广州赛宝认证中心服务有限公司技术规范

CEPREI-015-CTS-2020

智能安全认证—智能家电产品技术规范

（第一版）

2020-08-24 发布　　2020-08-24 实施

广州赛宝认证中心服务有限公司

目 录

前　言

本技术规范规定了专业、严谨、公正的测评方法，从贴近用户/行业所关注的信息安全角度选取测评内容，为用户提供专业的消费建议及指导，引导行业信息安全能力建设、可持续发展的目标制定。

本技术规范由广州赛宝认证中心服务有限公司提出。

本技术规范由广州赛宝认证中心服务有限公司归口。

本技术规范参与起草单位：广州赛宝认证中心服务有限公司、海尔智家股份有限公司、工业和信息化部电子第五研究所。

本技术规范主要起草人：刘群兴、刘茴茴、朱文立、彭琦、李乐言、赖怡聪、李荣、胡雄锋、黄伟明。

智能安全认证—智能家电产品技术规范

1 范围

本规范规定了智能家电产品的术语和定义、技术要求和测试方法。

本规范所指的智能家电产品是应用了智能化技术或具有智能化能力和功能的家用和类似用途的电器。

本规范适用于单相器具额定电压不超过 250V，其他器具额定电压不超过 480V 的智能家用和类似用途电器。

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，仅所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 18336-2015 信息技术 安全技术 信息技术安全性评估准则

GB/T 34975-2017 信息安全技术移动智能终端应用软件安全技术要求和测试评价方法

GB/T 35273-2020 个人信息安全技术个人信息安全规范

GB/T 22239-2019 信息安全技术网络安全安全等级保护基本要求

3 术语、定义和缩略语

3.1 术语和定义

GB/T 25069-2010界定的以及下列术语和定义适用于本文件：

3.1.1 移动应用 Mobile Application

指安装在移动智能终端上，通过网络链接服务端进行交互操作的应用程序软件。

3.1.2 完整性 integrity

保护资产准确性和完整的特征。

3.1.3 保密性 confidentiality

使信息不泄露给未授权的个人、实体、进程，或不被其利用的特性。

3.2 缩略语

下列缩略语适用于本技术规范：

ID	Identity	身份标识号码
MAC	Media Access Control	媒体访问控制

4 技术要求

4.1 终端要求

4.1.1 硬件安全

4.1.1.1 设备标识

智能家电终端应具备可用于通信识别的唯一标识。示例：设备ID、序列号、MAC地址等。

4.1.1.2 安全启动

智能家电终端应支持引入安全启动机制，系统启动按照用户设定的方式，建立初始环境，监督安全启动过程。开机时采用开机认证，系统启动后对操作系统装载信息，操作系统内核、硬件配置、关键应用等进行一致性校验。

4.1.1.3 调试接口安全

智能家电终端应满足如下调试接口安全要求：

a) 调试接口配置为限制使用；
b) 通过授权的方式管理调试端口的打开、关闭。

4.1.2 系统软件安全

4.1.2.1 设备绑定

用户使用智能家电终端前，须先将设备绑定或添加到自己的账户下，然后可在移动应用中对设备进行管理和操控。具体要求如下：

a) 智能家电终端只有在与合法账户绑定之后，方可执行网络控制操作；
b) 一个智能家电终端一次只能被一个账户绑定，该绑定账户作为设备的主控制账户，在主控制账户显式授权下或设备重置后方可更换主控制账户；
c) 其他账户如要添加智能家电终端，须获得主控制账户授权，添加后才可获取智能家电终端控制权；
d) 若智能家电终端通过重置方式更换主控制账户，之前所有添加该设备的用户账户下的该设备应自动解除绑定关系。

4.1.2.2 配置安全

对于智能家电终端的配置安全要求包括：

a) 系统服务授权应遵循最小化原则，除必要服务端口以外，尽量减少对外开放端口数量，应默认关闭Telnet和SSH服务端口。
b) 对于能够安装外部应用的系统，应提供对系统API的访问控制机制，防止应用对系统接口的非授权调用。
c) 对于可配置服务的系统，应具备修改默认配置的功能，具体功能要求包含但不限于修改默认身份和认证信息、服务启用和禁用、应用访问限制和应用后台刷新、数据上传、数据下载限制及监控。
d) 系统登录口令宜具有一定复杂度要求，字符长度不少于八位，由大小写字母、数字和特殊符号中两种或两种以上类型组成。
e) 对于支持远程连接的设备，系统应使用安全的通信协议保障通道安全，包括具备建立通道时的身份鉴别和传输数据的机密性与完整性保护能力。
f) 对于通过Web进行远程管理的设备，对其进行管理和配置的行为必须经过登录认证，其登录/退出过程需有日志记录。记录内容应至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的IP地址等信息。

4.1.2.3 数据保护

智能家电终端对存储在设备内的重要数据提供安全防护，要求如下：

a) 本地存储的敏感数据应采用加密存储、限制读取等安全保护措施；
b) 智能家电终端网络端口不应泄露敏感信息。

4.1.2.4 日志记录

智能家电终端上应对网络操作生成相应的事件记录，并支持在控制端移动应用或管理端应用服务平台上查看。

4.1.2.5 固件安全

智能家电终端的固件通过网络或本地接口升级，升级后新版本固件代替原固件，在设备启动后运行。安全要求如下：

a) 固件更新前应得到用户确认；
b) 固件下载传输通道应确保可信，防止中间人劫持或者嗅探；
c) 对固件升级包、固件升级版本进行完整性校验和来源可靠性验证，校验通过后才允许升级；
d) 应确保固件中使用的第三方组件和开源软件不存在已知高危安全漏洞；

e) 在固件升级失败时，应保持在可用状态，并能重新接受平台的指令。

4.1.2.6 漏洞要求

智能家电终端系统软件应保证不含有 CNVD 与 CNNVD6 个月前公布的高危漏洞。

4.1.3 应用软件安全

4.1.3.1 应用安装

若智能家电终端支持安装第三方应用软件，安装应用时，智能家电终端应能识别应用的权限、证书等安全信息，供用户进行决策。

4.1.3.2 安全调用

若智能家电终端支持安装第三方应用软件，安装应用或执行敏感操作需由用户确认。敏感操作包括拨打电话、发送短信、开启/关闭无线接入、开启定位功能、开启照相机、后台截屏、记录语音等操作，以及对通讯录、通话记录、照片、视频等个人数据进行读、写、修改、删除等。

4.1.3.3 预置应用软件安全

终端中预置的应用软件不应有未向用户明示且未经用户同意，擅自收集或修改用户数据的行为。

4.1.4 接口安全

4.1.4.1 有线外围接口

若智能家电终端支持有线外围接口，当有线外围接口建立数据连接时，智能家电终端给用户相应的提示，仅当授权用户确认本次连接时，连接才可以建立。智能家电终端可采用安全协议保障有线外围接口通信的安全。

4.1.4.2 无线外围接口

若智能家电终端具备开关，可开启、关闭蜂窝网络、WLAN、蓝牙、红外、NFC 等无线接入方式功能。则当无线外围接口建立数据连接时，智能家电终端能够发现该连接并给用户相应的状态提示，仅当用户确认建立本次连接时，连接才可建立。用户可以监测数据传输状态，以防止非法连通、非法数据访问和数据传输等。智能家电终端可采用安全协议保障无线外围接口通信的安全。

4.1.4.3 外置存储设备

对于支持外置存储设备的智能家电终端，限制非授权应用软件对外置存储设备的访问。授权应用软件存储、移动、复制、转存重要数据至外置存储设备时，智能家电终端应提供加密机制。

4.2 控制端移动应用安全要求

4.2.1 身份鉴别

移动应用在连接云管理平台进行操作前，需要用户通过身份鉴别，并提供登录失败处理措施，包括如下要求：

a) 应自动拒绝设置不符合复杂度和长度要求的口令，口令至少限制 8 位及其以上和 2 种字符组合；
b) 修改或找回口令时，应对用户信息进行鉴权，通过用户名、手机号、短信验证码、安全问题等多重绑定对用户身份进行判断，保证用户身份的不可伪造性，防止任意口令重置；
c) 应提供登录失败处理功能，支持设置登录失败次数阈值和锁定时间，并当用户连续登录失败次数超过该阈值时，应通过验证图形验证码、验证短信验证码、锁定账户等方式限制登录；
d) 移动应用应使用验证码、 限定请求频率等方式防止利用注册、登录、找回密码等功能发起暴力破解、 拒绝服务等攻击。

4.2.2 源代码安全

移动应用源代码安全满足以下要求：

a) 移动应用的源代码应进行混淆处理；
b) 移动应用应具备源代码完整性校验能力；
c) 移动应用应对签名信息进行安全校验。

4.2.3 源代码数据安全

移动应用应删除移动应用中的冗余或注释代码。比如开发人员信息、调试信息等；

4.2.4 日志数据安全

移动应用日志数据安全满足以下要求：

a) 移动应用应对日志数据进行加密保护；

b) 移动应用应删除与移动应用运行逻辑相关的日志数据；

c) 移动应用应关闭调试日志输出功能，防止关键逻辑信息和重要数据信息泄露。

4.2.5 入侵防范

移动应用应提供数据有效性检验功能，保证通过人机接口输入或者通信接口输入的内容符合处理要求。

4.2.6 运行安全

移动应用运行安全满足以下要求：

a) 移动应用在安装过程中，不得安装功能说明文档中未说明的额外功能；

b) 移动应用应包含可有效表征供应者或者开发者身份的签名信息、软件属性信息；

c) 卸载时应能删除安装和使用过程中产生的资源文件、配置文件、用户数据和其他临时文件；

4.2.7 漏洞要求

控制端移动应用应确保使用的第三方库和开源组件 CNVD 与 CNNVD6 个月前公布的高危漏洞。

4.3 云管理平台安全要求

4.3.1 口令策略

智能家电云管理平台应对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

4.3.2 登录失败处理

智能家电云管理平台应具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

4.3.3 默认口令处理

智能家电云管理平台应重命名或删除默认账户，修改默认账户的默认口令。

4.3.4 访问控制策略

智能家电终端、移动应用和云管理平台各执行主体访问控制策略规定主体对客体的访问规则，不应存在越权访问系统功能模块或查看、操作其他用户数据。

4.3.5 安全审计措施

智能家电云管理平台应启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

4.3.6 数据有效性检验功能

智能家电云管理平台应提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求，不应出现由于校验机制缺失导致的应用系统存在如 SQL 注入、跨站脚本、上传漏洞等高风险漏洞。

4.3.7 漏洞要求

智能家电云管理平台件应保证不含有 CNVD 与 CNNVD6 个月前公布的高危漏洞。

4.4 数据传输安全要求

4.4.1 通信完整性

智能家电终端、移动应用和云管理平台各执行主体应采用检验技术和密码技术保证重要数据在传输和存储过程中的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

4.4.2 通信保密性

智能家电终端、移动应用和云管理平台各执行主体应采用检验技术和密码技术保证重要数据在传输和存储过程中的保密性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

4.4.3 抗数据重放

智能家电终端、移动应用和云管理平台各执行主体应能够鉴别数据的新鲜性，避免历史数据的重放攻击，应能够鉴别历史数据的非法修改，避免数据的修改重放攻击。

4.5 个人信息保护

4.5.1 收集信息授权同意

智能家电终端、移动应用和管理平台各执行主体在收集个人敏感信息时需经用户授权同意。

4.5.2 敏感信息匿名化

除必须用户确认的情况下，应对用户个人信息数据采取适当的匿名化措施，如：移动应用在显示个人信息（身份证号、手机号、邮箱、姓名等）应屏蔽部分关键字段。

5 测试方法

5.1 终端测试

5.1.1 硬件安全测试

5.1.1.1 设备标识测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：检查智能家电终端是否具备可用于通信识别的唯一标识。示例：设备 ID、序列号、MAC 地址等。

预期结果：

结果应符合本规范 4.1.1.1 中的要求。

5.1.1.2 安全启动测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过代码注入工具，调试启动过程，检查如下内容：

智能家电终端是否支持引入安全启动机制，系统启动按照用户设定的方式，建立初始环境，监督安全启动过程。开机时是否采用开机认证，系统启动后是否对操作系统装载信息，操作系统内核、硬件配置、关键应用等进行一致性校验。

预期结果：

结果应符合本规范 4.1.1.2 中的要求。

5.1.1.3 调试接口安全测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过调试接口编程器工具，检查如下内容：

a) 调试接口是否配置为限制使用；

b) 是否通过授权的方式管理调试端口的打开、关闭。

预期结果：

结果应符合本规范 4.1.1.3 中的要求。

5.1.2 系统软件安全

5.1.2.1 设备绑定测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：进行如下操作：

a) 将设备与某个帐户进行绑定操作，检查是否只有成功绑定之后才能进行网络控制操作；

b) 设备与某个主控制账户绑定后，尝试绑定其他主控制账户，查看是否可以绑定成功；

c) 在设备未重置前、且未经当前主控制账户授权的情况下更换主控制账户，查看是否可以更换；

d) 设备添加其他帐户，检查是否需要主控制帐户显示授权；

e) 将设备重置后，重新绑定新的主控制账户，检查之前添加的帐户下该设备是否已自动解绑。

预期结果：

结果应符合本规范 4.1.2.1 中的要求。

5.1.2.2 配置安全测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过扫描、数据嗅探、修改和重放等分析手段，检查如下内容：

a) 系统服务授权是否遵循最小化原则，除必要服务端口以外，是否尽量减少对外开放端口数量，是否默认关闭Telnet和SSH服务端口。

b) 对于能够安装外部应用的系统，是否提供对系统API的访问控制机制，防止应用对系统接口的非授权调用。

c) 对于可配置服务的系统，是否具备修改默认配置的功能，具体功能要求是否修改默认身份和认证信息、服务启用和禁用、应用访问限制和应用后台刷新、数据上传、数据下载限制及监控。

d) 系统登录口令是否具有一定复杂度要求，字符长度不少于八位，由大小写字母、数字和特殊符号中两种或两种以上类型组成。

e) 对于支持远程连接的设备，系统是否使用安全的通信协议保障通道安全，是否具备建立通道时的身份鉴别和传输数据的机密性与完整性保护能力。

f) 对于通过Web进行远程管理的设备，对其进行管理和配置的行为是否必须经过登录认证，其登录/退出过程是否有日志记录。记录内容是否至少包括登录使用的账号、登录是否成功、登录时间以及远程登录发起方的IP地址等信息。

预期结果：

结果应符合本规范 4.1.2.2 中的要求。

5.1.2.3 数据保护测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：检查本地存储的音视频数据是否采用加密存储、限制读取等安全保护措施。检查智能家电终端网络端口是否存在泄露敏感信息。

预期结果：

结果应符合本规范 4.1.2.3 中的要求。

5.1.2.4 日志记录测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：检查智能家电终端上是否对网络操作生成相应的事件记录，是否支持在移动应用上查看。

预期结果：

结果应符合本规范 4.1.2.4 中的要求。

5.1.2.5 固件安全测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：进行如下操作：

a) 选择固件升级,检查固件升级前是否对固件升级包、固件升级版本进行校验；

b) 扫描设备固件的漏洞，检查是否存在已知高危安全漏洞。

预期结果：

结果应符合本规范 4.1.2.5 中的要求。

5.1.2.6 漏洞要求测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过漏洞扫描，检查如下内容：

智能家电终端系统软件是否含有 CNVD 与 CNNVD6 个月前公布的高危漏洞。

预期结果：

结果应符合本规范 4.1.2.6 中的要求。

5.1.3 应用软件安全测试

5.1.3.1 应用安装测试

若智能家电终端支持安装第三方应用软件，安装应用时，智能家电终端是否能识别应用的权限、证书等安全信息，供用户进行决策。

预期结果：

结果应符合本规范 4.1.3.1 中的要求。

5.1.3.2 安全调用测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过漏洞扫描，检查如下内容：

若智能家电终端支持安装第三方应用软件，安装应用或执行敏感操作是否需由用户确认。敏感操作包括拨打电话、发送短信、开启/关闭无线接入、开启定位功能、开启照相机、后台截屏、记录语音等操作，以及对通讯录、通话记录、照片、视频等个人数据进行读、写、修改、删除等。

预期结果：

结果应符合本规范 4.1.3.2 中的要求。

5.1.3.3 预置应用软件安全测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过数据嗅探、修改和重放等分析手段，检查如下内容：

终端中预置的应用软件是否有未向用户明示且未经用户同意，擅自收集或修改用户数据的行为。

预期结果：

结果应符合本规范 4.1.3.3 中的要求。

5.1.4 接口安全测试

5.1.4.1 有线外围接口测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过数据嗅探、修改和重放等分析手段，检查如下内容：

若智能家电终端支持有线外围接口，当有线外围接口建立数据连接时，智能家电终端是否给用户相应的提示，是否仅当授权用户确认本次连接时，连接才可以建立。智能家电终端是否采用安全协议保障有线外围接口通信的安全。

预期结果：

结果应符合本规范 4.1.4.1 中的要求。

5.1.4.2 无线外围接口测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过数据嗅探、修改和重放等分析手段，检查如下内容：

若智能家电终端具备开关，可开启、关闭蜂窝网络、WLAN、蓝牙、红外、NFC 等无线接入方式功能。则当无线外围接口建立数据连接时，智能家电终端是否能够发现该连接并给用户相应的状态提示，是否仅当用户确认建立本次连接时，连接才可建立。用户是否可以监测数据传输状态，以防止非法连通、非法数

据访问和数据传输等。智能家电终端是否采用安全协议保障无线外围接口通信的安全。
预期结果：
结果应符合本规范 4.1.4.2 中的要求。
5.1.4.3 外置存储设备测试
测试步骤：
步骤一：使智能家电终端和移动应用处于正常工作状态；
步骤二：通过数据嗅探、修改和重放等分析手段，检查如下内容：
对于支持外置存储设备的智能家电终端，是否限制非授权应用软件对外置存储设备的访问。是否授权应用软件存储、移动、复制、转存重要数据至外置存储设备时，智能家电终端是否提供加密机制。
预期结果：
结果应符合本规范 4.1.4.3 中的要求。

5.2 移动应用测试

5.2.1 身份鉴别测试

测试步骤：
步骤一：使智能家电终端和移动应用处于正常工作状态；
步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查如下内容：
a) 是否自动拒绝设置不符合复杂度和长度要求的口令，口令至少限制 8 位及其以上和 2 种字符组合；
b) 修改或找回口令时，是否对用户信息进行鉴权，通过用户名、手机号、短信验证码、安全问题等多重绑定对用户身份进行判断，是否存在任意口令重置漏洞；
c) 应提供登录失败处理功能，支持设置登录失败次数阈值和锁定时间，并当用户连续登录失败次数超过该阈值时，应通过验证图形验证码、验证短信验证码、锁定账户等方式限制登录；
d) 用户登录后长时间不进行任何操作，检查是否会对当前账号进行锁定或注销；
e) 检查控制端应用是否对注册、登录、找回密码过程采用验证码机制进行验证，是否对请求发起频率进行限制。
预期结果：
结果应符合本规范 4.2.1 中的要求。

5.2.2 源代码安全测试

测试步骤：
步骤一：使智能家电终端和移动应用处于正常工作状态；
步骤二：通过移动应用安全分析平台自动化扫描，检查如下内容：
a) 移动应用的源代码是否进行混淆处理；
b) 移动应用是否具备源代码完整性校验能力；
c) 移动应用是否对签名信息进行安全校验。
预期结果：
结果应符合本规范 4.2.2 中的要求。

5.2.3 源代码数据安全测试

测试步骤：
步骤一：使智能家电终端和移动应用处于正常工作状态；
步骤二：通过移动应用安全分析平台自动化扫描，检查如下内容：
移动应用是否存在冗余或注释代码。比如开发人员信息、调试信息等。
预期结果：
结果应符合本规范 4.2.3 中的要求。

5.2.4 日志数据安全测试

测试步骤：
步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过移动应用安全分析平台自动化扫描，检查如下内容：

a) 移动应用是否对日志数据进行加密保护；

b) 移动应用是否删除与移动应用运行逻辑相关的日志数据；

c) 移动应用是否关闭调试日志输出功能，是否存在关键逻辑信息和重要数据信息泄露。

预期结果：

结果应符合本规范 4.2.4 中的要求。

5.2.5 入侵防范测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过移动应用安全分析平台自动化扫描，检查如下内容：

移动应用是否提供数据有效性检验功能，是否能保证通过人机接口输入或者通信接口输入的内容符合处理要求。

预期结果：

结果应符合本规范 4.2.5 中的要求。

5.2.6 运行安全测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过移动应用安全分析平台自动化扫描，检查如下内容：

a) 移动应用在安装过程中，是否安装功能说明文档中未说明的额外功能；

b) 移动应用是否包含可有效表征供应者或者开发者身份的签名信息、软件属性信息；

c) 卸载时是否能删除安装和使用过程中产生的资源文件、配置文件、 用户数据和其他临时文件；

预期结果：

结果应符合本规范 4.2.6 中的要求。

5.2.7 漏洞要求测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过移动应用安全分析平台自动化扫描，检查如下内容：

控制端移动应用使用的第三方库和开源组件是否存在 CNVD 与 CNNVD6 个月前公布的高危漏洞。

预期结果：

结果应符合本规范 4.2.7 中的要求。

5.3 云管理平台安全测试

5.3.1 口令策略测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查如下内容：

是否对登录的用户进行身份标识和鉴别，身份标识具有唯一性，身份鉴别信息具有复杂度要求并定期更换。

预期结果：

结果应符合本规范 4.3.1 中的要求。

5.3.2 登录失败处理测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查如下内容：

是否具有登录失败处理功能，应配置并启用结束会话、限制非法登录次数和当登录连接超时自动退出等相关措施。

预期结果：

结果应符合本规范 4.3.2 中的要求。

5.3.3 默认口令处理测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查如下内容：

是否重命名或删除默认账户，修改默认账户的默认口令。

预期结果：

结果应符合本规范 4.3.3 中的要求。

5.3.4 访问控制策略测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查如下内容：

智能家电终端、移动应用和云管理平台各执行主体访问控制策略规定主体对客体的访问规则，是否存在越权访问系统功能模块或查看、操作其他用户数据。

预期结果：

结果应符合本规范 4.3.4 中的要求。

5.3.5 安全审计措施测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查如下内容：

是否启用安全审计功能，审计覆盖到每个用户，对重要的用户行为和重要安全事件进行审计。

预期结果：

结果应符合本规范 4.3.5 中的要求。

5.3.6 数据有效性检验功能测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查如下内容：

是否提供数据有效性检验功能，保证通过人机接口输入或通过通信接口输入的内容符合系统设定要求，是否出现由于校验机制缺失导致的应用系统存在如 SQL 注入、跨站脚本、上传漏洞等高风险漏洞。

预期结果：

结果应符合本规范 4.3.6 中的要求。

5.3.7 漏洞要求测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查如下内容：

智能家电云管理平台件是否保证不含有 CNVD 与 CNNVD6 个月前公布的高危漏洞。

预期结果：

结果应符合本规范 4.3.7 中的要求。

5.4 数据传输安全测试

5.4.1 数据传输完整性测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查是否采用检验技术和密码技术保证重要数据在传输和存储过程中的完整性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、

重要视频数据和重要个人信息等。

预期结果：

结果应符合本规范4.4.1中的要求。

5.4.2 数据传输可用性测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查是否采用检验技术和密码技术保证重要数据在传输和存储过程中的保密性，包括鉴别数据、重要业务数据、重要审计数据、重要配置数据、重要视频数据和重要个人信息等。

预期结果：

结果应符合本规范4.4.2中的要求。

5.4.3 抗数据重放测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：通过网络数据包嗅探、修改和重放等分析手段，检查是否能够鉴别数据的新鲜性，是否能避免历史数据的重放攻击，是否能够鉴别历史数据的非法修改，是否能避免数据的修改重放攻击。

预期结果：

结果应符合本规范 4.4.3 中的要求。

5.5 个人信息保护测试

5.5.1 收集信息授权同意测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：遍历智能家电终端各功能，检查智能家电终端、移动应用和管理平台各执行主体在收集个人敏感信息时需经用户授权同意。

预期结果：

结果应符合本规范 4.5.1 中的要求。

5.5.2 敏感信息匿名化测试

测试步骤：

步骤一：使智能家电终端和移动应用处于正常工作状态；

步骤二：遍历智能家电终端各功能，检查是否对用户个人信息数据采取适当的匿名化措施，如：移动应用在显示个人信息（身份证号、手机号、邮箱、姓名等）应屏蔽部分关键字段。

预期结果：

结果应符合本规范 4.5.2 中的要求。

参 考 文 献

[1] NIST SP800-183 Network of “Things”

[2] ISO/IEC 27030 Guidelines for security and privacy in Internet of Things (IoT)

[3] ISO/IEC 27033 Information technology -- Security techniques -- Network security

[4] ISO/IEC 9798 Information technology -- Security techniques -- Entity authentication

[5] ISO/IEC 27034 Information technology -- Security techniques -- Application security