广州赛宝认证中心服务有限公司技术规范

CEPREI-003-CTS-2020

智能安全认证—智能摄像产品技术规范

（第一版）

2020-05-22 发布　　2020-05-22 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、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、朱文立、彭琦、李乐言、赖怡聪、李荣、胡雄锋、黄伟明。

换版说明：本次换版变更技术规范名称为《智能安全认证-智能摄像产品技术规范》，修改了术语、定义和缩略语描述，更新技术要求和测试方法。除编辑性修改外主要技术变化如下：

——删除“管理平台”、“敏感信息”、“授权”、“传输安全”、“可用性”和“新鲜性”术语和定义；

——新增“设备绑定”（见4.1.2）；

——修改“身份鉴别”为“接入鉴别”（见4.1.3，第一版的4.1.3）；

——新增“数据保护”（见4.1.4）；

——删除“固件更新”（见第一版4.1.2）；

——新增“固件安全”（见4.1.5）；

——删除“源代码安全”、“源代码数据安全”、“运行环境安全”、“组件安全”、“日志数据安全”、“存储数据安全”和“第三方库安全”（见第一版4.2.1至4.2.7）；

——新增“身份鉴别”、“权限控制”和“代码安全”（见4.2.1、4.2.2和4.2.3）；

——删除“管理平台要求”（见第一版4.3）；

——删除“数据传输可用性”和“数据传输隐私”（见第一版4.4.2和4.4.3）

——新增“通信保密性”和“抗数据重放”（见4.3.2和4.3.4）

——新增“个人信息保护”（见4.4）

——新增“设备绑定测试”（见5.1.2）；

——修改“身份鉴别测试”为“接入鉴别测试”（见5.1.3，第一版的5.2.3）；

——新增“数据保护测试”（见5.1.4）；

——删除“固件更新测试”（见第一版5.2.2）；

——新增“固件安全测试”（见5.1.5）；

——删除“源代码安全测试”、“源代码数据安全测试”、“运行环境安全测试”、“组件安全测试”、“日志数据安全测试”、“存储数据安全测试”和“第三方库安全测试”（见第一版5.3.1至5.3.7）；

——新增“身份鉴别测试”、“权限控制测试”和“代码安全测试”（见5.2.1、5.2.2和5.2.3）；

——删除“管理平台测试”（见第一版5.4）；

——删除“数据传输可用性”和“数据传输隐私”（见第一版5.5.2和5.5.3）

——新增“通信保密性”和“抗数据重放”（见5.3.2和5.3.4）

——新增“个人信息保护”（见5.4）

智能安全认证—智能摄像产品技术规范

1 范围

本规范规定了智能摄像产品的术语和定义、技术要求和测试方法。

本规范所指的智能摄像产品是指物联网感知层中用于单向读取图像，并可以通过网络进行数据传输和控制的摄像机。

本规范适用的产品范围为：云台网络摄像机、高清网络摄像机、半球网络摄像机、红外网络摄像机、枪式网络摄像机、变速球型摄像机、无线网络摄像机及其它可以通过网络进行数据传输和控制的网络摄像产品。

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 35273-2017 个人信息安全技术个人信息安全规范

GB 35114-2017 公共安全视频监控联网信息安全技术要求

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 设备标识

智能摄像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。

4.1.2 设备绑定

用户使用智能摄像终端前，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) 智能摄像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) 一个智能摄像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摄像终端，须获得主控制账户授权，添加后才可获取智能摄像终端控制权；
d) 若智能摄像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。

4.1.3 接入鉴别

4.1.3.1 接入认证机制

智能摄像终端应具备对接入信息的身份鉴别功能，应提供用户身份标识唯一和鉴别信息复杂度检查功能，保证不存在重复用户身份标识，身份鉴别信息不易被冒用，并至少支持下列方式的一种：

a) 基于智能摄像终端标识和接入口令的单向认证；
b) 基于预共享密钥的单向或双向认证。

4.1.3.2 认证失败处理

智能摄像终端应具备接入认证失败的处理能力，应提供登录失败处理功能，可采取结束会话，限制非法登录次数和自动退出等措施。应满足以下要求：

a) 当认证超时，接入系统应能终止与待接入智能摄像终端之间的当前会话；
b) 在经过一定次数的鉴别失败以后，接入系统应能终止由该智能摄像终端发起的建立会话的尝试，并在一定的安全时间间隔后才能恢复。

4.1.4 数据保护

智能摄像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) 智能摄像终端网络端口不应泄露敏感信息。

4.1.5 固件安全

智能摄像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) 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；
b) 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。

4.1.6 日志记录

智能摄像终端上应对网络操作生成相应的事件记录，并支持在移动应用上查看。

4.2 移动应用要求

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 权限控制

智能摄像终端、移动应用和云管理平台各执行主体应授予不同帐户为完成各自承担任务所需的最小权限，并在它们之间形成相互制约的关系。

4.2.3 代码安全

移动应用代码安全满足以下要求：

a) 移动应用应具备防逆向反编译功能，抵抗对关键代码和数据的分析， 避免关键业务逻辑被破解分析和篡改；
b) 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；
c) 移动应用应确保使用的第三方库和开源组件不存在已公布的高危漏洞；
d) 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。

4.3 数据传输安全要求

4.3.1 通信完整性

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。

4.3.2 通信保密性

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。

4.3.3 抗数据重放

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。

4.4 个人信息保护

4.4.1 收集信息授权同意

智能摄像终端、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。

4.4.2 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 设备标识测试

测试步骤：

步骤一：使智能摄像产品和移动应用处于正常工作状态；

步骤二：检查智能摄像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 中的要求。

5.1.2 设备绑定测试

测试步骤：

步骤一：使智能摄像产品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 中的要求。

5.1.3 接入鉴别测试

测试步骤：

步骤一：使智能摄像产品和移动应用处于正常工作状态；

步骤二：检查智能摄像终端是否具备对接入信息的身份鉴别功能，是否提供用户身份标识唯一和鉴别信息复杂度检查功能，保证不存在重复用户身份标识，身份鉴别信息不易被冒用。

预期结果：

结果应符合本规范 4.1.3 中的要求。

5.1.4 数据保护测试

测试步骤：

步骤一：使智能摄像产品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。检查智能摄像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 4.1.4 中的要求。

5.1.5 固件安全测试

测试步骤：

步骤一：使智能摄像产品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 4.1.5 中的要求。

5.1.6 日志记录测试

测试步骤：

步骤一：使智能摄像产品和移动应用处于正常工作状态；

步骤二：检查智能摄像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 4.1.6 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：使智能摄像产品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 权限控制测试

测试步骤：

步骤一：使智能摄像产品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，检测智能摄像终端、移动应用和云管理平台各执行主体是否授予不同帐户为完成各自承担任务所需的最小权限，是否在它们之间形成相互制约的关系。

预期结果：

结果应符合本规范 4.2.2 中的要求。

5.2.3 代码安全测试

测试步骤：

步骤一：使智能摄像产品和移动应用处于正常工作状态，使移动应用软件信息安全测试系统（包括服务器和客户端软件）处于正常工作状态；

步骤二：使用基于特征码扫描、静态源码分析、动态行为监控等方法，检测如下内容：

a) 检查控制端应用是否具备防逆向反编译功能；

b) 检查控制端应用发布版本是否输出调试日志；

c) 检查控制端应用使用的第三方库和开源组件是否存在已公布的高危漏洞；

d) 构造错误的或畸形的输入内容，检查控制端应用是否具有数据有效性检验功能。

预期结果：

结果应符合本规范 4.2.3 中的要求。

5.3 数据传输安全测试

5.3.1 数据传输完整性测试

测试步骤：

步骤一：使智能摄像产品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4.3.1中的要求。

5.3.2 数据传输可用性测试

测试步骤：

步骤一：使智能摄像产品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4.3.2中的要求。

5.3.3 抗数据重放测试

测试步骤：

步骤一：使智能摄像产品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 4.3.3 中的要求。

5.4 个人信息保护测试

5.4.1 收集信息授权同意测试

测试步骤：

步骤一：使智能摄像产品和移动应用处于正常工作状态；

步骤二：遍历智能摄像产品各功能，检查智能摄像终端、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 4.4.1 中的要求。

5.4.2 敏感信息匿名化测试

测试步骤：

步骤一：使智能摄像产品和移动应用处于正常工作状态；

步骤二：遍历智能摄像产品各功能，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 4.4.2 中的要求。

参 考 文 献

[1] Vetting the Security of Mobile Applications,Steve Quirolgico, Jeffrey Voas. Tom Karygiannis. 2015

[2] The MITRE Corporation, Common Vulnerabilities and Exposures (CVE) [Web site], https://cve.mitre.org/

[3] NIST, Security Content Automation Protocol (SCAP) [Web site], http://scap.nist.gov/ (accessed 12/4/14).

[4] NIST SP 800-163 http://nvlpubs.nist.gov/nistpubs/SpecialPublications.

[5] OWASP Mobile TOP 10 Risks https://www.owasp.org/index.php/Mobile_Top_10_2016-Top_10.