CAICT 中国信通院　TAF 电信终端产业协会

OTT 终端数据安全和个人信息保护研究报告

（2022 年）

中国信息通信研究院泰尔终端实验室
电信终端产业协会移动安全工作委员会

2022 年 6 月

版权声明

编制说明

本报告编写参与单位：中国信息通信研究院泰尔终端实验室、电信终端产业协会移动安全工作委员会、秒针信息技术有限公司、海信视像科技股份有限公司、北京风行在线技术有线公司、四川长虹电器股份有限公司、深圳市易平方网络科技有限公司、蚂蚁科技集团股份有限公司、奇安盘古（上海）信息技术有限公司、北京启明星辰信息安全技术有限公司、北京娜迦信息科技发展有限公司、杭州安恒信息技术股份有限公司。

前　言

近年来 OTT 行业快速发展，OTT 本质上是互联网公司以互联网为媒介、以互联网电视为终端向用户提供各类服务。

2015 年以来，互联网电视用户规模加速扩大，出货率持续上升。据国家广播电视总局《2021 年全国广播电视行业统计公报》显示，截至 2021 年底，互联网电视用户数 10.83 亿户，互联网视频年度付费用户达到 7.1 亿，互联网音频年度付费用户 1.5 亿，短视频上传用户超过 7 亿，OTT 集成服务业务收入 78.02 亿元，同比增长 9.73%。据有关机构预测，到 2023 年中国 OTT 大屏相关的业务与带动的产业规模将达到 620 亿左右。

OTT 终端产业迅猛发展的同时，也带来了诸多安全问题，包括互联网电视系统版本落后、大量漏洞修补不及时、控制模块容易越权操控、语音控制内容容易被篡改、预置应用过度索取权限、用户数据非法采集共享、数据安全问题等。这些安全问题可能被不法分子以远程控制电视、远程安装恶意软件、远程监控家庭等方式利用，最终造成用户隐私泄露、财产损失。

2021 年 9 月 1 日和 11 月 1 日，《中华人民共和国数据安全法》和《中华人民共和国个人信息保护法》分别正式实施，为促进互联网电视行业及其生态系统的健康发展，厘清互联网电视行业目前在数据安全和个人信息保护方面面临的安全问题，中国信息通信研究院（以下简称：中国信通院）泰尔终端实验室、电信终端产业协会移动安全工作委员会联合安全团队和互联网电视厂商对多款主流品

牌型号的互联网电视产品开展安全评测，评测内容包括：硬件安全、操作系统和系统组件安全、预置应用安全、第三方软件安装安全、个人隐私和数据安全等 6 个方面 66 项内容，测试表明：75%的被测电视操作系统存在已知安全漏洞，60%的预装 APP 存在违规采集 MAC 地址等用户信息的问题，80%的电视系统的内置 SDK、预装应用存在未获得用户同意向第三方共享用户敏感数据的问题。

本报告重点梳理了 OTT 行业现状、互联网电视安全问题现状、安全管理现状，并分析了主流品牌型号的互联网电视产品测试情况，从加强行业监管、完善政策标准、强化技术研究、推进检测认证等方面提出发展建议。

党中央高度重视发展数字经济，OTT 行业是数字经济的实践者和先行者，在不断创造价值的同时，其安全保护、合规应用等问题需要产业生态共同努力。报告中如有不足之处，请各方专家读者不吝指正。

目 录

图 目 录

表 目 录

一、OTT 行业现状

OTT 是“Over The Top”的缩写，是指越过运营商，通过互联网向用户提供各种应用服务。狭义的 OTT 是指通过公共互联网面向 OTT 终端传输的由国有广播电视机构提供视频内容的可控可管服务。

OTT 终端指的是互联网电视、OTT（盒子）+电视机输出设备，国内一般指的就是互联网电视，本报告中 OTT 终端也特指为互联网电视。

（一）OTT 行业发展历程

全球 OTT 电视有 3 种发展模式，第一种是欧洲的兼顾传统广播电视与 OTT 服务的 Hybrid Broadcast/Broadband TV（简称: HBBTV）模式，第二种是完全以互联网架构为基础的美国开放式 OTT 模式，第三种则是中国所形成的强调内容监管的可管可控模式。

1.国外 OTT 行业发展概况

OTT 最早源于 1999 年微软的维纳斯计划，目的是通过机顶盒访问互联网的内容，通过该方式提供更为广泛的互联网服务。但由于当时用户使用习惯和技术限制，互联网没有在机顶盒上大规模开展。

2007 年苹果推出 iTV 一代，2009 年苹果研发了 iTV 二代，并更名为 APPLETV。同时时代华纳和康卡斯特推动“TV Everywhere”项目。

2010、2011 年谷歌相继推出 Google TV 一代和二代，Google TV 的推出将 OTT 推向了高潮，并且有成为主流视频传送技术和替代 IPTV 的趋势。

2012 年苹果发布第二代 Apple TV，奈飞（Netflix）、Roku、hulu、YouTube、亚马逊等也相继推出互联网电视服务及终端产品，全球互联网电视机行业进入快速发展阶段。

2.国内 OTT 行业发展概况

萌芽期：2008 年，中国彩电企业投入互联网电视研发，创维、长虹、海尔等厂商尝试搭建互联网电视的虚拟运营平台，为新款电视机探索更多亮点。主要形态是“液晶电视+网络接口+迅雷或搜狐”。

准入期：2009-2010 年，2009 年，中国实现互联网电视的量产，互联网玩家进入。2010 年，国家广电总局陆续发放了 7 张互联网电视牌照，分别为国广东方 CIBN、银河互联 GITV、百视通 BesTV、华数 TV、南方传媒、芒果 TV、未来电视（ICNTV），规范行业发展。

起步期：2010-2015 年，互联网电视内容服务牌照制度和互联网集成服务牌照制度建立后，互联网电视厂家纷纷与牌照方合作，互联网企业也强势进入，基于安卓平台的“互联网电视+牌照方内容+第三方内容”的互联网电视运作模式建立。有线电视、IPTV 和互联网电视三足鼎立局面形成。

发展期：2015-2019 年，行业进入爆发增长期。互联网电视用户规模加速扩大、出货率持续上升，互联网电视开启了多极发展、精细化运营的阶段。特别是 2015 年中国互联网广告份额首次超过电视广告，在整个中国互联网进程加速的大背景下，互联网加速向传统电视行业渗透，互联网电视广告爆发式增长，亦开启了电视程序化购买时代。

成熟期： 2019 年中国正式进入 5G 商用时代，场景互联网在 5G 和 IoT 技术赋能下加速落地，互联网电视逐渐向能够满足用户在家庭范围内不同需求的智慧屏生态时代过渡。

（二）互联网电视行业发展现状和趋势

1.互联网电视行业发展现状

目前在中国家庭收视市场上，传统的有线电视、IPTV 和互联网电视三种已形成三足鼎力之势，其中，互联网电视是目前发展最快的产业形态。

（1）互联网电视销量稳步增长

根据 2021 年 9 月份发布的《“逆风远略”-2021 智慧屏行业发展白皮书》显示，相较于 2020 年疫情时代影响下下半年销量的激增，2021 年互联网电视销量回归平稳，传统和互联网硬件制造商争夺互联网电视市场，传统五大厂商激活量较上半年增长 872 万台，互联网电视增长 276 万台，增幅减缓，销量稳步增长。

（2）传统和网生电视内容并驾齐驱

随着行业发展，传统的渠道通过自建渠道 APP、与互联网主流平台进行内容的分销、独播、联合制作等方式都在不同程度布局互联网电视渠道。随着用户收视习惯的变迁，互联网电视上以点播服务为主的收视模式也越来越受到用户的欢迎。在点播内容的提供方面，传统广播电视与互联网视频服务商在互联网电视上争相发力，目前以优爱腾芒的互联网电视视频应用领跑内容播出平台，占据领先优势。

（3）媒体价值继续快速增长

互联网电视收入模式以互联网广告为主、付费会员收入、付费影视、游戏、教育等为辅。

据韩联社报道，2021 年，超过 34%的韩国人是 OTT 媒体或视频流媒体服务的付费用户。同时，使用 OTT 服务的韩国付费用户占比达到 38.4%，较 2020 年增长了 20.4%；2021 年，韩国的 OTT 服务使用率上升至 69.5%。不止韩国，2021 年欧洲付费视频收入达到 142 亿美元，远远高于 2015 年的 18 亿美元。国外数据研究机构卡根预计欧洲 2022 年 OTT 服务收入将增长 8%，并拥有千万级的净增用户。

国内市场，据国家广播电视总局统计数据，2021 年，我国互联网电视用户数达 10.83 亿。数据显示，OTT 广告营收达到 150 亿，较去年涨幅 45%，具体收入见图 1。

来源：国家广播电视总局

图 1 2017-2021 年中国 OTT 广告运营总收入

2.互联网电视行业发展趋势

（1）硬件软件同步发力，行业发展更加全面

在中国，5G 时代将带动超高清视频产业的快速发展，硬件方面 AI、AIoT 等将成为行业发展核心，从 AI 控制接入到旋转屏，智慧屏不断向着 AIOT 方向建设发展，预示着 OTT 生态将向智慧屏生态全面转型。

内容方面随着音乐、教育、购物、游戏等服务类 APP 的不断发展，互联网电视承载的场景从长视频扩展到中视频、短视频，也将进一步延伸到健康、家居、健身、游戏、衣食住行等生活的方方面面，智慧屏生活场景服务将不断被完善。

（2）广告持续高速增长，发展空间巨大

在中国，随着互联网电视的逐步普及和用户的长期使用依赖，互联网电视广告运营收入有望持续高速增长。奥维互娱预测，到 2023 年互联网电视广告总收入可破 450 亿。

从互联网电视广告营销趋势来看，未来几年将逐步走向程序化、大小屏打通、精准化投放将成主流，“内容流量”“设备流量”“按需求量”的广告交易成为主要模式；内容方+硬件方+系统方+技术方+代理构成多方交易生态市场。广告形式也会结合互联网电视显示技术的升级以及 5G 带来的互动体验的升级，呈现出越来越多创新的形式。

（3）媒体服务竞争激烈，内容生态更加丰富

近年来，国外的主流电视网和工作室不断推出自己的直接面向消费者的流媒体服务，竞争者们争相提供内容库，为传媒娱乐公司提供了“重新组合”其内容库的机会。国内媒体通过提供优质的视频资源

的内容，结合如订阅、广告赞助、付费观看、电子销售等商业模式进行营销。

虽然长视频平台内容和电视直播内容依然占据主流，但随着越来越多的内容与娱乐形式入驻互联网电视，点播、短视频等业务服务也在快速发展。电视直播将逐步与其他服务进行打通，直播将与点播、轮播、电商、短视频等更多业态融合，实现直播价值的最大化。

二、互联网电视安全问题现状

随着互联网电视的日益普及，智能终端呈现出“强交互”与“强AI”特征，越来越多的软硬件及技术创新得以应用。与此同时，安全问题爆发的频次也有所升高，系统风险、DNS 劫持、WIFI 风险、恶意应用等，已经成为阻碍互联网电视发展的安全雷区。

(一) 数据安全和个人信息保护问题

1.互联网电视通过记录屏幕快照，采集用户数据

2019 年年底，华盛顿邮报报道，根据最近的实验，记者跟踪的最大的电视制造商在时时记录用户的观看记录。互联网电视记录屏幕快照并将其发送到服务器，服务器使用自动内容识别（ACR）系统得到各种内容的屏幕快照的每秒日志，电视制造商再将日志信息出售给其他公司或者他们对用户进行分析后出售目标广告。虽然收集的数据不是个人信息而是整个家庭的信息。但是，大数据分析能够分离信息并最终定位到用户的个人信息。

2.终端应用引发的数据安全和个人信息泄露问题

与移动端 APP 存在的安全风险类似，互联网电视上，APP 强制授权、过度索权、超范围收集个人信息的现象大量存在，用户数据存储、收集、共享环节等安全问题更甚于移动端。2021 年 4 月，有用户发帖曝光称，暗藏某第三方数据公司“数据服务”应用的互联网电视，会自动收集用户家中所有联网的智能设备信息并上传，甚至连邻居的 WIFI 信息也会收集。由于未得到用户授权，并且用户隐私政策提示不够清晰，引起了大量用户对隐私安全的担忧。

3.SDK 违规采集、处理数据现象严重

APP 使用第三方 SDK 已成为普遍现象。根据爱加密发布的 2020 年 Q1《全国移动 App 安全态势研究报告》，截至 2020 年 3 月底，爱加密大数据中心已收录 Android 应用超过 315 万款，iOS 应用超过 300 万款，其中 29.46%的应用嵌入了 SDK。

《软件开发包（SDK）安全与合规白皮书（2020）》中援引的一组数据显示：测评的 1000 多款主流 APP 中，各类别 APP 使用第三方 SDK 平均在 10 个以上，最高可达平均 30.6 个/类。

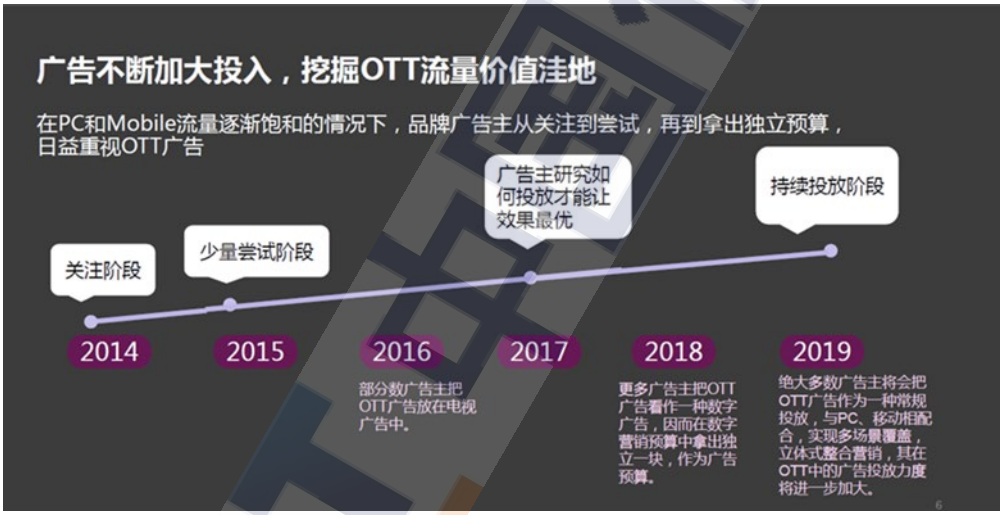
在带来高效、便捷的同时，SDK 也存在隐蔽性较强、自身安全性良莠不齐、与 APP 提供者合作关系复杂化等特点，暗含安全风险。一些 SDK 存在代码安全漏洞、恶意行为、违规收集使用个人信息、强制申请非必要权限等问题。加之部分 APP 未明显告知用户第三方 SDK 个人信息收集规则或未严格监管其使用的第三方 SDK，导致数据泄露等安全事件时有发生。

2020 年 4 月，Zoom APP 被披露，其内嵌的 Facebook SDK 在用

户不知情的情况下向 Facebook 传输用户的手机型号、城市、广告唯一标识符、IP 地址等用户个人信息，但 Zoom APP 在隐私政策内容中并未明确向用户描述这一操作，直接导致其股价大跌。

（二）流量欺诈问题

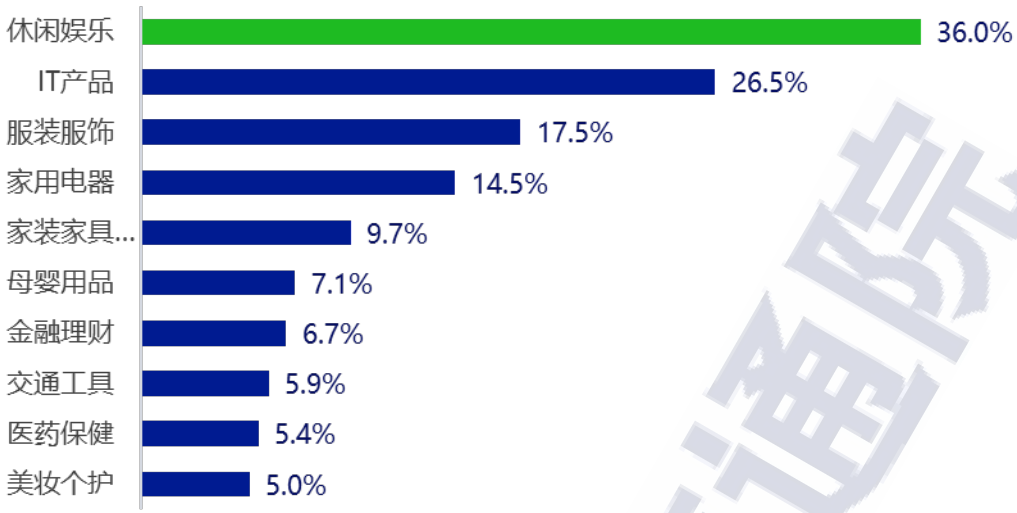
现阶段，OTT 流量持续扩张，并受到更多营销人员的重视，图 2 展示了市场不断挖掘 OTT 流量价值的趋势图。市场对 OTT 流量的青睐亦引起虚假作弊流量肆虐，榨取大量广告市场的预算，并威胁家庭用户的信息安全。



来源：秒针信息技术有限公司

图 2 市场挖掘 OTT 流量价值趋势

据秒针信息技术有限公司的监测，2021 年全年互联网异常广告流量占比为 10.1%。从广告位来看，常规 Banner 广告异常曝光占比最高，达到 20.5%；互联网电视异常流量占比以休闲娱乐业最为突出，占比近 3 成；其次为服装服饰，占比达到 26.8%。具体行业占比见图 3。



来源：秒针信息技术有限公司

图 3 2021 年互联网电视广告异常曝光占比最高的前十行业

（三）内容安全问题

操作系统的开放性吸引更多攻击者来破坏数字内容的机密性和完整性，泛滥的盗版内容也伤害整个互联网电视生态系统。

2020 年据外媒报道，自居家隔离以来，英国正成为一个盗版泛滥的国家，非法电影和电视网站的流量开始不断激增。据悉，3 月份的最后一周，电影盗版网站的访问量比 2 月的最后一周上升了 57%。允许观众非法观看电视节目和连续剧的网站同期增长了 29%。

在国内，视频内容消费呈现需求上扬态势的同时，盗版与软盗版的横行一定程度上也为视频行业的发展带来了消极影响。除了内容盗版侵权，在短视频内容领域，二创、搬运等软盗版行为也在影响着长视频付费市场发展。据某知名视频类互联网公司调查的数据显示，旗下某热播剧在播出期间，监测到盗版侵权条数超 1.2 万条，75%来自短视频。在剧集完整播出期间，盗版总量超 27 万条，约三分之二来自短视频。

(四)投屏安全问题

随着 WIFI 和互联网电视的普及，投屏变得非常便捷，但投屏存在泄漏用户隐私的风险。在手机、电脑采用镜像投屏的时候，会将手机、电脑屏幕同步到大屏幕上，这时如果手机上接收到信息会同步显示在大屏幕上，其余的分享人员亦可以通过大屏幕看到。而且如果投屏被别有用心的人利用，势必会造成比较严重的社会问题。2019 年 1 月 5 日，一男子破解位于江汉路的某知名连锁火锅店的公共 WIFI，在其店内电视上投屏播放不雅视频，一时引起网上热炒。

三、互联网电视安全管理现状

(一)国际上对互联网电视安全的研究与治理

1.行业组织监督行业发展，规范行业行为

2016 年 7 月，欧盟内部磋商，在修改的电子隐私权指令中对 Facebook、微软等企业的 OTT 通信业务做出更严格的管制规定。新规将适用于任何允许用户在线拨打电话或发送信息的 OTT 应用，还可能会取消原本对运营商有关用户位置数据的限制。

2016 年 12 月，欧盟透露网络安全新规定将严格监管谷歌、Facebook 等互联网公司的商业模式(即通过在线追踪用户的浏览足迹，以确定商业广告目标群体)，要求网站和浏览器在基于用户的浏览历史推荐广告前，要征得用户同意。新规定于 2017 年 1 月公布，如果 OTT 企业不遵守新规，可能会面临罚款，数额高达其全球营业额的 4%。

2019 年 11 月 26 日，美国联邦调查局（FBI）波特兰总部发布有

关互联网电视带来的风险警告。相关公告显示电视制造商、应用开发人员和黑客都有可能通过互联网电视获取隐私信息。同时 FBI 警告称黑客会控制互联网电视，在最坏的情况下可以控制摄像机和麦克风以观看和收听。同时，为了避免互联网电视制造商通过回收用户观看内容信息来提供定位广告，FBI 建议互联网电视用户在未使用的电视摄像机上贴黑胶布并及时更新互联网电视的固件，阅读隐私政策以便更好地使用互联网电视。

2.发展互联网电视安全技术

互联网电视安全方面的重点是基于硬件的可信执行环境技术,以及基于其上的内容安全、业务安全、终端管控等可信应用的安全。

基于硬件的可信执行环境技术，包括 ARM TrustZone、Intel SGX、AMD 的 PSP、MIPS Virtualization 等技术体系。近期,为满足对基于可信执行环境的终端设备及可信应用管理的需求，ARM 牵头研究了 OTrP（Open Trust Protocol），具体做法是将安全架构与可信程序管理结合起来,在 REE 建立 TA 服务管理 SDK（TSM），构建基于 PKI 的认证体系，通过 TSM 实现可信应用、用户应用和服务提供商的互信，并管理 TA 的安装、升级和删除。

3.推行企业权威认证检测，提升企业反欺诈能力

TAG（The Trustworthy Accountability Group）于 2014 年由美国广告业组织、互动广告局（IAB）、美国全国广告主协会（ANA）和美国广告代理协会（4A’s）共同创办，旨在打击数字广告供应链中的犯罪活动并提升品牌安全性。

TAG 在 2016 年推出了反欺诈认证计划，TAG 的流量反欺诈标准已经在亚太地区、美国以及欧洲地区主要市场发挥了重要作用，包括对 OTT 终端领域的流量造假打击。根据数据统计，超过 90%已获 TAG 认证的广告主在上述市场发生广告欺诈的概率低于行业平均水平。越来越多的广告主也对合作方提出 TAG 认证要求，2017 年宝洁公司就明确表示，不想再购买欺诈性的广告，要求宝洁的合作伙伴必须获得 TAG 认可。

4.数据安全和个人信息保护专项治理

（1）通过立法保护个人数据和信息安全

欧盟《通用数据保护条例》（GDPR），英国《数据保护法案》（Data Protection Act）、瑞典《瑞典数据法案》（Swedish Data Act）、爱尔兰《2018 数据保护法案》、美国加利福尼亚州颁布《加州消费者隐私保护法案》（CCPA）等，都围绕个人数据的收集、使用、保存、分享、转移等，对数据控制者和处理者、数据主体的权利义务进行全面规定。

（2）高压执法、强力处罚制止违法行为

美、欧等国保护消费者隐私和个人信息最主要的手段就是采取强制执法措施来制止违法行为，并要求企业采取积极整改措施。

美国联邦贸易委员会（FTC）已建立两年一次的独立专家评估制度，并针对一系列移动互联网应用隐私问题开展执法行动，通过高罚款、禁止销售运营等强力处罚手段，震慑移动应用提供者。

2019 年 1 月 21 日，法国国家与信息通信委员会（CNIL）以“未向 Android 用户正确披露其数据如何被收集、并向用户违法推送广告”

对谷歌开出了 GPDR 罚单，金额高达 5000 万欧元（约 5700 万美元）。

2021 年 9 月 3 日，WhatsApp 因违反欧盟数据隐私法，没有告诉用户如何与其母公司 Facebook 共享数据而面临爱尔兰数据保护委员会罚款 2.25 亿欧元（2.66 亿美元）。

（二）国内对互联网电视安全的研究与治理

1.国家监查，整改行业违法行为

2016 年 8 月，国家新闻出版广电总局要求各大牌照机构对互联网电视内容进行整改，整改内容主要包括严格控制盗版以及直播出现的“涉黄涉暴”问题。

2020 年 7 月 8 日，广电总局网络司召集七大互联网电视牌照运营商就互联网电视目前发展中所存在的部分不合规的现象进行了沟通。并就各牌照商强化播控监管职能，完善备案上报沟通机制，确保互联网电视健康有序、合规发展提出了具体的要求。

2020 年年底，国家广播电视总局向互联网电视集成服务平台运营方下发了《关于对互联网电视集成平台开展年度内容安全检查的通知》（网字（2020）284 号）。要求集成牌照方对集成平台推出的 EPG 版本和终端产品、节目源管理、节目内容、集成平台运营机构等进行年度检查。

2021 年 8 月，广电总局网络司针对 OTT 行业出台了多份整改要求。在本轮的行业管理和整改中，总局网络司主要针对互联网电视集成平台、电视机厂家、第三方应用商店下文，分别就内容、新业务、数据管理、播控平台、应用商店等多方面提出了针对性的整改要求。

2.行业自律，建立行业标准规范

2014 年 1 月 15 日，中国电子视像行业协会正式发布《智能电视系列规范》，发布的《智能电视系列规范》共分为 6 个部分，分别是智能电视机总规范、智能电视操作系统技术规范、平台及第三方应用接口技术规范、人机交互技术规范、智能电视应用商店技术规范以及智能电视系统安全技术规范。

2018 年，中国网络视听节目服务协会和互联网电视工作委员会在国家广播电视总局网络视听节目管理司的指导下，推出了《互联网电视应用商店(应用)管理规范》，促使互联网电视应用商店浏览、下载、安装、管理更加规范化。

2018 年 9 月 21 日，在互联网电视行业合作发展恳谈会上，7 大互联网电视集成服务牌照方现场签署《中国互联网电视集成服务机构自律公约》，通过机制的建立，规范行业从业者行为，依法促进和保障互联网电视行业健康发展。

2018 年，七大牌照商组成的互联网电视工作委员会还推出了《互联网电视集成服务平台服务能力与业务规范》和《互联网电视数据通用处理规范》两大规范，对整个互联网电视行业的发展进行了细致的规范，OTT 产业更加合规、合法化。

2019 年 10 月，部分电视终端与数据监测公司签订《OTT 流量安全倡议》书，杜绝 OTT TV 虚假广告刷量，致力于打造一个 OTT TV 的清朗广告环境。

2020 年 3 月，中国电子视像行业协会联合创维、海信、TCL、长

虹、康佳、索尼等国内外主流彩电品牌厂商以及智能电视运营服务平台、学术研究等机构发布《智能电视开机广告服务规范》，对售前提前告知消费者开机广告以及开机广告的播放时长、关闭能力、广告内容的合法性等方面提出了明确要求，规范化管理互联网电视开机广告。

2021 年 6 月，在国家广电总局网络司推动下，中国网络视听节目服务协会互联网电视工作委员会与广电总局广科院联合开发建设的互联网电视客户端号码和应用白名单管理平台正式上线。

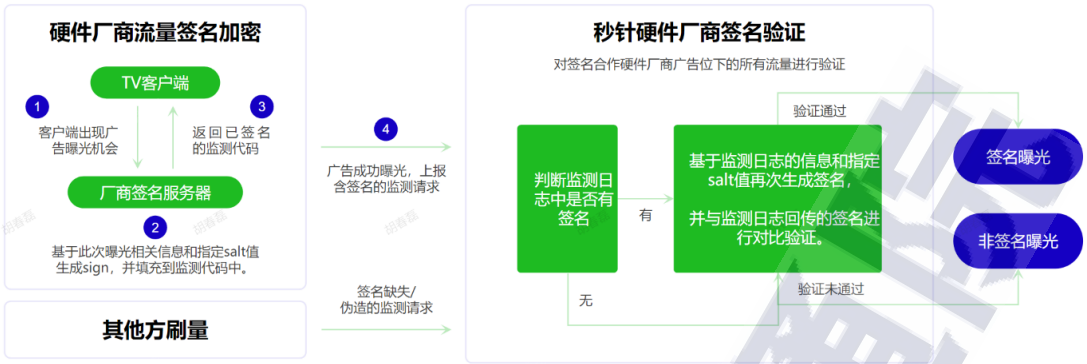
2021 年 12 月 15 日，中国网络视听节目服务协会发布了《网络短视频内容审核标准细则》，其中提到，短视频不得未经授权自行剪切、改编电影、电视剧、网络影视剧等各类视听节目及片段。

3.跨行业合作，共建安全生态系统

电视产业链复杂，安全环节众多，单独一家厂商难以形成完善的安全防护体系，在专业团队的协助下共同面对安全挑战无疑是更优的选择。

2018 年 10 月开始，国内多家主流电视品牌陆续宣布与某头部互联网公司安全团队达成技术合作，借助该安全团队的互联网电视安全解决方案，帮助互联网电视扫除安全雷区，共同建设智慧家庭安全生态系统。

针对流量欺诈问题，互联网电视硬件厂商协同监测公司研发的流量签名加密技术，可对互联网电视硬件厂商进行流量验证，规避刷量风险，图 4 展示了互联网电视硬件厂商广告流量签名加密验证流程。

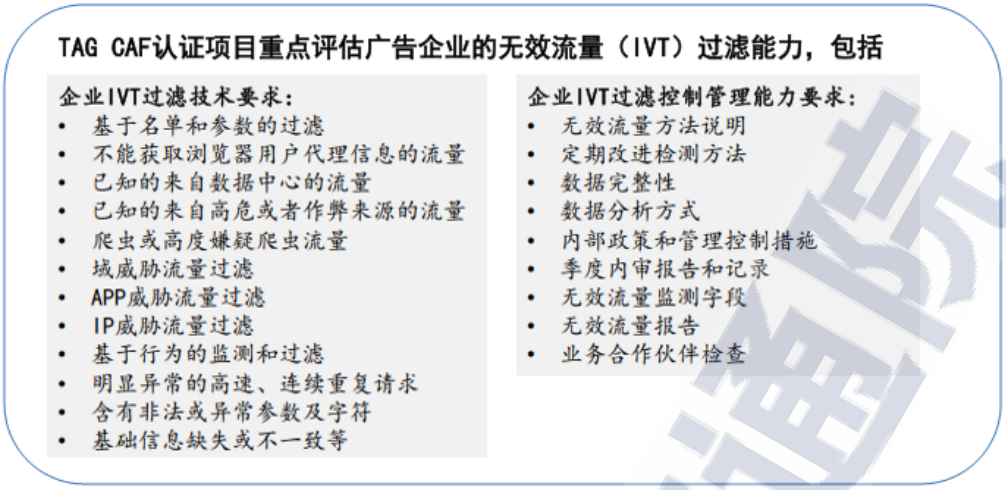


来源：秒针信息技术有限公司

图 4 互联网电视硬件厂商广告流量签名加密验证流程

4.权威检测认证，提升自身安全能力

2020 年 4 月，TAG 与中国广告协会（CAA）开启合作，共同推动中国市场国际标准及应用。由 CAA 和中国信通院联合发起的中国互联网广告技术实验室（CDA Tech Lab）于 2021 年正式启动“TAG 流量反欺诈认证项目”，为企业提供独立验证服务，帮助中国市场消除广告流量作弊风险。据 TAG 官方网站显示，多家中国公司已通过流量反欺诈认证评估，获得标签。图 5 展示了 TAG CAF 认证项目对广告企业无效流量（IVT）过滤能力的评估要求。



来源：中国信通院

图 5 企业无效流量（IVT）过滤能力的评估要求

5.数据安全和个人信息保护专项治理

（1）数据安全和个人信息相关法律颁布和实施

以 2012 年《全国人大关于加强网络信息保护的决定》为开端，为进一步加强对个人信息的保护，国家先后出台了《中华人民共和国网络安全法》《全国人民代表大会常务委员会关于加强网络信息保护的决定》《最高人民法院、最高人民检察院关于办理侵犯公民个人信息刑事案件适用法律若干问题的解释》《中华人民共和国刑法修正案（九）》等一系列法律法规。这些法律法规解释了个人信息的定义，提出了个人信息收集、使用、传输、存储的相关要求，并明确了个人信息泄露后的罚则。

2021 年我国两部重磅的数据安全和个人信息基础性法律接连落地。9 月 1 日起实施的《数据安全法》，对我国境内数据收集、存储、使用、加工、传输、提供、公开等数据处理活动做出了基础性法律依

据。11 月 1 日起实施的《个人信息保护法》明确不得非法收集、使用、加工、传输他人个人信息，个人信息权益受到法律保护，企业等组织对个人信息的处理需要合法合规。

（2）APP 个人隐私保护专项治理

2019 年，中央网信办、工信部、公安部、市场监管总局指导成立了 APP 违法违规收集使用个人信息专项治理工作组，在全国范围内组织开展 APP 违法违规收集使用个人信息专项治理行动。

2021 年，聚焦热点难点，强化专项治理。针对用户反映强烈的 APP 开屏弹窗信息“关不掉、乱跳转”问题开展专项整治，推动主要互联网企业基本解决了相关问题。尤其是在重要节假日等关键时间节点，聚焦假日出行、住宿等民生服务类 APP 开展专项检查。2021 全年，累计开展了 12 批次技术抽检，通报了 1549 款违规 APP，下架 514 款拒不整改的 APP。

2021 年 11 月，工信部印发《关于开展信息通信服务感知提升行动的通知》。督促企业建立个人信息保护的“双清单”，完善终端隐私政策和权限调用管理，提升客服服务能力，形成服务提质和感知提升良性互动。

2022 年工信部坚持综合治理，完善全链条监管。重点突出关键责任链监管，对应用商店、第三方软件开发工具包（SDK）、终端企业、重点互联网企业等实现监管全覆盖，打造更为安全的信息通信消费环境。

四、互联网电视安全检测与分析

针对互联网电视可能存在的安全问题，中国信通院泰尔终端实验室联合蚂蚁、盘古、安恒、启明星辰、娜迦等安全团体，组织开展了互联网电视安全评测。本次安全评测实验室选取了目前市场上互联网电视的 7 个主流品牌型号的产品，评测内容包括：硬件安全、操作系统和系统组件安全、预置应用安全、第三方软件安装安全、个人隐私和数据安全等 6 个方面 66 项内容，检测内容具体如表 1 所示。

表 1 互联网电视检测内容说明

模块	检测项	检测指标
硬件	固件安全	是否存在固件更新风险；能否直接读取固件内容，还是仅能通过系统预留的更新接口来读写；固件符号调试信息是否去除
操作系统	系统安全配置	系统是否进行了安全配置，如开启 SElinux
	调试安全	调试接口（adb）是否可远程非授权开启
	安全启动	系统是否有安全启动校验机制，逐层验证系统的完整性，保证系统不被篡改
	系统更新	是否有更新功能，更新过程是否有数据加密和身份验证，是否有完整性交验，是否有签名。
	系统回滚	系统是否存在回滚风险，即是否不允许系统进行版本降级更新
	安全漏洞（已知安全漏洞）	是否存在未修复已知高危或严重漏洞
	端口安全	是否不存在开放端口，可供下载安装任意软件、远程静默安装、远程打开应用
	第三方应用安装	是否关闭未知来源安装，不能允许随意安装第三方应用
	账号权限安全	多用户账号的系统，用户权限分配是否遵循最小权限原则，普通用户只拥有系统赋予的最小权限，禁止越权操作
	串口安全	检测是否存在调试串口；串口是否输出敏感调试信息；若存在串口交互外界模组或设备，应评估场景是否影响业务安全
	数据分级存储保护	检测数据存储是否对敏感数据使用权限保护机制进行保护

系统组件	电视控制权限管理	是否进行权限的校验；是否禁用工程模式
	组件更新安全	关键组件更新是否采用签名校验
	通信传输安全	系统通信是否采用安全传输信道，如 SSL 传输等
	已知漏洞检测	是否存在已知漏洞
	用户信息保护	是否存在未告知联网行为情况下传输用户数据
	蓝牙协议	是否存在重放攻击等
	系统内置应用组件安全	系统内置应用组件是否存在安全性风险，例如提权，信息泄露等问题
	语音控制安全	检测语音控制模块是否存在安全缺陷，如可窃取用户语音数据等
	摄像头安全	检测电视自带摄像头是否存在控制缺陷，可被远程恶意控制，如远程静默开启等
客户端 APP	安全加固	是否经过加固保护
	进程注入	是否有防注入防护功能
	逆向分析	dex 文件、SO 文件能否被反编译进行逆向分析
	二次打包	APK 是否能够重打包
	用户数据传输	数据传输是否存在未加密的用户关键数据
	用户数据泄漏	检测客户端 APP 是否存在用户敏感数据未加密写入外部存储空间或日志输出
	网络端口监听	检测客户端 APP 是否监听网络端口
	敏感 API 调用	检测客户端 APP 是否调用录音/录像/地理位置等敏感 API
	Manifest 文件高风险标志检测	检测客户端 APP 的 Manifest 文件是否存在高风险标志
	ZipperDown 漏洞	检测客户端 APP 是否存在 ZipperDown 漏洞
	本地拒绝服务漏洞	检测客户端 APP 是否存在本地拒绝服务漏洞
预置第三方应用	漏洞扫描	是否存在中、高危安全漏洞
	恶意行为检测	是否存在用户信息窃取、恶意吸费等恶意行为
个人信息保护检测	隐私政策相关安全检测	隐私政策内容展示、展示规则是否合法
	采集用户信息是否合法合规	规则是否合理、是否获得用户同意，是否超范围采集
	APP 权限申请是否合法合规	权限申请是否符合业务最小化原则
	第三方 SDK 隐私政策安全检测	检测第三方 SDK 中个人信息采集、用户数据共享和权限申请是否出现在 APP 的隐私声明

	用户授权是否可撤回、数据可删除	是否提供有效的注销账号的途径（如在线操作、客服电话、电子邮件等），并在用户注销账号后，及时删除其个人信息或进行匿名化处理，后台是否同步更新删除等操作
数据安全检测	用户敏感信息脱敏检测	检测系统内置 SDK、预装应用、APP 的敏感数据及个人信息在使用和展示过程中是否使用脱敏方式进行处理
	用户数据共享安全检测	检测系统内置 SDK、预装应用、APP 在运行过程中是否向第三方私自传输用户数据的行为
	用户数据传输安全检测	检测系统内置 SDK，预置应用、APP 是否存在用户关键数据未加密传输行为
	用户权益保障检测	检测系统、预装应用、APP 在运行过程中是否存在侵害用户权益的行为
	用户数据加密存储检测	检测系统内置 SDK、预装应用、APP 在运行过程中产生的本地数据权限是否安全，敏感数据是否经过加密

来源：中国信通院

通过检测，发现安全评测的产品普遍存在：安全漏洞未修复、越权操作、调试端口防护不足、应用可远程静默安装、漏洞修复率低、用户敏感信息明文存储和传输、预置应用安全防护缺失、APP 应用个人信息、权限过度索取、第三方 SDK 隐私协议缺失等安全问题，这些问题将会给用户带来非常大的安全风险。表 2 展示了互联网电视安全评测总体情况。

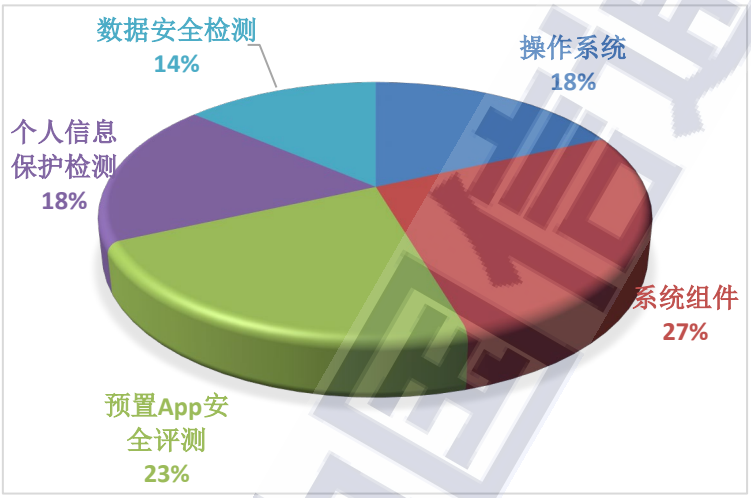
表 2 互联网电视安全评测总体情况展示

模块	检测项	存在安全风险的互联网电视所占比例
硬件	固件安全	20%
操作系统	系统安全配置	67%
	调试安全	67%
	安全启动	43%
	系统更新	75%
	安全漏洞（已知安全漏洞）	75%

	端口安全	29%
	第三方应用安装	100%
	账号权限安全	29%
	串口安全	67%
系统组件	电视控制权限管理	67%
	组件更新安全	25%
	通信传输安全	83%
	已知漏洞检测	100%
	用户信息保护	83%
	蓝牙协议	50%
	内置组件安全	100%
	语音控制安全	100%
客户端 APP	安全加固	86%
	进程注入	86%
	逆向分析	86%
	二次打包	71%
	用户数据传输	100%
	用户数据泄漏	50%
	网络端口监听	33%
	敏感 API 调用	67%
	Manifest 文件高风险标志检测	57%
	ZipperDown 漏洞	33%
	本地拒绝服务漏洞	17%
预置第三方应用	漏洞扫描	100%
	恶意行为检测	67%
	采集用户信息是否合法合规	60%
	APP 权限申请是否合法合规	80%
	第三方 SDK 隐私政策安全检测	40%
	用户授权是否可撤回、数据可删除	40%
数据安全检测	用户敏感信息脱敏检测	80%
	用户数据共享安全检测	100%
	用户数据传输安全检测	80%
	用户权益保障检测	20%
	用户数据加密存储检测	40%

来源：中国信通院

从问题分布来看，来自系统组件的问题最多为 27%，其次为预置 APP 的安全问题，占到 23%，来自操作系统和涉及个人信息保护的安全问题各占到 18%，数据安全问题则占到 14%。图 6 展示了互联网电视上几大安全问题的分布占比，以下进行分别的分析。

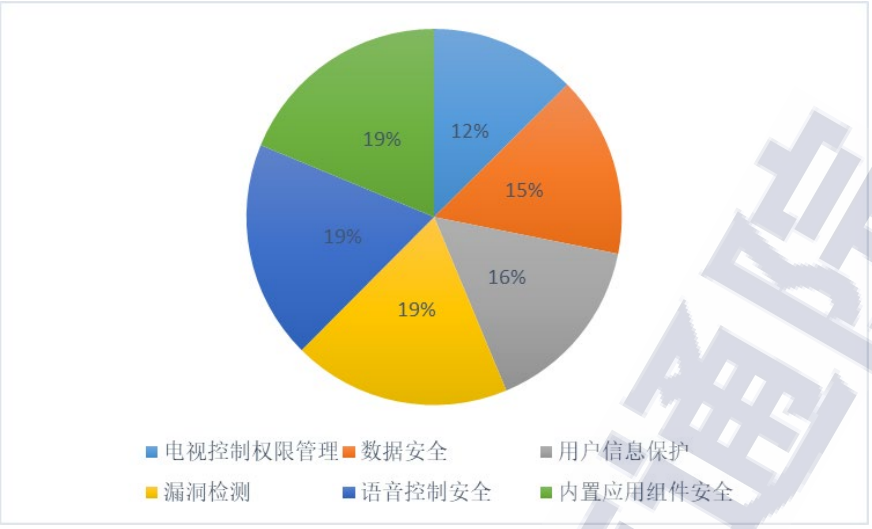


来源：中国信通院

图 6 互联网电视安全问题分布

(一) 系统组件安全问题

图 7 展示了测试中系统组件存在的主要安全问题，数据安全和用户信息保护问题整体占比为 31%。



来源：中国信通院

图 7 系统组件安全问题分布

1.存在大量未修复漏洞，易被黑客利用

目前 70%以上的互联网电视都采用的 Android，或在 Android 的基础上进行修改，由于 Android 系统的高度开放性，再加上互联网电视搭载的操作系统版本通常较旧，且安全更新不完全，使得对其进行漏洞挖掘更加容易。通过对被测互联网电视的操作系统进行漏洞扫描发现，大部分电视的操作系统存在大量未修复漏洞，甚至存在已被公开利用的漏洞。以测试的某款互联网电视为例，严重级别的漏洞有 25 个，如图 8 所示，漏洞年份可追踪到 2018 年。高危级别有 74 个，整体测出的漏洞数达 110 个，理论上讲，这些漏洞都可以被不法分子利用，利用这些漏洞对厂商、企业和用户利益造成损害。

序号	漏洞名称	问题简介	披露时间	严重程度	影响范围	修复情况
1	CVE-2018-9411	Android Media framework 安全漏洞	Jul-18	严重	AOSP	存在
2	CVE-2018-9427	Android Media framework 安全漏洞	Aug-18	严重	AOSP	存在
3	CVE-2018-9473	Android 安全漏洞	Oct-18	严重	AOSP	存在
4	CVE-2018-9497	Android 安全漏洞	Oct-18	严重	AOSP	存在
5	CVE-2018-9498	Android 安全漏洞	Oct-18	严重	AOSP	存在
6	CVE-2018-9527	Android 缓冲区错误漏洞	Nov-18	严重	AOSP	存在
7	CVE-2018-9549	Android 缓冲区错误漏洞	Dec-18	严重	AOSP	存在
8	CVE-2018-9552	Android 信息泄露漏洞	Dec-18	严重	AOSP	存在
9	CVE-2019-1987	Android 缓冲区错误漏洞	Feb-19	严重	AOSP	存在
10	CVE-2019-1988	Android 缓冲区错误漏洞	Feb-19	严重	AOSP	存在
11	CVE-2019-1989	Android 缓冲区错误漏洞	Mar-19	严重	AOSP	存在
12	CVE-2019-2027	Android 缓冲区错误漏洞	Apr-19	严重	AOSP	存在
13	CVE-2019-2028	Android 输入验证错误漏洞	Apr-19	严重	AOSP	存在
14	CVE-2019-2094	Android Media Framework 缓冲区错误漏洞	Jun-19	严重	AOSP	存在
15	CVE-2019-2106	Android 缓冲区错误漏洞	Jul-19	严重	AOSP	存在
16	CVE-2019-2107	Android 缓冲区错误漏洞	Jul-19	严重	AOSP	存在
17	CVE-2019-2130	Android 代码问题漏洞	Aug-19	严重	AOSP	存在
18	CVE-2019-2176	Android Media Framework 缓冲区错误漏洞	Sep-19	严重	AOSP	存在
19	CVE-2019-2184	Android Media Framework 缓冲区错误漏洞	Oct-19	严重	AOSP	存在
20	CVE-2019-2205	Android System组件资源管理错误漏洞	Nov-19	严重	AOSP	存在
21	CVE-2020-0096	Android Framework 安全漏洞	May-20	严重	AOSP	存在
22	CVE-2020-0441	Google Android 资源管理错误漏洞	Nov-20	严重	暂无数据	存在
23	CVE-2020-0442	Google Android 输入验证错误漏洞	Nov-20	严重	暂无数据	存在
24	CVE-2020-0458	Google Android Pixel 输入验证错误漏洞	Dec-20	严重	暂无数据	存在
25	CVE-2020-9589	Adobe DNG Software Development Kit 缓冲区错	Jul-20	严重	AOSP	存在

来源：中国信通院

图 8 某互联网电视系统上的严重漏洞

2.调试接口防护不足，容易越权操作

测试的 7 款互联网电视，67%的厂商在出厂时默认开启了 5555 端口，可使用 ADB 直接连接，开启 shell，可通过 shell 向设备中植入恶意代码，控制设备，如播放插播视频信息。测试信息如图 9 所示。

测试方法	**通过 adb connect host:port 命令对所有端口进行尝试连接。**
测试结果	在通过遥控器暗码打开 adb 后，可远程开启 ADB，无需用户授权，存在风险。 bogon:~ admin$ adb connect 192.168.1.130:5555 connected to 192.168.1.130:5555 bogon:~ admin$ adb devices List of devices attached FA69M0302845 device 192.168.1.130:5555 device
面临风险	暗码开启 adb 后，可以远程开启 ADB，静默安装应用
修复建议	禁止远程连接

来源：中国信通院

图 9 远程执行 adb shell 命令

3.应用安装方式多样，系统缺乏安全措施

搭载安卓系统的互联网电视可以安装丰富的应用扩展电视的功

能，应用的安装途径也是多种多样，用户既可以通过 PC 传输 APK 文件安装，也能在浏览器上随意下载安装。测试中，通过浏览器下载、U 盘、蓝牙、可连接的 ADB 接口尝试安装非本机应用市场的 APK 文件时，几乎所有的厂商都可以成功安装，并且没有任何安全措施，这样很容易遭受恶意 APP 的入侵。图 10 展示了具体的测试结果。

测试方法	**通过浏览器下载、U 盘、可连接的 ADB 接口尝试安装非本机应用市场的 APK 文件**
测试结果	可通过 ADB、 U 盘的安装任意应用，危险，电视应用市场没有浏览器。
面临风险	用户可能会安装到未经验证来源的应用，其中可能包含病毒木马等恶意应用
修复建议	当应用安装时，检查安装包是否属于本设备应用市场中的应用，如果不属于，应当给予用户提示，待确认后再进行安装，或者直接禁用安装非可信签名的应用。

来源：中国信通院

图 10 应用安装风险

4.语音控制模块存安全隐患，播报内容易被篡改

互联网电视为了向用户提供更加便利地使用功能，均加入了语音识别和控制功能，可实现语音控制开关机、搜索节目、打开应用等。测试人员对语音控制模块进行测试发现，部分产品的语音控制模块存在安全隐患。例如某设备内电视语音播报服务组件可被导出，并且无鉴权，攻击者可以启动该服务，并播报任意内容。在用户不知情情况下，播报任意内容，不仅存在内容安全风险，还会降低用户安全感，造成恐慌。图 11 展示了具体的测试结果。

测试方法	**通过漏洞扫描工具结合逆向分析，判断是否存在可导致用户数据泄漏的漏洞。**
测试结果	电视语音播报服务组件导出，并且无鉴权，攻击者可以启动该服务，并播报任意内容。 播报任意内容
面临风险	在用户不知情情况下，播报任意内容，不仅存在内容安全风险，还会降低用户安全感，造成恐慌。
修复建议	语音播报服务对调用包名验证。或者对播报内容加签和验签。

来源：中国信通院

图 11 语音控制模块播报风险

（二）APP 应用安全问题

1.安装软件包未加固，易被攻击者篡改

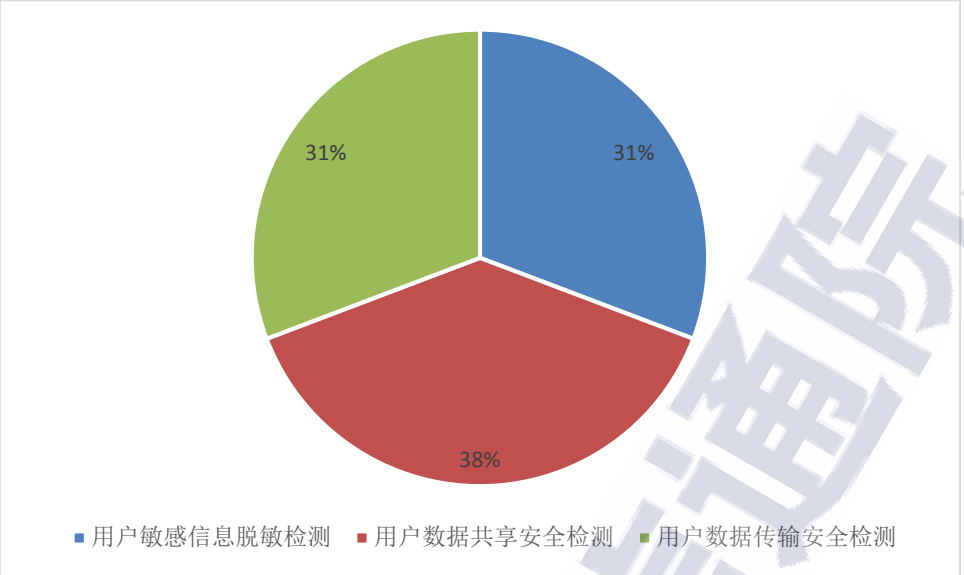
当前已上市的互联网电视中，80%的电视应用 APP 存在未加固的问题。由于应用未加固，攻击者可以以较低成本进行逆向分析，对应用解包后插入恶意代码进行二次打包发布。用户安装伪造的应用后，造成用户可能被钓鱼攻击，造成信息泄露和财产损失。图 12 展示了具体的测试结果。

来源：中国信通院

图 12 系统内预装 APP 未加固检测

2.数据安全问题严重，导致用户数据易被获取

数据安全主要侧重于在数据存储、传输和使用过程当中的数据保护的安全级别。图 13 展示了用户数据安全问题分布，数据安全问题主要集中在以下方面：



来源：中国信通院

图 13 用户数据安全问题分布

首先，数据共享安全问题比较突出。几乎所有的 APP 都存在和集成的第三方 SDK 共享数据的问题，但均未在隐私协议中有任何体现。

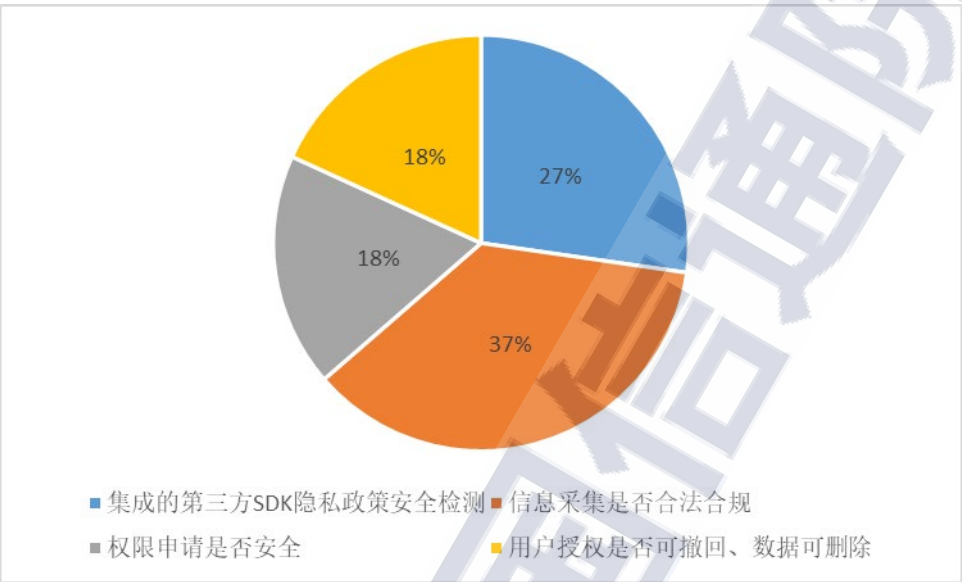
第二、用户敏感信息的未脱敏展示，具体表现在部分 APP 的登录账号是用户手机号，但在账号信息页面手机号码显示未进行脱敏展示，在数据传输过程中也没有进行脱敏处理。

第三、数据传输过程中，明文传输问题普遍存在。被测互联网电视的预置应用存在明文传输用户信息的行为，用户的遥控器操作、语音控制内容、个人收视习惯信息等可被攻击者窃取或被恶意劫持。例如，某款产品在接收用户手机端 APP 发来的遥控控制请求时使用明文传输，导致内容可被中间人监听，拦截遥控器操作、语音控制内容。

3.权限滥用，信息过度采集，导致用户隐私泄露

测试发现，互联网电视上的 APP 均涉及私自收集个人信息这个

问题，同时也包括私自共享给第三方、超范围收集个人信息、不给权限不让用、过度索取权限等问题，图 14 展示了测试中发现的隐私保护主要安全问题分布。

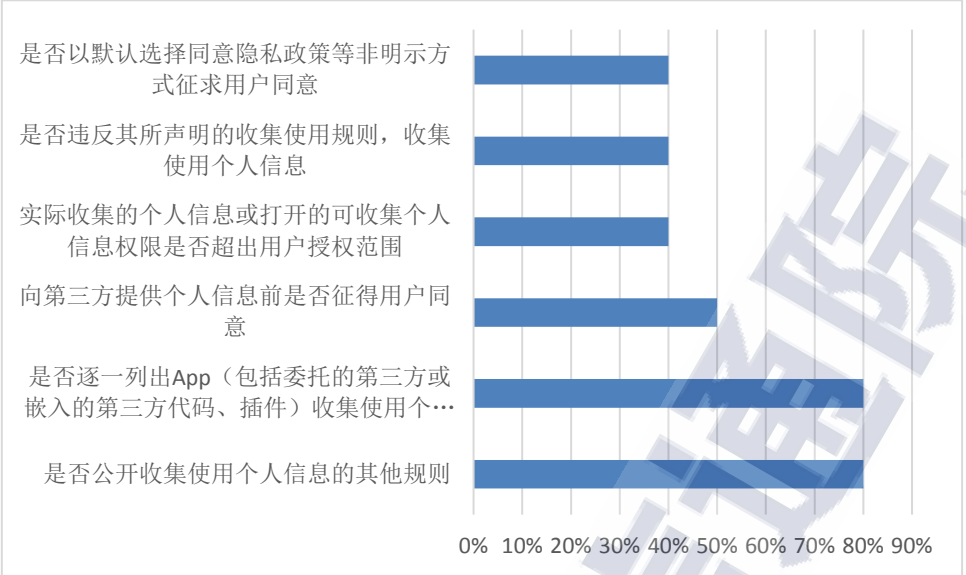


来源：中国信通院

图 14 隐私保护安全问题分布

4.隐私政策展示不完善，侵犯用户隐私保护权利

权限申请声明和信息采集声明在隐私政策中的展示问题也是隐私保护的一个重灾区。测试中发现，隐私政策问题主要集中在隐私政策展示时用户确认缺失、隐私政策中所声明内容和实际运行不符、隐私政策关于第三方权限申请和信息采集申明缺失等问题，图 15 展示了测试中发现的隐私政策展示问题分布。



来源：中国信通院

图 15 隐私政策展示问题分布

5.应用漏洞普遍存在，易被黑客利用

应用中漏洞普遍存在，极易被黑客攻击利用。以代码隐患引起的漏洞为例：测试发现，57%的互联网电视上的预置 APP 代码中的配置文件存在高风险标志位开启隐患，主要表现在配置文件中 allowBackup（是否允许备份）标志、debuggable（是否可调试）标志和 exported（是否导出）设置为 true，一旦设置这些属性，容易引发应用漏洞被黑客利用。如图 16 中某家测试报告所示，通过 exported 属性引发的导出漏洞，使得第三方应用可以直接调起组件，通过组件传送非法数据，进而影响应用的正常运行，进行业务流程劫持或入侵。

来源：中国信通院

图 16 组件导出漏洞检测展示

五、发展建议

OTT 行业是数字经济的实践者和先行者，在不断创造价值的同时，其数据安全、隐私保护等等问题需要产业生态共同努力，应从加强行业监管、完善政策标准、强化技术研究、推进检测认证、加强宣传教育等方面多管齐下，统筹发展。

(一) 加强行业管理，完善全链条监管

近年来工信部等行业监管机构纵深推进了对移动互联网终端和 APP 的侵害用户权益专项整治，取得显著成效。应加大对 OTT 终端如互联网电视及其 APP、SDK 的管理，重点突出关键责任链监管，

对 OTT 终端企业、电视应用商店、重点电视 APP、第三方软件开发工具包（SDK）、实现监管全覆盖，打造更为安全的信息通信消费环境。

（二）加快制定技术标准，解决行业痛点难点

针对目前互联网电视各家服务商对于用户隐私保护协议尚不规范的现状，特别是在数据管理、广告活动所需采集的个人信息种类和如何使用、存储和保护用户数据等方面，迫切需要制定《OTT 终端用户隐私保护协议要求》标准规范。

欧洲已实施的《通用数据保护条例》、我国已实施的《个人信息保护法》均将不可变更的设备标识（如 MAC 地址、IMEI）定义为个人信息，测试表明目前互联网电视终端里的 APP 和 SDK 均存在违规直接采集 MAC 地址等问题，亟需制定符合国家数据安全与个人信息保护要求，同时能够满足不同业务需求的《OTT 终端补充设备标识体系》标准规范。

（三）利用隐私计算技术，发挥数据要素价值

互联网电视的安全问题牵涉到设备厂商、应用厂商、媒体厂商等产业链的众多环节，任何一个企业都难以独善其身，合作共生更能合力解决复杂多样的安全问题。鼓励企业建立整体数据隐私安全策略，增强操作系统和应用软件在数据安全和个人信息保护方面的安全能力。同时将策略告知用户，内部对隐私保护和数据安全形成制度规则，形成流程，利用区块链、隐私计算技术等来建设安全体系。在信息使用过程中，通过匿名化等手段来推进信息的应用，将信息数据和具体

个人脱钩，从而达到信息数据流通的目的。

（四）推进安全检测认证，加强平台审核与管理

应借助社会团体、科研机构等力量，建立完善、规范的第三方检测体系，建立 OTT 终端安全检测能力，对智能电视的操作系统、应用软件、第三方 SDK、用户数据、个人信息保护等方面的安全开展检测认证，对互联网电视行业的信息安全进行规范性的指导和监督，促进法规和标准有效执行，从整体上保障行业的健康发展。为提升企业流量欺诈检测和识别能力，应继尽快推进三方企业进行流量反欺诈认证。

（五）加强宣传教育，提高用户隐私保护意识

人工智能和大数据的时代已然来临，大数据为大众的生活提供了极大的便利，但同时大数据也是一把双刃剑，如果使用不当，会对个人信息安全、财产安全造成严重损失。应加强用户教育，提高人信息保护意识，鼓励用户在选择互联网电视产品时，尽量选择经过安全认证的互联网电视产品和应用软件，使用软件时（如电视购物、电视支付）仔细阅读隐私政策相关内容，谨慎操作相关敏感权限，保护自己的合法权益。

中国信息通信研究院 泰尔终端实验室

地址：北京市海淀区花园北路 52 号

邮编：100191

电话：010-62309656

传真：010-62304364

网址：www.caict.ac.cn