ICS 33.050
M 30

团　体　标　准

T/TAF 086-2021

智能电视安全能力技术要求和测试方法

Technical requirements and test methods for security capabilities of smart television

2021-05-12 发布　　2021-05-12 实施

电信终端产业协会　发布

目　　次

前　言

本文件按照 GB/T 1.1-2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件凡涉及密码算法的相关内容，按国家有关法规实施；凡涉及到采用密码技术解决保密性、完整性、真实性、不可否认性需求的应遵循密码相关国家标准和行业标准。

本文件中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。

本文件由电信终端产业协会提出并归口。

本文件起草单位：中国信息通信研究院，百度在线网络技术（北京）有限公司，联想（北京）有限公司，高通无线通信技术(中国)有限公司，郑州信大捷安信息技术股份有限公司，小米科技有限责任公司，青岛海信通信有限公司，青岛海尔通信有限公司，北京豆荚科技有限公司，惠州 TCL 移动通信有限公司，深圳康佳通信科技有限公司、四川长虹信息技术有限责任公司。

本文件主要起草人：唐佳伟、王海棠、吴月升、宁华、刘陶、杜云、王婧琦、李汝鑫、王江胜、刘为华、康亮、陈灿峰、郑梁、刘新平、窦丽娟、林舜大、卢小涛、唐博、黄德俊。

引　　言

智能电视，是基于互联网应用技术，拥有开放式应用平台，可实现双向人机交互功能，集影音、娱乐、数据等多种功能于一体，以满足用户多样化和个性化需求的电视产品。科技在给用户带来新的应用体验的同时，也带来了很多安全风险，如用户隐私泄漏、内容劫持、第三方应用静默安装等。为提高智能电视的安全能力，促进我国智能电视安全生态的稳定发展，制定本文件。

本文件主要对智能电视安全能力提出技术要求，并根据设备达到的安全能力，对智能电视进行分级，同时设计相应的测试方法。

智能电视安全能力技术要求和测试方法

1 范围

本文件规定了智能电视的硬件，操作系统，预置应用，第三方应用，网络通信和人工智能服务 6 个方面的安全能力，并从基本的安全保障、实现难度、安全能力等层面对智能电视安全能力进行分级，制定相应的测试方法

本文件适用于提供互联网内容服务的智能电视设备

本文件适用于智能电视的设计、开发、测试和评估

本文件仅提出智能电视安全能力技术要求和测试方法，对具体技术实现方式不作规定。

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 35273-2020 信息安全技术 个人信息安全规范

GB XXX-XXX 互联网电视接收设备技术规范

SJ/T 11688-2017 智能电视智能化技术评价方法

GY/T 277-2019 视音频内容分发数字版权管理技术规范

T/TAF 071.1-2020 智能家居终端设备 通用安全能力技术要求

3 术语和定义

3.1

智能电视 smart TV

具有操作系统、能安装和卸载应用软件、具备一种或多种人机交互方式，接入互联网或其他网络并实现网络服务，可扩展其他应用或业务的电视终端。

注：本文件不包括机顶盒或集成在电视中的机顶盒。

3.2

超级用户 superuser

一种用于进行系统管理的特殊用户。超级用户拥有最高权限，能够进行全系统的配置、维护等工作。

3.3

固件 firmware

存储在加密边界硬件中的加密模块的可行性代码，在不可修改或受限操作环境中运行时，不能被动态写入或修改。

注：存储硬件包括但不限于PROM，EEPROM，FLASH，固态存储器，硬盘驱动器等。

3.4

通用口令 universal code

指智能电视网络系统中初始设定的口令。通过通用口令，攻击者可以轻易的获取操作权限，进行进一步的入侵。

3.5

预置应用 pre-installed applications

预置应用是指由智能电视厂商自行或与互联网信息服务提供者合作在智能电视出厂前安装在其系统中的应用程序。

3.6

第三方应用 third-party applications

指非智能电视厂商自行或与互联网信息服务提供者合作在智能电视出厂前安装的应用软件，以及非系统升级时新增加的应用软件。

3.7

隐藏语音命令 hidden voice commands

对用户来说无法理解，但可以被设备理解的指令。

3.8 缩略语

下列缩略语适用于本文件。

API：应用程序编程接口（Application Programming Interface）

APP：应用 （Application）

AI：人工智能（Artificial Intelligence）

CNVD：国家信息安全漏洞共享平台（China National Vulnerability Database）

CNNVD：中国国家信息安全漏洞库（China National Vulnerability Database of Information Security）

DNS：域名系统（Domain Name System）

DLNA：数字生活网络联盟（Digital Living Network Alliance）

DRM：数字版权管理（Digital Rights Management）

HTTP：超文本传输协议（Hyper Text Transfer Protocol）

HTTPS：超文本传输安全协议（Hyper Text Transfer Protocol over Secure Socket Layer）

ITVID：互联网电视接收设备标识（Internet TV Receiving Device Identification）

SSH：安全外壳协议（Secure Shell）

SSL：安全套接层（Secure Socket Layer）

WLAN：无线局域网络（Wireless Local Area Networks）

TEE：可信执行环境（Trusted Execution Environment）

TLS：安全传输协议（Transport Layer Security）
TV：电视（Television）
USB：通用串行总线（Universal Serial Bus）

4 智能电视安全架构

4.1 概述

图1为智能电视安全能力框架，主要包含6个部分：最底层是智能电视硬件安全能力，之上为操作系统安全能力，顶层为预置应用安全能力和第三方应用安全能力，网络通信安全能力和人工智能安全能力涉及上述层面。个人信息处理活动应遵照GB/T 35273相应部分的规定执行。数字版权保护相关技术要求应参照GY/T 277-2019相应部分的规定执行。

图1 智能电视安全能力架构图

其中：

a) 硬件安全能力：保障智能电视存储安全及处理芯片安全，避免芯片内的操作系统、数据、程序等被非法获取或者篡改；
b) 操作系统安全能力：对智能电视操作系统进行安全配置，提出相应的安全要求，利用操作系统及其接口保护智能电视业务及应用的权限与安全性；
c) 预置应用安全能力：智能电视出厂时会预置一些常见的应用，如娱乐播放、视频通信等，智能电视应对这些预置应用做出安全要求，使其不可进行越权、恶意收集敏感数据或盗取媒体内容等操作；
d) 第三方应用安全能力：部分智能电视支持用户安装第三方应用，智能电视应对这些应用来源的合法性进行验证，并对应用的安装进行鉴权，防止攻击者利用恶意应用进行非法操作；
e) 网络通信安全能力：保障智能电视通信安全，包括WLAN、蓝牙等通信协议安全以及传输层通信协议安全；
f) 人工智能服务安全能力：对于提供AI服务的智能电视，AI服务应具备抵抗模型窃取或机器学习对抗性攻击等恶意行为的能力，防止攻击者借助人工智能服务进行恶意操作。

5 智能电视安全能力技术要求

5.1 硬件安全能力

5.1.1 可调试物理接口安全

a) 智能电视保留可调试物理接口（包括但不局限于 JTAG，串口等），可调试物理接口不向用户开放。

b) 智能电视保留可调试物理接口，可调试物理接口访问受限，如非拆机状态下不可访问或用户访问需要进行口令认证；

c) 智能电视保留可调试物理接口，访问可调试物理接口采用非通用口令认证或证书认证。

d) 智能电视保留可调试物理接口，访问可调试物理接口采用证书认证，且证书保存在 TEE 或安全芯片中。

5.1.2 存储安全

a) 硬件平台应具备不可改写的用于存储校验密钥、ITVID 等信息的安全存储区域。

b) 应支持对存储在芯片内的固件等重要数据进行签名以及签名验证；

c) 应支持对存储在芯片内的固件进行签名以及签名验证；

d) 芯片支持对安全要求不同的应用区提供不同等级的安全管理机制；

e) 存储在芯片内的用户数据以密文形式存在。

5.1.3 硬件实现密码算法

a) 智能电视使用安全芯片实现密码算法。

b) 智能电视应使用安全芯片实现视频加解密算法。

5.1.4 外部存储设备接入安全要求

a) 智能电视接入外部存储设备时，应给予用户相应的提示。

5.2 操作系统安全能力

5.2.1 安全启动

a) 智能电视应对启动过程中每个步骤加载的组件验证签名的正确性，包括但不限于引导加载程序、内核、内核扩展项，确保系统分区不被恶意程序修改，校验根密钥受硬件保护，不可修改。

b) 开机广告须提供 “一键关闭”功能。

5.2.2 固件安全

智能电视编译固件时，应去除二进制固件中的符号表信息，增加固件调试及破解的难度。进行加密加固等措施。

5.2.3 系统配置安全

a) 默认关闭操作系统调试接口和远程登录端口（如 SSH 端口和 Telnet 端口）。

b） 核心系统守护进程和业务应用应隔离到不同的安全域，并为每个域定义不同的访问策略。

5.2.4 系统与固件更新安全

a） 离线方式进行系统与固件升级时，应对升级文件的完整性进行校验，包括验证升级包的哈希值、大小、版本号和签名；

b） 在线方式进行系统与固件升级时，应对升级文件的来源和完整性进行校验，包括验证升级包的哈希值、大小、版本号和签名；

c） 进行系统与固件更新，当发生更新失败时，不应出现系统不可用的情况。

d） 提醒用户进行升级，并给出最新版本号以及更新内容简要说明。

e） 在线方式进行系统与固件升级时，应对升级包文件进行加密；

f） 紧急情况下可在线强制升级，若需强制升级，应提示并告知用户原因；

5.2.5 漏洞修复

a） 系统应保证不包含有 CNVD 与 CNNVD 6 个月前公布的中危及以上漏洞；

b） 应支持高危漏洞修复及安全防御机制。

5.2.6 端口安全

按需进行服务端口的打开，或开放系统端口时进行访问控制。

5.2.7 权限管理

a） 应默认禁止系统用户或应用获取系统的超级用户权限。

b） 应为系统进程进行分组，并对不同的组配置相应的文件访问权限；

5.3 预置应用软件安全能力

5.3.1 遥控端认证

a） 智能电视使用射频或蓝牙遥控器时，射频或蓝牙遥控器应支持与智能电视之间的双向认证配对；

b） 智能电视应对遥控端APP实施身份认证，以防止非授权的操作；或支持在使用遥控端APP执行敏操作时，通过验证码等手段进行二次校验，同时验证码应限制一定时间内的尝试频次，以防止暴力破解。

5.3.2 软件安装安全

a） 预置应用软件不应存在 CNVD 和 CNNVD 6 个月前公布的高危漏洞。

b） 智能电视应对获取应用过程中与服务器的相关通信进行证书验证。

5.3.3 软件更新安全

a） 进行更新时，应对更新包进行版本号、哈希值、签名和文件大小校验；

b） 进行预装应用软件更新时，应对软件更新包进行加密。

5.3.4 身份凭证

a) 应验证登录应用的用户身份及凭据的有效性，采用二维码扫描或用户名密码登录方式；
b) 应验证登录应用的用户身份及凭据的有效性，采用二维码扫描或用户名密码登录方式，并对登入用户设置一定的有效期，超过有效期需要用户进行重新登录；
c) 应验证登录应用的用户身份及凭据的有效性，宜支持生物特征认证登录形式。

5.4 第三方应用软件安全能力

5.4.1 软件安装安全

a) 应不允许安装未签名应用或者不受信任的代码，禁止安装未授权的第三方应用软件。
b) 智能电视应对获取应用安装过程中与服务器的相关通信进行证书验证；
c) 应用安装应经过电视厂商的安全校验。

5.5 网络通信安全能力

5.5.1 协议一致性

智能电视在采用 WLAN、蓝牙等无线传输协议时，应准照 T/TAF 071.1-2020 中 5.6 章节实现设备授权认证、加密传输等安全功能。

5.5.2 数据传输安全

a) 智能电视应支持对称加密算法对用户数据进行加密传输保护。支持安全 OS 和安全存储，对称密钥应进行安全存储保护；
b) 智能电视应支持 TLS 协议对用户数据进行安全传输，应使用 TLS V1.2 及以上版本， TLS V1.0 和 TLS V1.1 默认关闭，禁止使用 SSL V2 及 SSL V3；
c) 智能电视采用的 TLS 协议应使用 128 位或更强的加密、认证套件；
d) 安全传输协议应具备抵抗因编程语言固有缺陷造成的安全漏洞，如使用可抵抗内存安全漏洞的传输层协议。
e) 智能电视宜支持手机投屏 HDCP 协议

5.5.3 DNS 劫持

a) 智能电视应具备检测 DNS 劫持的能力；
b) 智能电视应具备修复 DNS 劫持的能力。

5.6 人工智能服务安全能力

5.6.1 上传数据安全

应防止攻击者将用户使用人工智能功能时的交互数据上传指向到自己的服务器，如设置上传服务器地址是不可配置的。

5.6.2 对抗性攻击防护

a） 智能电视机器学习算法应具备抵抗对抗性攻击的能力，如可抵抗隐藏语音命令攻击等。

5.6.3 机器学习模型隐私保护

应对机器学习模型进行安全保护，以保护机器学习模型不被非法窃取，如为机器学习模型参数或预测API接口设置一定的访问控制机制，使之不可被公开获取。机器学习模型可被限制在TEE加载和运行，保护隐私数据不被非法获取。

6 智能电视安全能力分级

6.1 概述

智能电视所支持的安全能力划分为5个等级，第五级是最高等级。智能电视可选择支持到不同的等级。达到相应等级的智能电视可在说明书上进行明确标识。

6.2 安全能力分级

根据智能电视所支持的安全能力程度，将智能电视的安全能力自高到低划分为 5 个等级。在每一等级定义了智能电视对应的安全能力的最小集合，也就是智能电视必须支持该集合中的所有安全能力才能标识为该级别，例如达到第五级的智能电视应支持本文件第五章所定义的所有安全能力。具体的等级划分详见表 1.

表 1 智能电视安全能力分级

安全能力		安全能力等级				
		一级	二级	三级	四级	五级
1	5.1.1 可调试物理接口安全	√	√	√	√	√
2	5.1.2 存储安全	√	√	√	√	√
3	5.1.3 硬件实现密码算法	-	-	-	√	√
4	5.1.4 外部存储设备接入安全要求	√	√	√	√	√
5	5.2.1 安全启动	√	√	√	√	√
6	5.2.2 固件安全	-	-	√	√	√
7	5.2.3 系统配置安全	√	√	√	√	√
8	5.2.4 系统与固件更新安全	√	√	√	√	√
9	5.2.5 漏洞修复	-	-	√	√	√
10	5.2.6 端口安全	-	-	-	√	√
11	5.2.7 权限管理	-	-	√	√	√
12	5.3.1 遥控端认证	-	-	√	√	√
13	5.3.2 软件安装安全	-	√	√	√	√
14	5.3.3 软件更新安全	-	√	√	√	√
15	5.3.4 身份凭证	-	-	√	√	√
16	5.4.1 软件安装安全	√	√	√	√	√
17	5.5.1 协议一致性	√	√	√	√	√

表 1　智能电视安全能力分级（续）

安全能力		安全能力等级				
		一级	二级	三级	四级	五级
18	5.5.2 数据传输安全	√	√	√	√	√
19	5.5.3 DNS 劫持	-	-	√	√	√
20	5.6.1 上传数据安全	-	-	-	√	√
21	5.6.2 对抗性攻击防护	-	-	-	-	√
22	5.6.3 机器学习模型隐私保护	-	-	-	-	√

7　智能电视安全能力测试方法

7.1 概述

本章节按照智能电视的最高安全能力要求，即四级安全要求给出测试方法。智能电视可根据支持的安全能力等级，进行相应的安全能力测试项。

7.2 硬件安全能力测试项

7.2.1　可调试物理接口安全测试项

7.2.1.1 测试项 HW-1

测试项目：智能电视保留可调试物理接口，可调试物理接口不向用户开放。

测试步骤：

步骤 1：检查厂商提交的文档，查看被测智能电视的接口设计文档，检查智能电视是否保留可调试物理接口；

步骤 2：模拟用户通过调试命令连接可调试物理接口，查看可调试物理接口是否向用户开放。

预期结果：

在步骤 1 之后，若智能电视不存在可调试物理接口，测评结果为“未见异常”，测评结束；否则进行步骤 2；

在步骤 2 之后，若可调试物理接口未向用户开放，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.1.2 测试项 HW-2

测试项目：智能电视保留可调试物理接口，可调试物理接口访问受限，如非拆机状态下不可访问或用户访问需要进行口令认证。

测试步骤：

步骤 1：检查厂商提交的文档，查看被测智能电视的接口设计文档，检查智能电视是否保留可调试物理接口；

步骤 2：模拟用户通过调试命令连接可调试物理接口，查看访问可调试物理接口是否采用了一定的保护机制，如非拆机状态不可访问，或访问需要进行用户名口令认证。

预期结果：

在步骤 1 之后，若智能电视不存在可调试物理接口，测评结果为“未见异常”，测评结束；否则进行步骤 2；

在步骤 2 之后，若访问智能电视可调试接口采用了一定的限制措施，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.1.3 测试项 HW-3

测试项目：智能电视保留可调试物理接口，访问可调试物理接口采用非通用口令认证或证书认证。

测试步骤：

步骤 1：检查厂商提交的文档，查看被测智能电视的接口设计文档，检查智能电视是否保留可调试物理接口；

步骤 2：模拟用户通过调试命令连接可调试物理接口，查看可调试物理接口是否对用户进行非通用口令或证书认证。

预期结果：

在步骤 1 之后，若智能电视不存在可调试物理接口，测评结果为“未见异常”，测评结束；否则进行步骤 2；

在步骤 2 之后，若访问可调试物理接口需要用户使用非通用口令或证书进行认证，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.1.4 测试项 HW-4

测试项目：智能电视保留可调试物理接口，访问可调试物理接口采用证书认证，且证书保存在 TEE 或安全芯片中。

测试步骤：

步骤 1：检查厂商提交的文档，查看被测智能电视的接口设计文档，检查智能电视是否保留可调试物理接口；

步骤 2：模拟用户通过调试命令连接可调试物理接口，查看可调试物理接口是否对访问用户进行证书认证；

步骤 3：步骤 2 之后，检查访问可调试物理接口的用户证书存储模式，是否将证书存储在 TEE 或安全芯片中。

预期结果：

在步骤 1 之后，若智能电视不存在可调试物理接口，测评结果为“未见异常”，测评结束；否则进行步骤 2；

在步骤 2 之后，若智能电视可调试物理接口不支持对访问用户进行证书认证，测评结果为“不符合要求”，测评结束。否则，进行步骤 3；

在步骤3之后，若用户证书存储在 TEE 或安全芯片中，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.2 存储安全测试项

7.2.2.1 测试项 HW-5

测试项目：硬件平台应具备不可改写用于存储校验密钥、ITVID 等信息的安全存储区域。

测试步骤：

步骤 1：检查厂商提交的文档，查看智能电视采用的芯片；

步骤 2：根据智能电视采用的芯片，核查该芯片是否具备安全存储区。

预期结果：

在步骤 2 之后，若智能电视采用的芯片支持安全存储区，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.2.2 测试项 HW-6

测试项目：应支持对存储在芯片内的固件重要分区进行签名以及签名验证。

测试步骤：

步骤 1：检查厂商提交的文档，查看芯片安全设计；

步骤 2：模拟攻击者，对存储在芯片内的固件的重要分析，如 boot 分区，进行逆向分析，查看关键的代码和数据是否有完整性校验。

预期结果：

在步骤 2 之后，若智能电视芯片支持对固件关键分区的完整性校验，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.2.3 测试项 HW-7

测试项目：应支持对存储在芯片内的固件进行签名以及签名验证。

测试步骤：

步骤 1：检查厂商提交的文档，查看芯片安全设计；

步骤 2：模拟攻击者，对存储芯片内固件进行逆向分析，查看关键的代码和数据是否有完整性校验。

预期结果：

在步骤 2 之后，若智能电视存储芯片支持对固件的完整性校验，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.2.4 测试项 HW-8

测试项目：芯片支持对安全要求不同的应用区提供不同等级的安全管理机制。

测试步骤：

步骤 1：检查厂商提交的文档，查看存储芯片型号；

步骤 2：根据智能电视采用的芯片，核查该芯片支持对不同的应用区提供不同等级的安全管理机制。

预期结果：

在步骤 2 之后，若智能电视存储芯片芯片支持对不同的应用区提供不同等级的安全管理机制，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.2.5 测试项 HW-9

测试项目：存储在芯片内的用户数据以密文形式存在。

测试步骤：

步骤 1：检查厂商提交的文档，查看存储芯片型号；

步骤 2：查看存储在芯片内的用户数据，是否以密文形式存储。

预期结果：

在步骤 2 之后，若用户数据以密文形式存储，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.2.3 硬件实现密码算法安全测试项

7.2.3.1 测试项 HW-11

测试项目：智能电视使用安全芯片实现密码算法。

测试步骤：

步骤 1：检查厂商提交的文档，查看智能电视所采用的芯片型号；

步骤 2：检查厂商提交的文档，查看密码算法的实现形式，或验证密码算法是否在安全芯片中运行。

预期结果：

在步骤 1 之后，若智能电视不支持安全芯片，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若智能电视使用安全芯片实现密码算法，或密码算法在安全芯片中运行，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

四级、五级

7.2.4 外部存储设备安全测试项

7.2.4.1 测试项 HW-12

测试项目：智能电视插入外部存储设备时，应给与用户相应的提示。

测试步骤：

步骤 1：开启智能电视，使其处于正常运行状态；

步骤 2：将外部存储设备或输入输出设备插入正在运行的智能电视。

预期结果：

在步骤 2 之后，若智能电视给与用户相应的提示，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3 操作系统安全能力测试项

7.3.1 安全启动测试项

7.3.1.1 测试项 OS-1

测试项目：智能电视应对启动过程中每个步骤加载的组件验证签名的正确性，包括但不限于引导加载程序、内核、内核扩展项，并验证签名的正确性，确保系统分区不被恶意程序修改。

测试步骤：

步骤 1：检查厂商提交的文档，查看智能电视是否具有安全启动机制；

步骤 2：在非授权的情况下修改启动分区；

步骤 3：重新启动操作系统，检查修改后的启动代码是否可以通过完整性验证。

预期结果：

在步骤 1 之后，若智能电视不具备安全启动机制，测评结果为“不符合要求”，测评结束；否则进行步骤 2 和步骤 3；

在步骤 3 之后，若修改后的启动代码无法通过完整性验证，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3.1.2 测试项 OS-2

测试项目：开机广告须提供 “一键关闭”功能。

测试步骤：

步骤 1：在智能电视正常联网状态下，开启智能电视，查看是否具有开机广告；

步骤 2：若具有开机广告，查看是否具备“一键关闭”功能

在步骤 1 之后，若智能电视没有开机广告，测评结果为“未见异常”，测评结束；否则进行步骤 2；

在步骤 2 之后，若具备“一键关闭”功能，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3.2 固件安全测试项

7.3.2.1 测试项 OS-3

测试项目：智能电视编译固件时，应去除二进制固件中的符号表信息，增加固件调试及破解的难度。

测试步骤：

步骤 1：开启智能电视，使其处于正常运行状态；

步骤 2：通过网络抓包的方式抓取设备的固件升级包或者直接利用硬件编程器从设备中读取固件；

步骤 3：对抓取或读取的固件进行逆向分析，查看是否去除了固件符号表信息。

预期结果:

在步骤 3 之后，若固件去除了固件符号表信息，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级及以上

7.3.3 系统配置安全测试项

7.3.3.1 测试项 OS-4

测试项目：默认关闭操作系统调试接口和远程登录端口（如 SSH 端口和 Tenlent 端口）。

测试步骤：

步骤 1：检查厂商提交的文档，查看其是否默认关闭了操作系统调试接口和远程登录接口；

步骤 2：模拟攻击者，尝试通过系统服务和远程登录端口（SSH 端口和 Tenlent 端口）开启调试接口或超级用户权限。

预期结果：

在步骤 1 之后，若智能电视未关闭操作系统调试接口和远程登录接口，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若模拟的攻击者无法开启调试接口或超级用户权限，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3.3.2 测试项 OS-5

测试项目：核心系统守护进程和业务应用应隔离到不同的安全域，并为每个域定义不同的访问策略。

测试步骤：

步骤 1：检查厂商提交的文档，查看智能电视是否配置并开启了自主访问策略，如 SELinux；

步骤 2：根据智能电视采用的访问控制策略机制，执行相应的命令，验证访问策略是否开启。如执行“adb shell getenforce”命令，若结果为 Enforcing，则表示系统已开启 SELinux，并为每个域定义不同的访问策略。否则显示 Permissive 表示未开启 SELinux。

预期结果：

在步骤 1 之后，若智能电视不具备相应的自主访问策略，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若执行命令，根据返回结果判断访问策略开启，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3.4 系统与固件更新安全测试项

7.3.4.1 测试项 OS-6

测试项目：离线方式进行系统与固件升级时，应对升级文件的完整性进行校验，包括验证升级包的哈希值、大小、版本号和签名。

测试步骤：

步骤 1：获取智能电视系统与固件离线升级包，分析升级包是否包含身份信息、版本信息；

步骤 2：逆向分析系统与固件更新包，检查是否对更新包进行了 SHA-256 等完整性校验；

步骤 3：尝试刷入伪造的更新包。

预期结果：

在步骤 1 之后，若升级包不包含身份信息、版本信息，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若没有对升级包进行 SHA-256 等完整性校验，测评结果为“不符合要求”，测评结束；否则进行步骤 3；

在步骤 3 之后，若伪造的升级包无法成功刷入智能电视，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3.4.2 测试项 OS-7

测试项目：在线方式进行系统与固件升级时，应对升级文件的来源和完整性进行校验，包括验证升级包的哈希值、大小、版本号和签名。

测试步骤：

步骤 1：在智能电视进行系统与固件升级的过程中进行网络抓包，分析升级包是否包含身份信息、版本信息；

步骤 2：逆向分析系统与固件升级包，检查是否对升级包进行了 SHA-256 等完整性校验；

步骤 3：通过 DNS 劫持或 HTTP 劫持替换伪造的升级包。

预期结果：

在步骤 1 之后，若升级包不包含身份信息、版本信息，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若没有对升级包进行 SHA-256 等完整性校验，测评结果为“不符合要求”，测评结束；否则进行步骤 3；

在步骤 3 之后，伪造的升级包无法成功刷入智能电视，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3.4.3 测试项 OS-8

测试项目：进行系统与固件更新，当发生因更新包缺陷而导致更新失败时，不应出现系统不可用的情况。

测试步骤：

步骤 1：检查厂商提交的文档，查看被测智能电视是否提供了系统与固件更新失败时的处理机制；

步骤 2：模拟终端进行因更新包缺陷而导致更新失败，查看智能电视是否进入到系统不可用的状态；

预期结果：

在步骤 1 之后，若智能电视未提供更新失败时的处理机制，测评结果未“不符合要求”，测评结束，否则进行步骤 2；

在步骤 2 之后，若智能电视系统可用，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测试等级：

一级及以上

7.3.4.4 测试项 OS-9

测试项目：以在线方式进行系统与固件升级时，应对升级包文件进行加密。

测试步骤：

步骤 1：在智能电视进行系统与固件更新的过程中进行网络抓包；

步骤 2：逆向分析系统与固件更新包代码，查看是否采用了 HTTPS 等安全传输协议；

预期结果：

在步骤2之后，若更新过程中，采用了HTTPS等安全传输协议，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3.4.5 测试项 OS-10

测试项目：紧急情况下可在线强制升级，若若需强制升级，应提示并告知用户原因。

测试步骤：

步骤 1：开启智能电视，使其处于正常运行状态；

步骤 2：模拟紧急状态模式，在未经用户许可的情况下，刷入系统升级包。

预期结果：

在步骤 2 之后，若可以成功刷入系统升级包，且智能电视告知用户原因，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.3.5 漏洞修复安全测试项

7.3.5.1 测试项 OS-11

测试项目：系统应保证不包含有 CNVD 与 CNNVD 6 个月前公布的高危漏洞。

测试步骤：

步骤 1：使用已知漏洞自动检测工具，对智能电视进行漏洞扫描；

步骤 2：结合 CNVD 和 CNNVD 漏洞库，判断是否存在 6 个月前公布的高危漏洞。

预期结果：

在步骤2之后，若未发现6个月前公布的高危漏洞，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级及以上

7.3.5.2 测试项 OS-12

测试项目：系统应保证不包含有 CNVD 与 CNNVD 6 个月前公布的中危及以上漏洞。

测试步骤：

步骤 1：使用已知漏洞自动检测工具，对智能电视进行漏洞扫描；

步骤 2：结合 CNVD 和 CNNVD 漏洞库，判断是否存在 6 个月前公布的中危及以上漏洞。

预期结果：

在步骤2之后，若未发现6个月前公布的中危及以上漏洞，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级及以上

7.3.5.3 测试项 OS-13

测试项目：应支持漏洞修复及安全防御机制。

测试步骤：

步骤 1：检查厂商提交的文档，查看是否采用了漏洞修复机制或安全防御机制；

步骤 2：模拟终端紧急缺陷或漏洞，尝试通过修复机制，进行补丁下发修复系统缺陷或漏洞，或查看是否具备安全防御机制。

预期结果：

在步骤 1 之后，若智能电视未采用漏洞修复机制，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若可成功下发补丁，进行系统缺陷或漏洞修复，或具备安全防御机制，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级及以上

7.3.6 端口安全测试项

7.3.6.1 测试项 OS-14

测试项目：按需进行服务端口的打开，或开放系统端口时进行访问控制。

测试步骤：

步骤 1：检查厂商提交的文档，查看是否支持服务端口按需打开或访问控制机制；

步骤 2：使用接口扫描工具对智能电视进行扫描，检查所有开启的接口是否存在可疑行为，是否可以访问可疑接口。

预期结果：

在步骤 1 之后，若智能电视未开启防火墙或采用端口访问控制机制，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若智能电视开启的接口未见可疑行为且可疑接口不可访问，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

四级、五级

7.3.7 权限管理安全测试项

7.3.7.1 测试项 OS-15

测试项目：应默认禁止系统进程或应用获取系统的超级用户权限。

测试步骤：

步骤 1：检查厂商提交的文档，查看操作系统权限管理文档；

步骤 2：检查操作系统是否禁止系统进程或应用获取系统的超级用户权限。

预期结果：

在步骤 2 之后，若智能电视默认禁止系统进程或应用获取系统的超级用户权限，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级及以上

7.3.7.2 测试项 OS-16

测试项目：应为系统进程进行分组，并对不同的组配置相应的文件访问权限。

测试步骤：

步骤 1：检查厂商提交的文档，查看智能电视是否提供进程分组安全机制；

步骤 2：检查智能电视系统是否开启了进程分组，并为每个组配置了相应的文件访问权限。

预期结果：

在步骤 1 之后，若智能电视未提供进程分组安全机制，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若开启了进程分组，并进行了相应的权限配置，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级及以上

7.4 预置应用软件安全能力测试项

7.4.1 遥控端认证测试项

7.4.1.1 测试项 AP-1

测试项目：智能电视使用射频或蓝牙遥控器时，射频或蓝牙遥控器应支持与智能电视之间的双向认证配对。

测试步骤：

步骤 1：检查厂商提交的文档，查看是否支持射频或蓝牙遥控器与智能电视之间的双向认证配对；

步骤 2：开启智能电视，使其处于正常运行状态；

步骤 3：使用未与智能电视配对的射频或蓝牙遥控器向智能电视发出控制信号。

预期结果：

在步骤 1 之后，若智能电视不支持射频或蓝牙遥控器与智能电视之间的双向认证配对，测评结果为“不符合要求”，测评结束；否则进行步骤 2 和步骤 3；

在步骤 3 之后，若智能电视未能成功执行控制信号，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级及以上

7.4.1.2 测试项 AP-2

测试项目：智能电视应对遥控端 APP 实施身份认证，以防止非授权的操作。或支持在使用遥控端 APP 执行敏操作时，通过验证码等手段进行二次校验，同时验证码应限制一定时间内的尝试频次，以防止暴力破解。

测试步骤：

步骤 1：检查厂商提交的文档，查看是支持对控制端 APP 的身份认证；

步骤 2：开启智能电视，使其处于正常运行状态；

步骤 3：使用未经认证的遥控端 APP 向智能电视发送控制信息；

步骤 4：尝试使用遥控端 APP 向智能电视发送操作信息。

预期结果：

在步骤1之后，若智能电视不支持对控制端APP的身份认证，测评结果为“不符合要求”，测评结束；否则进行步骤 2，步骤 3 和步骤 4；

在步骤 3 之后，若智能电视未能成功执行控制信号，测评结果为“未见异常”，测评结束；否则进行步骤 4；

在步骤4之后，若控制端APP提醒用户进行二次认证，如采用验证码验证，且限制一定时间内的尝试频次，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级及以上

7.4.2 软件安装安全测试项

7.4.2.1 测试项 AP-3

测试项目：预置应用软件不应存在 CNVD 和 CNNVD 6 个月前公布的高危漏洞。

测试步骤：

步骤 1：查阅 CNVD 和 CNNVD 六个月前公布的高危漏洞；

步骤 2：使用自动化扫描工具扫描并验证预置软件是否存在 CNVD 和 CNNVD 六个月前公布的高危漏洞。

预期结果：

在步骤 2 之后，若未存在高危漏洞，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

二级及以上

7.4.2.2 测试项 AP-4

测试项目：智能电视应对获取应用过程中与服务器的相关通信进行证书验证。

测试步骤：

步骤 1：检查厂商提交的文档，查看应用安装过程是否具备通信证书验证环节；

步骤 2：预置应用使用不正确的证书与智能电视进行通信，判断是否可以完成应用安装流程。

预期结果：

在步骤 1 之后，若智能电视不具备通信证书验证环节，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未能成功完成应用安装流程，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

二级及以上

7.4.3 软件更新安全测试项

7.4.3.1 测试项 AP-5

测试项目：进行更新时，应对更新包进行版本号、哈希值、签名和文件大小进行校验。

测试步骤：

步骤 1：检查厂商提交的文档，查看应用安装更新过程中，是否进行更新包校验；

步骤 2：在预置软件更新过程中进行网络抓包，分析更新包是否有身份信息、版本信息，是否对更新包进行了 SHA-256 等完整性校验；

步骤 3：劫持替换预置应用软件的更新包，查看修改后的更新包是否可以安装。

预期结果：

在步骤 1 之后，若智能电视不具备软件更新包校验能力，测评结果为“不符合要求”，测评结束；否则进行步骤 2 和步骤 3；

在步骤 2 之后，若软件更新包未包含有身份信息、版本信息，且未进行完整性校验，测评结果为“不符合要求”，测评结束；否则进行步骤 3；

在步骤 3 之后，若未能成功完成应用更新流程，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

二级及以上

7.4.3.2 测试项 AP-6

测试项目：进行预置应用软件更新时，应对软件更新包进行加密。

测试步骤：

步骤 1：检查厂商提交的文档，查看预置应用安装过程对更新包进行加密；

步骤 2：在预置软件更新过程中进行网络抓包；

步骤 3：对预置应用软件更新包进行解析，检查是否可以获取正常的文件格式。

预期结果：

在步骤 1 之后，若智能电视不提供更新包加密能力，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未能获取正常的文件格式，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

二级及以上

7.4.4 身份凭证安全测试项

7.4.4.1 测试项 AP-7

测试项目：应验证登录应用的用户身份及凭据的有效性，如采用二维码扫描或用户名密码登录方式。

测试步骤：

步骤 1：检查厂商提交的文档，查看是否具备验证登录应用的用户身份能力；

步骤 2：模拟未验证身份的用户进行预置应用登录操作，并执行视频播放等操作，检查用户在执行预置应用操作之前是否必须验证用户身份凭证。

预期结果：

在步骤 1 之后，若预置应用不具备用户身份验证能力，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若预置应用提示用户进行身份凭证验证，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级、四级、五级

7.4.4.2 测试项 AP-8

测试项目：应验证登录应用的用户身份及凭据的有效性，如采用二维码扫描或用户名密码登录方式，并对登入用户设置一定的有效期，超过有效期需用户重新登录。

测试步骤：

步骤 1：检查厂商提交的文档，查看是否具备验证登录应用的用户身份能力；

步骤 2：模拟未验证身份的用户进行预置应用登录操作，并执行视频播放等操作，检查用户在执行预置应用操作之前是否必须验证用户身份凭证；

步骤 3：检查厂商提交的用户登录代码，检查是否对登录后的用户令牌设置了一定的有效期。

预期结果：

在步骤 1 之后，若预置应用不具备用户身份验证能力，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若预置应用不具备用户身份验证能力，测评结果为“不符合要求”，测评结束；否则进行步骤 3；

在步骤 3 之后，若厂商代码中包含有用户令牌有效期，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级、四级、五级

7.4.4.3 测试项 AP-9

测试项目：应验证登录应用的用户身份及凭据的有效性，宜支持生物特征认证登录形式。

测试步骤：

步骤 1：检查厂商提交的文档，查看是否具备根据生物特征验证登录应用的用户身份能力；

步骤 2：模拟未验证身份的用户进行预置应用登录操作，并执行视频播放等操作，检查预置应用是否支持使用生物特征验证用户身份；

预期结果：

在步骤 1 之后，若预置应用不具备生物特征验证能力，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若预置应用支持生物特征验证能力，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级、四级、五级

7.5 第三方应用软件安全能力测试项

7.5.1 软件安装安全测试项

7.5.1.1 测试项 TAP-1

测试项目：应不允许安装未签名应用或者不受信任的代码，禁止安装未授权的第三方应用软件。

测试步骤：

步骤 1：检查系统选项中是否默认关闭未知来源安装，不存在静默安装接口；

步骤 2：模拟进行未签名应用以及不受信任代码的安装。

预期结果：

在步骤 1 之后，若智能电视存在静默安装接口，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未成功安装，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.5.1.2 测试项 TAP-2

测试项目：智能电视应对获取应用过程中与服务器的相关通信进行证书验证。

测试步骤：

步骤 1：检查厂商提交的文档，查看第三方应用安装过程是否具备通信证书验证环节；

步骤 2：使用不正确的证书与智能电视进行通信，进行第三方应用安装。

预期结果：

在步骤 1 之后，若不具备通信证书验证环节，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未能成功完成应用安装流程，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.5.1.3 测试项 TAP-3

测试项目：应用安装应经过电视厂商的安全校验。

测试步骤：

步骤 1：检查厂商提交的文档，检查第三方应用安装说明；

步骤 2：进行未经电视厂商安全校验的应用安装。

预期结果：

在步骤 1 之后，若第三方应用安装说明未要求经过电视厂商安全校验，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未能成功进行应用安装，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.6 网络通信安全能力测试项

7.6.1 协议一致性安全测试项

7.6.1.1 测试项 NC-1

测试项目：智能电视在采用 WLAN、蓝牙等无线传输协议时，应准照 T/TAF 071.1-2020 中 5.6 章节实现设备授权认证、加密传输等安全功能。

测试步骤：

步骤 1：检查厂商提交的文档，查看是否准照 T/TAF 071.1-2020 中 5.6 章节实现设备授权认证、加密传输等安全功能。

预期结果：

在步骤 1 之后，若经过相应的认证，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.6.2 数据传输安全测试项

7.6.2.1 测试项 NC-2

测试项目：智能电视应支持对称算法对用户数据进行加密传输保护，对称密钥应进行安全存储。

测试步骤：

步骤 1：检查厂商提交的文档，查看在数据传输过程中是否采用了加密保护；

步骤 2：逆向分析用户数据的加密方式，是否使用了对称算法进行加密传输；

步骤 3：检查对称密钥的存储方式，查看其是否存储安全。

预期结果：

在步骤 1 之后，若未采用加密保护，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未采用对称算法进行加密保护，测评结果为“不符合要求”，测评结束；否则进行步骤 3；

在步骤 3 之后，若密钥安全存储，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.6.2.2 测试项 NC-3

测试项目：智能电视应支持 TLS 协议对用户数据进行安全传输，应使用 TLS V1.2 作为主要协议，继续支持 TLS V1.1 和 TLS V1.0，禁止使用 SSL V2 及 SSL V3。

测试步骤：

步骤 1：检查厂商提交的文档，查看在和厂商服务器间的用户数据传输过程中是否采用了加密保护；

步骤 2：逆向分析用户数据的加密方式，查看其使用的安全传输协议。

预期结果：

在步骤 1 之后，若未采用加密保护，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若采用的传输协议符合为 TLS V1.2，支持 TLS V1.1 和 TLS V1.0，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.6.2.3 测试项 NC-4

测试项目：智能电视采用的 TLS 协议应使用 128 位或更强的加密、认证套件。

测试步骤：

步骤 1：检查厂商提交的文档，查看在数据传输过程中是否采用了加密保护；

步骤 2：查看智能电视安全传输协议代码，检查其采用的加密、认证套件。

预期结果：

在步骤 1 之后，若未采用加密保护，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若采用的传输协议密码套件为 128 位或更强，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

一级及以上

7.6.2.4 测试项 NC-5

测试项目：安全传输协议应具备抵抗因编程语言固有缺陷造成的安全漏洞，如使用可抵抗内存安全漏洞的传输层协议。

测试步骤：

步骤 1：检查厂商提交的文档，查看在数据传输过程中是否采用了加密保护；

步骤 2：对智能电视安全传输协议进行如内存安全攻击。

预期结果：

在步骤 1 之后，若未采用加密保护，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若安全传输协议可以抵抗内存攻击，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

四级、五级

7.6.3 DNS 劫持安全测试项

7.6.3.1 测试项 NC-6

测试项目：智能电视应具备检测 DNS 劫持的能力。

测试步骤：

步骤 1：检查厂商提交的文档，查看其是否具备 DNS 劫持检测机制；

步骤 2：模拟攻击者对智能电视进行 DNS 劫持攻击，查看智能电视是否有相应的提示。

预期结果：

在步骤 1 之后，若未具备 DNS 劫持检测机制，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若智能电视有相应的提示，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

二级及以上

7.6.3.2 测试项 NC-7

测试项目：智能电视应具备修复 DNS 劫持的能力。

测试步骤：

步骤 1：检查厂商提交的文档，查看其是否具备防止 DNS 劫持的机制；

步骤 2：模拟攻击者对智能电视进行 DNS 劫持攻击，查看是否可以成功劫持。

预期结果：

在步骤 1 之后，若未具备防止 DNS 劫持机制，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未能进行成功劫持，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

三级、四级、五级

7.7 人工智能服务安全能力测试项

7.7.1 上传数据安全测试项

7.7.1.1 测试项 AI-1

测试项目：应防止攻击者将用户使用人工智能服务时的交互数据上传指向到自己的服务器，如设置上传服务器地址是不可配置的。

测试步骤：

步骤 1：检查厂商提交的文档，查看智能电视是否采用了安全机制防止攻击者将数据上传到自己的服务器；

步骤 2：模拟攻击者，尝试修改数据上传服务器地址，查看是否可以成功接收到用户数据。

预期结果：

在步骤 1 之后，若未具备该类安全机制，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未能进行接收用户数据，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

四级、五级

7.7.2 对抗性攻击防护安全测试

7.7.2.1 测试项 AI-2

测试项目：智能电视机器学习算法应具备抵抗对抗性攻击的能力，如抵抗隐藏语音命令攻击。

测试步骤：

步骤 1：模拟攻击者，尝试进行隐藏语音命令攻击操作，如使用大于 20KHZ 的超声波，查看是否可以控制智能电视执行相应的操作。

预期结果：

在步骤 1 之后，若未能成功操作智能电视，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

五级

7.7.3 机器学习模型保护安全测试

7.7.3.1 测试项 AI-3

测试项目：应对机器学习模型进行安全保护，以保护机器学习模型不被非法窃取。

测试步骤：

步骤 1：检查厂商提交的文档，查看智能电视是否采用了安全机制对机器学习模型进行了保护；

步骤 2：尝试利用公共访问接口的方式，对智能电视机器学习模型进行构造。

预期结果：

在步骤 1 之后，若未进行安全保护，测评结果为“不符合要求”，测评结束；否则进行步骤 2；

在步骤 2 之后，若未能进行成功构造模型算法，测评结果为“未见异常”，否则为“不符合要求”，测评结束。

测评等级：

五级

附　录　A
（资料性）
安全能力等级建议

智能电视提供的应用功能包括视频直播、投屏功能、USB 扩展、投屏功能、家庭相册、语音操作、休闲游戏、视频聊天、购物支付、远程控制、人脸识别等。智能电视分场景的安全级别建议见表 A.1。

表 A.1 智能电视分场景安全级别建议

应用场景	建议级别
视频直播、休闲游戏	一级及以上
USB 扩展、投屏功能	二级及以上
家庭相册、视频聊天	三级及以上
购物支付、远程控制	四级及以上
人脸识别、语音交互	五级

电信终端产业协会团体标准

智能电视安全能力技术要求和测试方法

T/TAF 086-2021

*

电信终端产业协会印发
地址：北京市西城区新街口外大街 28 号
电话：010-82052809
电子版发行网址：www.taf.org.cn