ICS 35.020
A 90

中华人民共和国国家标准

GB/T 37714—2019

公安物联网感知设备数据传输安全性评测技术要求

Technical requirements for security evaluation of sensing device data transmission of IoTPS

2019-06-04 发布　　2019-06-04 实施

国家市场监督管理总局
中国国家标准化管理委员会　发布

目　　次

前言 …… Ⅲ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　感知设备读取或状态控制过程中数据传输安全性评测要素和技术要求 …… 1
4.1　评测要素 …… 1
4.2　评测技术要求 …… 2
5　感知设备间通信安全性评测要素和技术要求 …… 3
5.1　评测要素 …… 3
5.2　评测技术要求 …… 3
参考文献 …… 5

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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：公安部第一研究所、公安部第三研究所、中国电子技术标准化研究院。

本标准主要起草人：范红、杜大海、李海涛、韩煜、王冠、张洪斌、李娜、闫建华、陶源、金丽娜、赵会敏、龚洁中。

公安物联网感知设备数据传输安全性评测技术要求

1 范围

本标准规定了公安物联网感知设备进行数据读取或状态控制过程中数据传输和感知设备间通信的安全性评测要素及技术要求。

本标准适用于公安物联网感知设备数据传输安全性评测。

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 17626.3—2016 电磁兼容 试验和测量技术 射频电磁场辐射抗扰度试验

GB/T 25069—2010 信息安全技术 术语

GA/T 1266—2015 公安物联网术语

3 术语和定义

GB/T 25069—2010 和 GA/T 1266—2015 界定的术语和定义适用于本文件。

4 感知设备读取或状态控制过程中数据传输安全性评测要素和技术要求

4.1 评测要素

4.1.1 保密性

感知设备进行读取或状态控制过程中数据传输具备密码算法等数据传输保密性保护能力。

4.1.2 完整性

感知设备读取或状态控制过程中数据传输具备完整性校验技术等数据传输完整性保护能力。

4.1.3 新鲜性

感知设备读取或状态控制过程中数据传输具备时间戳、序列号等数据传输新鲜性保护能力。

4.1.4 抗干扰

感知设备读取或状态控制过程中数据传输具备电磁屏蔽等数据传输抗干扰能力。按照GB/T 17626.3—2016 中第 2 级的要求，感知设备应能正常进行读取或状态控制操作。

4.1.5 安全审计

感知设备具备读取或状态控制过程中数据传输审计能力，对读取或状态控制过程中传输的数据审

计记录至少应包括以下内容：

a） 数据传输时间；

b） 数据传输大小；

c） 数据传输目标；

d） 数据源。

4.2 评测技术要求

4.2.1 保密性

4.2.1.1 评测要求

应根据感知设备读取或状态控制过程中进行数据传输所提供的密码算法等保密性机制对需要传输的数据进行加解密计算，对比计算出来的加解密数据与传输的数据是否一致。

4.2.1.2 结果判定

数据一致为符合要求，其他情况为不符合要求。

4.2.2 完整性

4.2.2.1 评测要求

应根据感知设备读取或状态控制过程中数据传输所提供的完整性校验方法进行完整性校验，对比校验产生的数据与感知设备读取或状态控制过程中传输的完整性校验数据是否一致。

4.2.2.2 结果判定

校验数据一致为符合要求，其他情况为不符合要求。

4.2.3 新鲜性

4.2.3.1 评测要求

应根据感知设备读取或状态控制过程中所提供的数据传输新鲜性验证方法检查是否存在新鲜性保护机制，比如时间戳、序列号等内容。

4.2.3.2 结果判定

感知设备读取或状态控制过程中传输的数据中含有保护传输数据新鲜性的相关信息，比如时间戳、序列号或者其他新鲜性保护信息的为符合要求，其他为不符合要求。

4.2.4 抗干扰

4.2.4.1 评测要求

应按照 GB/T 17626.3—2016 中给出的试验方法进行评测，试验等级采用 2 级。

4.2.4.2 结果判定

按照 GB/T 17626.3—2016 中 2 级的干扰试验方法进行干扰，感知设备能够正常进行读取或状态控制的为符合要求，其他情况为不符合要求。

4.2.5 安全审计

4.2.5.1 评测要求

感知设备进行读取或状态控制操作，查看感知设备审计记录的正确性。

4.2.5.2 结果判定

感知设备应能对读取或状态控制过程中传输的数据进行审计，且审计记录至少包括 4.1.5 规定的内容为符合要求，其他情况为不符合要求。

5 感知设备间通信安全性评测要素和技术要求

5.1 评测要素

5.1.1 保密性

感知设备间通信具备数据传输保密性保护能力。

5.1.2 完整性

感知设备间通信具备数据传输完整性保护能力。

5.1.3 抗干扰

感知设备间通信具备抗干扰能力。按照 GB/T 17626.3—2016 中第 2 级的要求，感知设备能够正常进行通信。

5.1.4 安全审计

感知设备具备通信安全审计能力，对感知设备间通信的审计记录至少应包括以下内容：

a) 时间；

b) 数据大小；

c) 数据发送者和接收者。

5.1.5 抗抵赖性

感知设备间通信具备抗抵赖能力。例如，感知设备信息发送者对发送的数据进行数字签名，数据的接收者能够对接收的数字签名进行验证。

5.2 评测技术要求

5.2.1 保密性

5.2.1.1 评测要求

应根据感知设备间通信时所提供的数据传输保密性措施对需要传输的数据进行处理，对比处理后的数据与感知设备通信时传输的数据是否一致。

5.2.1.2 结果判定

数据一致为符合要求，其他情况为不符合要求。

5.2.2 完整性

5.2.2.1 评测要求

根据感知设备所提供的通信内容完整性校验方法进行完整性校验，对比校验数据与感知设备通信时传输的完整性校验数据是否一致。

5.2.2.2 结果判定

校验数据一致为符合要求，其他情况为不符合要求。

5.2.3 抗干扰

5.2.3.1 评测要求

按照 GB/T 17626.3—2016 中给出的试验方法进行评测，试验等级采用 2 级。

5.2.3.2 结果判定

按照 GB/T 17626.3—2016 中 2 级的干扰试验方法进行干扰，感知设备能够正常进行通信的为符合要求，其他情况为不符合要求。

5.2.4 安全审计

5.2.4.1 评测要求

模拟感知设备间通信事件，查看感知设备审计记录的正确性。

5.2.4.2 结果判定

感知设备应能对感知设备间通信事件进行审计，且审计记录至少包括 5.1.4 规定的内容为符合要求，其他情况为不符合要求。

5.2.5 抗抵赖性

5.2.5.1 评测要求

根据感知设备所提供的抗抵赖性验证方法进行抗抵赖数据验证，对比验证数据结果。

5.2.5.2 结果判定

验证数据结果一致为符合要求，其他情况为不符合要求。

参 考 文 献

[1] GB/T 33474—2016 物联网 参考体系结构
[2] GB/T 33745—2017 物联网 术语
[3] GB/Z 33750—2017 物联网 标准化工作指南
[4] GB/T 35317—2017 公安物联网系统信息安全等级保护要求
[5] GB/T 35318—2017 公安物联网感知终端安全防护技术要求
[6] GB/T 35592—2017 公安物联网感知终端接入安全技术要求
[7] GA/T 1267—2015 公安物联网感知层信息安全技术导则