安全

9.3.1 用户管理

同 7.3.1 中 a)、b)的规定。

9.3.2 用户身份鉴别

同 7.3.2 的规定。

9.3.3 口令安全

同 7.3.3 的规定。

10 无线 IP 类无操作系统型补充要求

10.1 硬件安全

感知终端应具备安全功能硬件。

10.2 软件安全

同 9.1 的规定。

10.3 数据存储安全

感知终端应保障存储在终端内的公安物联网业务数据的安全，满足以下安全要求：

a) 实体认证密钥、数据通信密钥存储在安全功能硬件中的专用区域，该区域实行访问控制；

b) 同 8.3.3 中 b)的规定；

c) 同 8.3.3 中 c)的规定。

10.4 管理安全

10.4.1 用户管理

同 7.3.1 中 a)、b)的规定。

10.4.2 用户身份鉴别

同 7.3.2 的规定。

10.4.3 口令安全

同 7.3.3 的规定。

11 有线非 IP 类型补充要求

感知终端的软件安全要求同 9.1。

12 无线非 IP 类型补充要求

12.1 硬件安全

同 10.1 的规定。

12.2 软件安全

同 9.1 的规定。

12.3 数据存储安全

感知终端应保障存储在终端内的公安物联网业务数据的安全，并满足以下要求：

a) 同 10.3 中 a)的规定；

b) 安全日志/审计信息、备份的业务数据等应存储在专用区域，数据应加密并保障其完整性。

参 考 文 献

[1] GB/T 20269—2006 信息安全技术 信息系统安全管理要求
[2] GB/T 20270—2006 信息安全技术 网络基础安全技术要求
[3] GB/T 20271—2006 信息安全技术 信息系统通用安全技术要求
[4] GB/T 20272—2006 信息安全技术 操作系统安全技术要求
[5] GB/T 21052—2007 信息安全技术 信息系统物理安全技术要求
[6] GB/T 22239—2008 信息安全技术 信息系统安全等级保护基本要求
[7] GB/T 22240—2008 信息安全技术 信息系统安全等级保护定级指南
[8] GB/T 25068.1—2012 信息技术 安全技术 IT 网络安全 第 1 部分:网络安全管理
[9] GB/T 29240—2012 信息安全技术 终端计算机通用安全技术要求与测试评价方法
[10] 《商用密码产品使用管理规定》(国家密码管理局 2007 年 5 月)

中 华 人 民 共 和 国
国 家 标 准
公安物联网感知终端安全防护技术要求
GB/T 35318—2017
*
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.spc.net.cn
总编室:(010)68533533 发行中心:(010)51780238
读者服务部:(010)68523946
中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销
*
开本 880×1230 1/16 印张 1 字数 22 千字
2017 年 12 月第一版 2017 年 12 月第一次印刷
*
书号:155066·1-58897 定价 18.00 元

GB/T 35318-2017