中国科学: 信息科学 2015 年 第 45 卷 第 10 期: 1289–1309
www.scichina.com info.scichina.com
《中国科学》杂志社
SCIENCE CHINA PRESS
面向感知中国的新一代信息技术专刊 · 论文

智能云电视公共安全服务平台建设

王雅哲, 徐震, 王瑜, 晏敏, 张妍, 刘桐*

中国科学院信息工程研究所信息安全国家重点实验室, 北京 100093
* 通信作者. E-mail: liutong@iie.ac.cn

收稿日期: 2015–05–07; 接受日期: 2015–08–05; 网络出版日期: 2015–09–15
国家自然科学基金 (批准号: 61202476)、中国科学院战略性先导科技专项 (批准号: XDA06040502, XDA06010701) 资助项目

摘要 随着三网融合的推进, 智能电视行业得到了迅猛发展, 云电视是智能电视发展到目前的高级阶段, 更强调电视终端作为平台入口及其与海量云服务资源的平滑对接, 这势必将引发电视生态系统在硬件平台、操作系统、软件应用、网络云服务等多层面的信息安全问题. 本文针对 "行业内尚无统一有效的安全治理支撑手段"、"多源资源整合带来的内容安全问题" 以及 "云电视系统的开放性所引发的用户数据隐私保护威胁" 的现状, 构建了 "智能云电视公共安全服务平台"—— 主要包括证书认证服务子系统、终端安全代理子系统、安全监测中心子系统以及安全测评服务子系统. 该平台的建设, 将提供行业级的可管控的产业生态和可信的商业环境.

关键词 智能云电视 安全 公共服务平台 设备证书激活 安全代理 安全评测

1 概述

2010 年 1 月 13 日, 国务院首次将 "三网融合" 纳入国家发展战略后, 在相关管理部门和产业界的合力推进下, 新的一轮创新大潮汹涌而至. 在这轮创新大潮中, 作为 "三网" 中最为传统的终端 —— 电视, 先后经历了 "互联网电视"、"智能电视"、"云电视" 等不同的演进阶段. 其中, "智能电视" 具有开放式平台、可扩展功能、丰富软件应用、新型人机操控等技术特点, 而 "云电视" 是智能电视发展到目前的高级阶段, 更加强调电视终端作为平台入口及其与海量云服务资源的平滑对接, 这对芯片、设备、智能操作系统、应用、云资源的整体集成度提出了更高要求, 使电视摇身一变成为一个复杂生态系统的门户.

目前, 智能电视行业的发展呈现出如下的趋势:

(1) 开放式创新和产业链垂直整合将成为新时期智能电视产业发展的重要特征, 智能电视领域的创新模式发生了重大变化, 即开放式创新与商业模式的变更. 创新不仅仅要依靠研究所、研究机构、企业当中的科研人员, 任何人都可成为创新的主体, 任何有技术的人都可通过网络实现创新, 这是一种以用户为主导的开放型创新模式.

产业链的分工和整合模式发生了重大变化, 产业垂直整合成为大行其道的一种新模式. 只有垂直整合才能打造极致体验的产品, 从硬件终端到服务系统业务平台, 形成完整的 "平台 + 终端 + 应用" 的良好生态, 方可形成面向用户的强大生命力. 同时, 注重技术融合的趋势, 每一个产品、每一个系统,

引用格式: 王雅哲, 徐震, 王瑜, 等. 智能云电视公共安全服务平台建设. 中国科学: 信息科学, 2015, 45: 1289–1309, doi: 10.1360/N112014-00339

都在融合着更多的技术和装备, 垂直整合是纵向的, 而融合是横向的, 如电子技术、通信技术、安全技术等的融合, 正不断促进智能电视技术的完善与发展.

(2) 自主可控智能终端操作系统演进与生态发展, 电视领域的终端智能化产品形态 —— 智能电视, 目前引领了国内外彩电市场更新换代的发展方向. 而智能终端操作系统牢牢把控着智能终端产业的战略高地. 2013 年初, 工业和信息化部电信研究院发布的《移动互联网白皮书 (2013)》[1] 指出, 我国智能终端产业对安卓智能系统 (Android) 存在严重的 "路径依赖", 在发展中处于被动的劣势地位, 尤其是在智能电视操作系统领域, Andriod 系统几乎处于垄断地位. 虽然国内部分运营商、互联网厂商和终端厂商都做出了推出自主开发智能电视终端操作系统的尝试, 但由于缺乏战略性的布局, 无论是在技术成熟度还是在用户规模上, 都无法与国外的操作系统巨头如谷歌、微软、苹果等厂商匹敌. 这需要国家层面的政府牵引、全产业链的各方协同配合, 工信部、广电总局、科技部等各技术部门, 已在对此进行积极的部署, 并有多个自主可控操作系统项目的实施, 随着 HTML5 WEB 等开放应用生态的发展壮大, 电视用户操控、电视信息安全、电视服务系统等技术的发展完善, 势必将推动国内智能电视产业链的构建与完善, 并形成良性运行的应用生态环境.

(3) 以智能电视终端为核心的智慧家庭构建 [2], 随着电视终端智能化水平、运算处理能力及硬件配置水平的提高, 电视逐步成为家庭客厅的信息及娱乐服务中心, 同时通过多屏互动、设备互联互通, 延展为智慧家庭的构建中心, 电视作为家庭中心有其自身优势所在: 掌握客厅出入口、具有最广大的用户基础、家庭中最稳定的智能设备 (位置固定、存在时间长久), 为此, 以智能电视终端为核心, 开展智慧家庭的研究, 具有重要意义. 但目前, 此方面还存在诸多限制, 有待完善, 如: 不同制造商设备间协议不统一、互联互通困难; 业务处理能力较强, 但网络能力相对薄弱, 需要与网络能力设备 (如: 家庭路由器、NAS 等) 的紧密配合, 以及家庭网络拓扑结构和设备自组织发现互联机制的优化, 以方便用户使用; 与云端协同及智能电视终端设备间协同的机制有待建立, 使得家庭之间可以通过各自智能电视中心设备展开分布式拓扑结构, 实现以上各部分之间的交互协商、分工合作、资源调度等协同工作; 为家庭内海端设备提供云接入能力, 实现海云协同, 同时汇聚家庭内海端资源和服务能力, 实现彼此之间相互协作、集合承载.

我国彩电企业在国际智能电视产业发展中虽然占据了一定先机, 但智能电视的推广与应用仍面临诸多制约因素, 主要表现在:

(1) 智能电视设备的核心基础软件智能终端操作系统, 目前以谷歌公司的 Android 系统为主流, 其已占据智能电视终端 80% 以上的市场份额, 虽然目前 Android 采用开源开放的平台策略, 但作为国外公司的商业化产品, 随时会依据其商业策略的调整而改变发布策略, 对国内智能电视产业发展形成极大隐患以及潜在的信息安全等问题, 急需自主可控的国产操作系统的研发与推广;

(2) 智能电视在为用户提供个性化体验的同时, 面临信息领域的安全威胁和挑战, 为操作系统、应用程序、传输网络、资源服务等建立全方位的实时也安全着监测已迫在眉睫; 目前面向智能电视、智能终端的网络信任体系不健全, 需要完善的身份认证体系;

(3) 彩电企业单独建设的 "私有云服务平台", 平台之间几乎不能互联互通, 无法真正进入云产业环境, 企业付出成本高, 难以转型;

(4) 智能电视应用内容杂乱无章, 公共软件服务缺位, 用户体验感差, 安全性差, 缺少统一规范的软件评测系统或模型;

(5) 彩电行业与云服务行业间的产业相互渗透性不强, 适合电视特点的云平台的产业标准缺位, 彩电企业陷入了投入与产出失衡的窘境.

长期来看, 云电视的发展将引发电视行业乃至三网融合大产业链的格局和资源配置的变革. 各类

公司的涌入为电视行业带来了产品创新和发展活力, 有助于提升电视终端的用户粘性, 同时这种融合带来的云电视产业生态碎片化的风险也应尽早关注. 在这方面, 基于 Android 的智能移动终端生态碎片化的现状是前车之鉴. 尤其在目前绝大多数国产云电视采用 Android 操作系统的情况下, 更应该提前准备行业治理对策. 此外, 电视与互联网的融合, 必然导致当前视频内容管理模式与互联网海量用户自生成视频内容的矛盾, 对云电视视频内容生态的治理也需要进行战略布局. 最后, 在云电视生态系统构建和整合过程中, 必然在硬件平台、操作系统、应用、网络、云服务等多个层面引发信息安全问题. 在这样复杂的产业生态环境中, 单凭厂商自身很难系统性的构建安全体系.

因此, 为加快推进彩电产业转型升级, 促进智能电视在我国的推广应用, 亟需在行业层面上建设一个智能电视公共安全服务平台, 从公共信息安全服务的角度建立信息安全基础设施, 以保证产业链各方资源交换和控制、公共数据的采集与分发, 实现云服务与电视服务的融合以及电视企业间的资源聚合协同, 从而加速形成更加完整、健康、有序的云电视生态产业链.

本文第 2 节分析了智能云电视所面临的安全威胁和挑战; 第 3 节介绍了智能云电视公共安全服务平台的建设架构; 第 4 节重点介绍了平台建设中的关键技术; 第 5 节展示了智能云电视公共安全服务平台的主要技术成果; 最后给出了全文的总结与展望.

2 安全威胁与挑战

智能电视是三网融合的终端交汇点, 因此也是信息安全问题的汇聚点, 主要体现在以下方面: 内容安全与保护、通道安全、终端平台安全、应用安全以及用户安全与隐私.

互联网与智能操作系统的引入, 使智能电视安全成为人们关注的焦点. 近年来, 智能电视所暴露的安全问题层出不穷. 当智能电视被入侵, 不仅可以窃取智能电视上本身存储的隐私信息, 还可以通过智能电视的摄像头等周边设备, 随时随地监控用户的生活. 此外, 用户观看电视节目时, 界面有可能被强制跳转, 存储的个人隐私被盗, 甚至通过 WiFi 网络将家庭所有连接 WiFi 的设备进行监控. 智能电视与互联网连接后, 和电脑、智能手机一样, 面临病毒、木马及恶意程序等安全威胁.

2.1 智能电视相关安全事件

近年来, 发生了一系列与智能电视相关的安全事件, 比如, LG 电视隐私泄露事件、三星智能电视系列漏洞事件以及 HbbTV 协议攻击事件, 引发了人们的广泛关注.

2.1.1 事件一 LG 智能电视收集用户数据

2013 年 11 月, LG 智能电视被曝会自动收集用户的浏览记录、观看历史等私人数据 [3], 并通过 HTTP 流量加密传输到 GB.smartshare.lgtvsdp.com 上, 这些信息可能被制造商用于在电视屏幕上投放智能广告. 即使电视本身的 “collection of watching (收集观看数据)” 设置被切换到 “off” 状态, LG 智能电视依然能捕获用户数据.

2.1.2 事件二 三星智能电视漏洞

(1) 2012 年 12 月三星电视 Linux 固件漏洞[1)] —— ReVuln 的专家发现, 采用最新版 Linux 固件的三星智能电视所存在的漏洞允许黑客定位联网的 IP 地址、远程访问和遥控电视, 甚至获得 root 权限

1) Samsung Smart TV security hole allows hackers to watch you, change channels or plug in malware. HighBit Security, 2012. http://www.highbitsecurity.com/news-20121212-samsungtv.php.

并安装恶意软件.

(2) 2013 年 7 月 Samsung PS50C7700 3D Plasma-TV 漏洞[2] —— 该款三星电视中的 web 服务器 (DMCRUIS/ 0.1) 会开放 TCP5600 端口, 如果攻击者通过电视的 IP 地址发送一个冗长的 GET 请求, 会使得设备瘫痪并重启.

(3) 2013 年 8 月黑帽大会曝摄像头远程开启漏洞 —— iSEC partner 公司专家使用多款三星智能电视的网络浏览器攻破前置摄像头, 控制 DNS 设置, 并向其他应用植入了类似病毒的代码, 通过利用这个漏洞, 入侵者将能够: 远程激活电视上的内置摄像头并监控客厅中的观看者; 劫持浏览器, 访问目标恶意网站, 比如一个假冒的银行网站, 从而盗取用户的银行账户密码等信息.

2.1.3 事件三 智能电视 HbbTV 漏洞[3]

(1) 2014 年 5 月, 哥伦比亚大学 Yossi Oren 公布红色按钮攻击漏洞, 主要攻击采用 HbbTV 标准的智能电视.

(2) 在广播塔与电视之间实施中间人攻击, 向数字流中注入恶意代码, 恶意代码可在用户打开某一频道时自动运行: 控制 WiFi 路由器和 PC、获取使用者的信用卡信息、更敏感的私人信息等.

(3) 一次攻击可同时将攻击代码注入多个频道, 黑客使用售价 1500 美元的 25 瓦放大器, 一次攻击能覆盖 35 平方公里, 使攻击目标达到数十万人.

2.2 威胁与挑战

在云电视产业升级过程中, 将主要面临 3 方面的安全挑战. 首先, 在行业治理方面, 目前行业内的网络信任体系不健全、设备层面和云服务层面的安全基础设施缺失、智能电视应用无序安装、电视操作系统运行环境缺乏监测. 其次, 在媒体内容管控方面, 云电视会对接大量网络视频资源, 尤其是用户自生成媒体内容, 恶意非法视频发现和播出控制的内容安全技术和机制需要更新. 最后, 在电视用户安全和隐私方面, 云电视会对接面向用户的大量商业应用, 账号、支付类的业务, 用户的数据资产安全亟待保障, 同时智能电视自身丰富的感知功能 (例如摄像头、智能家居信息采集等) 也会带来大量家庭和用户隐私泄露的风险. 以下, 我们从 3 个角度阐述主要的安全挑战:

(1) 云电视行业目前缺乏统一有效的安全治理技术支撑手段, 云电视产业和技术生态的健康运行和演化, 需要在电视终端、操作系统、应用和云服务间建立结构化的安全管控体系.

首先, 云电视作为一种新型的云端设备, 传统的身份标识已经无法支持各个业务实体在不同网络、不同业务间建立可靠的身份认证. 云电视行业可信设备标识及行业级设备管理体系的缺乏, 使得电视面向用户提供的各类增值业务安全得不到保障. 传统的异构认证机制带来的复杂性, 将降低实体用户对网络和业务的使用效率, 无法为各种业务应用提供统一、可靠的信息安全保障.

此外, 随着云电视平台向种类繁多的第三方应用程序敞开大门, 云电视应用环境急剧膨胀, 安装无序, 缺乏统一的程序安全准入机制. 隐藏在应用中的病毒、木马程序和流氓软件等可以直接进入电视, 对终端系统资源和 API 进行无限制的访问, 将对用户信息、终端设备甚至网络造成巨大损害.

最后, 云电视作为三网融合重要的承载终端, 缺乏终端至云端互动的整体监测防护体系, 无法判断云电视终端整体运行防护状态, 无法有效获知终端的异常事件和安全漏洞, 从而及时对终端异常情

2) Samsung TV Denial Of Service. 2013. http://packetstormsecurity.com/files/122502/samsungtv5600-dos.txt.

3) HbbTV potential security issue. http://www.supportforum.philips.com/en/showthread.php?16072-HbbTV-potential-security-issue.

况作出反应. 若无完善的安全监测防护体系, 云电视将会步智能移动终端后尘, 成为下一个碎片化的安全重灾区.

(2) 云电视多源视频资源整合带来的内容安全问题堪忧, 电视一直是我国主流传播媒介, 如何有效实现舆论引导、满足文化内容安全需求是领域管理需要应对的重大挑战.

通过有机融合传统功能电视与互联网媒体资源, 云电视让用户可以在互联网内容、数字卫星电视间进行自由选择. 不法分子有可能通过不同渠道对电视节目进行恶意的插播、篡改和流量攻击, 同时通过对业务网络的非法监视来破坏数字内容的机密性和完整性, 例如未授权的删除、插入、修改或重新排序、未授权的访问及未授权的拷贝与传播等.

互联网繁荣的根源之一在于包括视频在内的海量用户自生成内容制作、传播与使用. 而现有管控手段, 更多地聚焦在企业和机构层面, 在用户生成内容层面仅有些粗粒度的处理方式. 如何高效甄别违反我国文化内容安全政策的视频内容, 并推动健康内容的有效传播, 是亟待解决的重要问题. 云电视采用开放的智能操作系统, 这意味着 PC、智能移动终端上木马和僵尸网络问题的出现成为必然. 除去纯粹安全技术问题之外, 云电视环境下的木马和僵尸网络可以为敌对分子向海量观众实时推送非法宣传视频内容的通道, 针对其潜在的巨大风险, 我们必须做到防患于未然.

(3) 云电视生态系统的开放性给个人用户的隐私与数据资产安全带来隐患, 云电视生态系统的开放性是其活力的关键性影响因素, 然而开放性处理不好将危及用户的隐私及其数据资产的安全.

一方面, 作为用户访问互联网服务的入口之一, 云电视上会聚合电子商务、电子支付、微博、微信等应用, 进而存储大量用户个人的数据资产, 保护不当可能给用户带来巨大经济损失.

另一方面, 随着用户在云电视上观看视频、使用应用, 将会持续积累用户行为信息. 电视接入云平台后, 海量用户行为数据的释放与大数据技术的结合, 将潜在地危及云电视用户的个人隐私. 云电视操作系统、应用以及云平台的漏洞被不法分子利用后, 可能用来窃取用户的隐私, 甚至直接控制, 从而监视用户个人和家庭. 例如, 最近爆出的某款三星智能电视安全漏洞, 入侵者可以通过它控制电视上的摄像头, 随时观看客厅中的影像.

3 智能云电视公共安全服务平台的建设架构

2013 年, 中国科学院作为牵头单位, 与国内六大彩电制造商及百度共同推动了工信部智能云电视技术改造专项项目群的立项, 并承担了其中 “智能云电视产业链公共服务平台” 项目的建设工作, 中国科学院信息工程研究所在项目中负责云电视公共安全服务平台建设, 如图 1 所示.

云电视公共安全服务平台主要由以下子系统组成:

(1) 证书认证服务子系统, 建立整个智能电视产业链的身份管理基础设施, 为上层各种业务应用提供基于可信身份的电子认证服务;

(2) 云电视终端安全代理子系统, 负责安全存储、证书激活、应用安装管理、心跳数据采集, 监控海量云电视应用的合法安装, 防止恶意应用破坏整个服务平台生态环境;

(3) 安全监测中心子系统, 负责云电视安全运行各类数据的按需采集、统一集中管理、安全事件及时响应;

(4) 安全测评服务子系统, 负责安全漏洞分析、源代码安全性测试、升级包安全测试、应用程序签名发布等服务.

云电视公共安全服务平台建设, 将为云电视产业链生态环境提供安全技术支撑, 重点建设以下 3 个方面的能力:

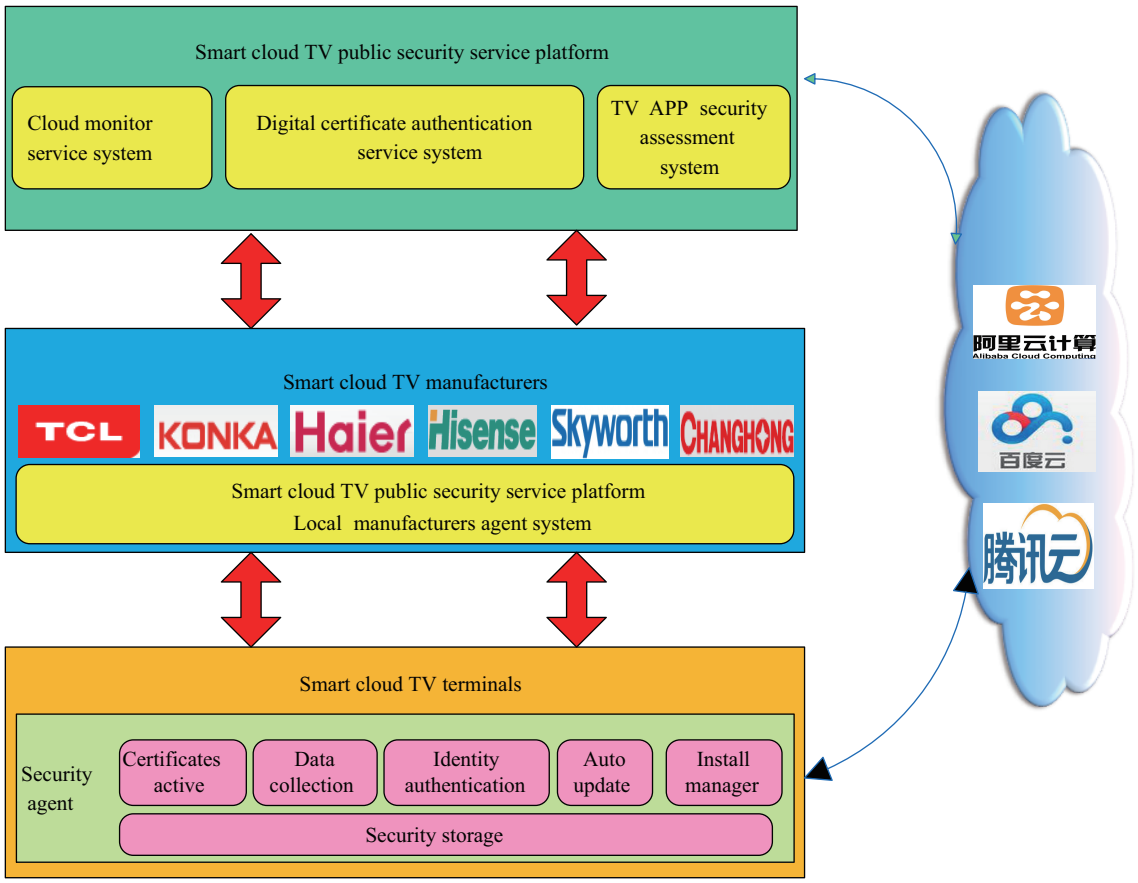

图 1　云电视公共安全服务平台架构图

Figure 1　The architecture of public security service platform for Smart cloud TV

(1) 面向云电视产业和配套服务环境的信任体系

建立基于数字证书的云电视生态链可信身份管理基础设施, 通过云电视设备证书激活机制, 建立行业级的统一设备标识管理体系, 为上层各种云服务账号系统提供可信身份绑定, 为公共服务平台与云服务商建立信任关系和身份联合服务; 基于设备标识和账号绑定建立电视用户身份可追溯凭据, 有效防止违法言论传播并支撑恶意内容传播源的取证工作.

(2) 云电视第三方应用程序安全测评与安全准入控制

建立面向云电视的安全测评中心, 通过检测第三方应用程序内部潜在的已知与未知恶意代码、安全漏洞、有害行为等安全问题, 通过安全等级测评保证电视操作系统的安全, 构建面向云电视产业链的市场安全准入机制, 形成云电视应用的第一道安全防线, 帮助云电视制造商与第三方软件开发商增强产品的安全开发意识, 提升其产品的安全等级, 力求从源头减少不安全的因素, 保护电视用户的安全和隐私, 促进云电视系统与软件市场健康有序发展.

(3) 云电视终端运行环境整体安全监测

与云电视制造商合作, 在电视终端部署安全代理系统, 定时监测终端中的异常事件和安全漏洞, 并依托监测中心对终端安全进行在线诊断, 保证用户及监测中心能对终端异常情况及时做出反应并进行安全更新; 监测中心同时提供云电视应用服务后台系统的安全运行状态, 并提供漏洞扫描、攻击防护

和应急处置等服务.

云电视公共安全服务平台的建设, 将为云电视行业提供可管控的产业生态和可信的商业环境:

(1) 产业监管方面

通过云电视设备层身份标识与上层应用服务账号系统的映射关联, 建立业务层面的用户资源, 为后期更多的应用系统导入和政府层面的用户行为合法监管提供信任支撑. 通过可信的计算环境构建, 为未来播控系统提供安全性支撑. 针对应用程序的安全审核、测评及验签安装管控流程有利于防止云电视生态的碎片化.

(2) 商业环境支撑方面

面向云电视终端运行的安全代理系统和面向云端数据中心的安全监测系统构建了云电视生态安全运行基础支撑体系. 为后继将视频服务、金融支付、电商平台等商业模式引入云电视生态系统提供了扩展空间.

4 关键技术

4.1 证书认证服务中心

4.1.1 证书认证服务中心架构

证书认证服务中心旨在利用 PKI 证书安全机制建立智能电视行业的可信身份安全基础设施, 构建起行业级中心 CA 和电视制造商子 CA 两级主从架构的信任管理模式, 支持千万级终端设备的身份溯源和异常定位, 从而为智能电视安全体系提供信任支撑, 并借助基于终端证书的二级架构身份认证服务, 实现智能电视终端与云资源的安全互通访问. 如图 2 所示.

行业级中心 CA 作为智能电视行业信任源, 负责签发管理制造商子 CA 根证书及一般运营性 CA 根证书 (如认证服务中心平台根证书、电视 APP 安全测评服务签名证书、社区开发者签名证书等), 同时采用安全策略与子 CA 系统完成签发证书同步, 实现中心 CA 系统对子 CA 系统证书签发量统计备案. 制造商子 CA 负责完成电视终端设备证书的在线激活及生命周期管理, 并定期完成与行业级中心 CA 证书同步工作.

中心统一身份认证系统负责同步对接二级身份认证系统的认证信息, 实现对子认证系统认证信息的统计备案管理. 二级身份认证系统负责与智能电视终端完成基于终端设备证书的身份认证、断言凭证发布、身份凭证状态同步等, 实现智能电视设备证书身份标识体系与云服务资源账号管理体系的安全对接, 从而使电视终端对各种云资源的安全互通访问.

4.1.2 基于设备指纹及设备人为特性的证书激活

针对智能电视设备证书在生命周期管理、使用流程等方面与传统用户数字证书有显著差异性, 设计了针对智能电视设备基于设备指纹 [4~6] 及设备人为特性的证书激活安全协议与实现方案, 支持设备实体触发的证书申请颁发机制. 如图 3 所示.

基于设备指纹及设备人为特性的证书在线激活安全协议涉及到厂商设备识别模块、证书申请代理模块、证书申请代理服务模块、厂商设备验证服务模块和二级 CA. 厂商设备识别模块负责将获取的设备人为特性 (人为定义固化的设备信息, 如设备 ID 白名单) 提交厂商设备验证服务模块处理, 同时提取设备自身某些自然属性 [3,7~10] (如恒定时钟偏移值、固件和驱动差异性、CPU 瞬时启动特性等), 并对设备自然属性进行特征抽取、样本训练、分类识别 [11,12] 和评价判定 [13] 生成该设备专有的设备

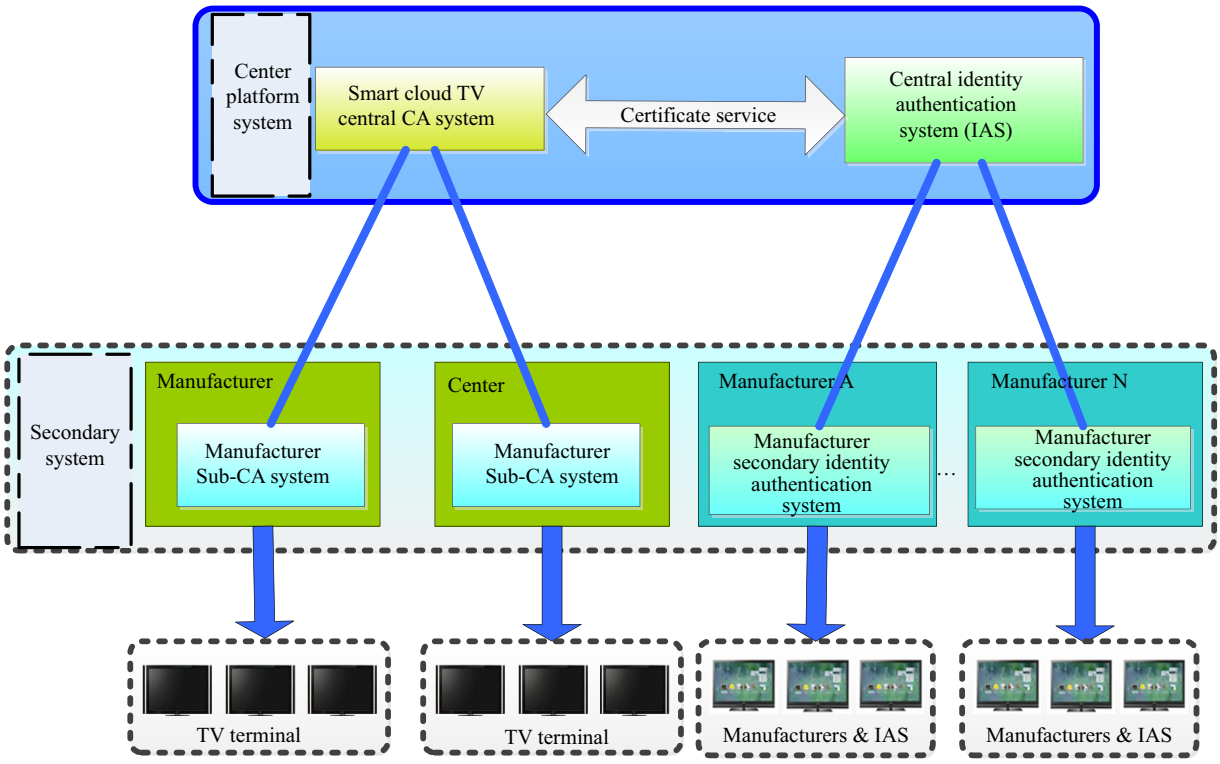

图 2　智能电视证书认证服务中心二级管理架构

Figure 2　Two-level management architecture of Smart cloud TV certificate authentication service center

指纹, 设备人为特性和设备指纹被作为申请设备证书的最重要组成信息, 以保证激活设备证书的唯一性; 证书申请代理模块负责将设备识别模块发起证书的签发申请 PKCS#10 (PKCS#10 包含证书请求信息 + 签名算法 + 签名值, 同时证书请求信息包含: 证书版本号 + 主体 (设备 ID + 设备指纹) + 主体公钥信息 (公钥生成算法 + 公钥比特值) + 其他设备属性 (可扩展设备唯一信息)) 转发给证书申请代理服务模块, 并处理证书申请代理服务返回结果; 证书申请代理服务模块基于白名单机制 (设备 ID 白名单) 完成设备人为特性二次验证, 将验证通过设备的证书申请请求转发给二级 CA, 由二级 CA 完成基于设备指纹 + 设备人为特性的设备证书在线激活. 该协议所有通信数据都在安全加密信道中传输, 设备人为特性的合法性必须由厂商验证和设备指纹由设备自然属性抽取生成, 可效避免山寨机通过复制软件模块完成身份激活, 以支持智能电视终端身份溯源和异常定位.

4.1.3　基于设备证书断言凭证的跨域应用身份绑定

针对智能云电视终端用户访问除了制造商资源、公共平台资源之外的其他云服务资源的单点登录的需求, 设计了基于设备证书断言凭证的跨域身份绑定 (称为跨域令牌交换) 的安全协议与实现方案, 实现用户 “一点联合, 多点访问”, 减少登录频率, 全面提升用户在智能云电视上跨域应用访问的体验. 如图 4 所示.

基于设备证书断言凭证的跨域身份绑定的安全协议涉及到身份认证代理模块、厂商设备识别模块、身份认证代理服务模块、二级身份认证系统和跨域应用 IdP 中心. 身份认证代理模块负责接受域

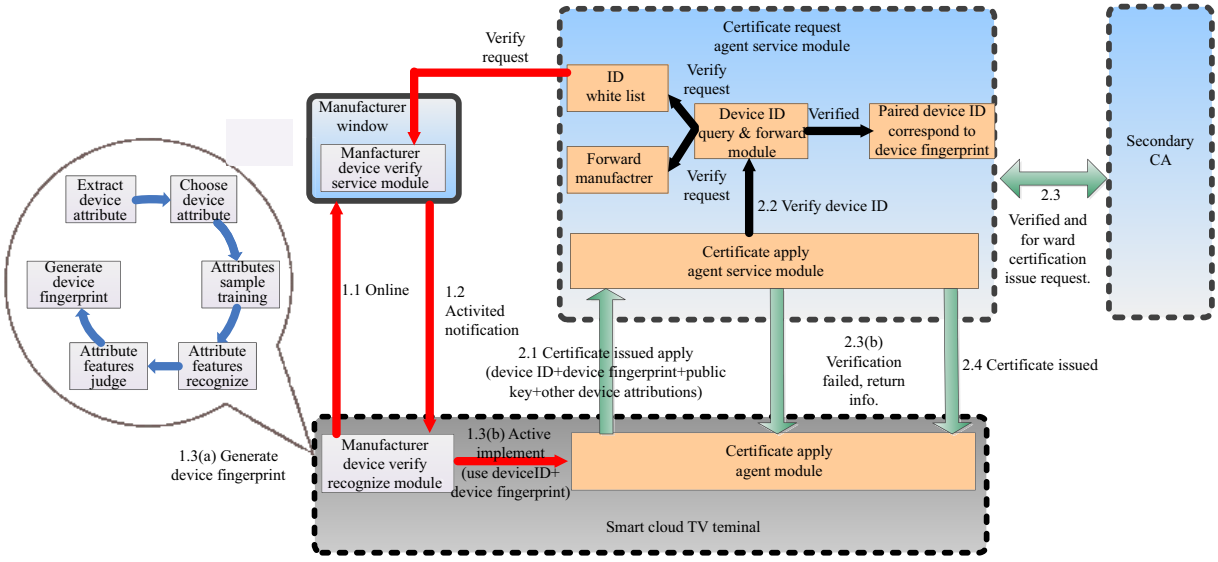

图 3 基于设备指纹和设备人为特性的电视实体触发的证书申请颁发机制

Figure 3 Certificate application publish mechanism based on device fingerprint and device characters

内应用/跨域应用身份认证请求, 从厂商设备识别模块获得设备 ID 和设备指纹, 将身份认证请求、设备 ID 和设备指纹提交身份认证代理服务模块处理; 身份认证代理服务模块负责依据设备 ID 查找对应设备指纹, 将查找到设备指纹与长传设备指纹比对一致后, 向二级身份认证系统发起身份认证请求; 二级身份认证系统负责与身份认证代理模块完成基于设备证书挑战/响应式的身份认证, 并生成用户身份断言凭证 (即用认证系统证书私钥对挑战值签名, 并将挑战值数以及挑战值签名通过代理服务返回给身份认证代理服务模块; 身份认证代理模块验证挑战值签名正确后, 使用安全存储区中激活设备证书私钥对响应值签名, 将设备证书和响应值签名通过身份代理服务模块转发给二级身份认证系统, 由二级身份认证系统先后完成终端证书和响应值签名验证通过后, 将生成包含制造商 ID、设备 ID、身份认证系统签名等信息的用户身份断言凭证 (如 SMAL, WS-federation, Json web token 等) 发送给身份认证代理模块安全存储); 跨域应用 IdP 中心负责将接收到身份断言凭证发送给二级身份认证系统验证通过后, 若判定该用户账号在 IdP 有效, 则为该用户生成一个有效期的跨域应用访问控制令牌发送给身份认证代理模块, 身份认证代理模块将用户身份断言凭证与跨域应用访问控制令牌绑定并安全存储, 从而为用户的跨云应用提供良好的单点登录体验, 简化了用户管理并提升了身份认证效率.

4.2 安全监测中心

4.2.1 安全监测中心架构

智能电视终端安全监测中心, 具体架构见图 5. 通过在智能电视终端预埋安全代理, 为智能电视提供了完整的安全策略执行机制, 能够被轻松的移植到 Android 的多个系统中, 无需更改电视操作系统原始架构. 在服务端, 通过对安全代理上传的数据进行实时采集, 实现对终端运行日志审计、终端认证及终端管控策略分发. 此外, 监测中心还对终端上传的应用运行数据进行统计查询并做多样化的展示.

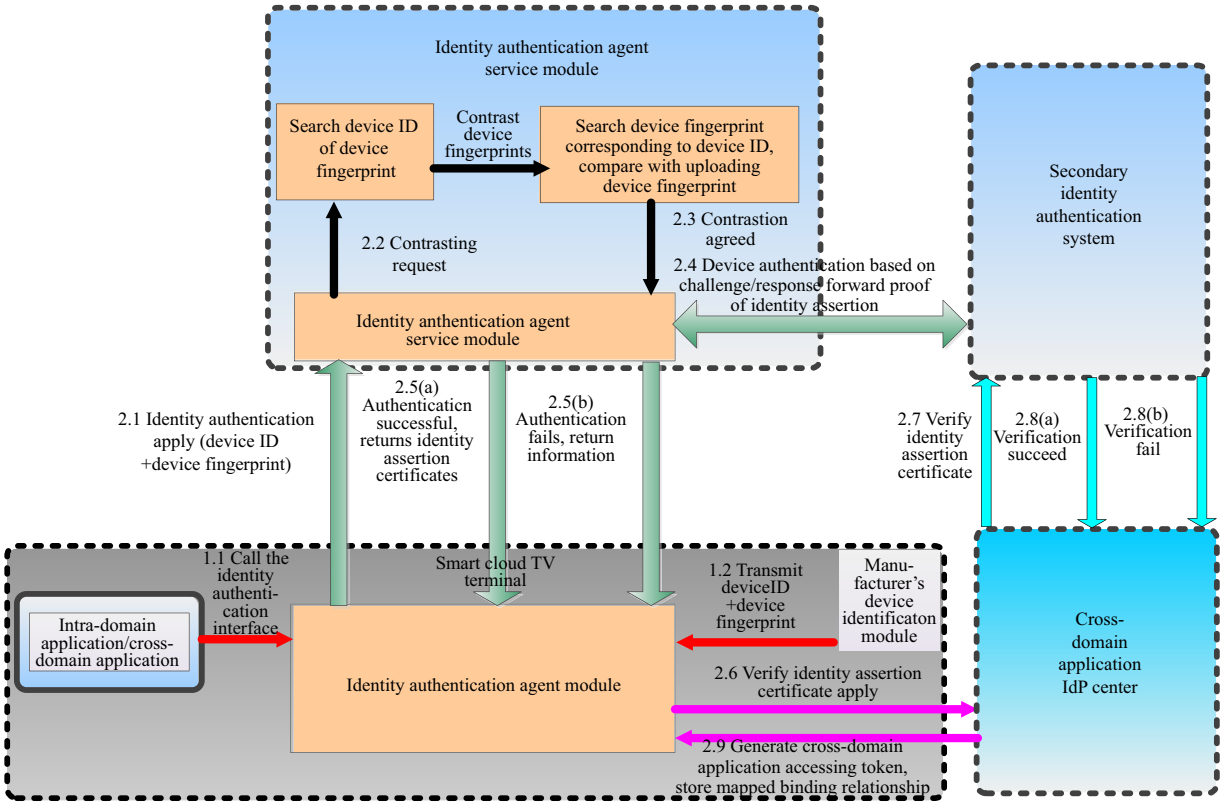

图 4　基于设备证书断言凭证的跨域应用身份绑定机制

Figure 4　Cross-domain identity binding mechanism based on device certificate assertion

4.2.2　基于企业策略分发的安全监测机制

在功能方面, 监测中心主要包括终端认证模块、策略分发模块、日志审计模块及历史数据查询统计展示模块. 认证模块负责对已经颁发终端设备证书的终端进行认证授权, 一旦被授权认证通过, 监测中心和终端将共享对称密钥, 他们的对话及传输数据会由共享密钥进行加密构成. 策略分发模块能够根据不同的电视厂商的安全需求或用户安全级别进行个性化定义, 并实时将定义好的策略分发到终端设备. 日志审计模块通过和终端的应用运行数据采集模块进行交互, 收集终端的软硬件运行相关信息, 并最终通过历史数据统计、查询及展示模块将搜集到的安全数据存储到数据库中并集中到展示运行平台进行动态实时展示. 在性能方面, 安全监测中心通过实时事务调度处理事务由不同的线程进行处理, 利用多处理器多核能力, 按照高优先级先行的原则进行调度处理. 并发控制采用多版本技术, 根据数据的性质划分不同的区域, 最大化事务处理的并行能力与数据访问的效率. 安全监测中心数据的存储, 采用关系数据库 (存储: 报警类数据、日志) 和实时数据库 (存储: 运行数据) 结合的方式实现对数据的存储和处理. 高效的历史数据压缩, 采用改进的旋转门有损数据压缩算法和 LZO 无损压缩算法, 不仅具有更高的数据压缩比, 而且不需要用户专门针对压缩参数进行设置, 能够根据数据特点自动进行调整以达到最佳性能. 安全监测中心采用将多个实时/历史数据库进行联合部署的方式从而实现所谓 "群集数据库". 合理地设计表结构 —— 合理地设计表字段, 表字段应该有合理的冗余以便于减少不必要的联表查询; 合理地增加字段索引, 以优化查询效率; 合理分表, 使单表数据规模适中. 具体结构如图 6.

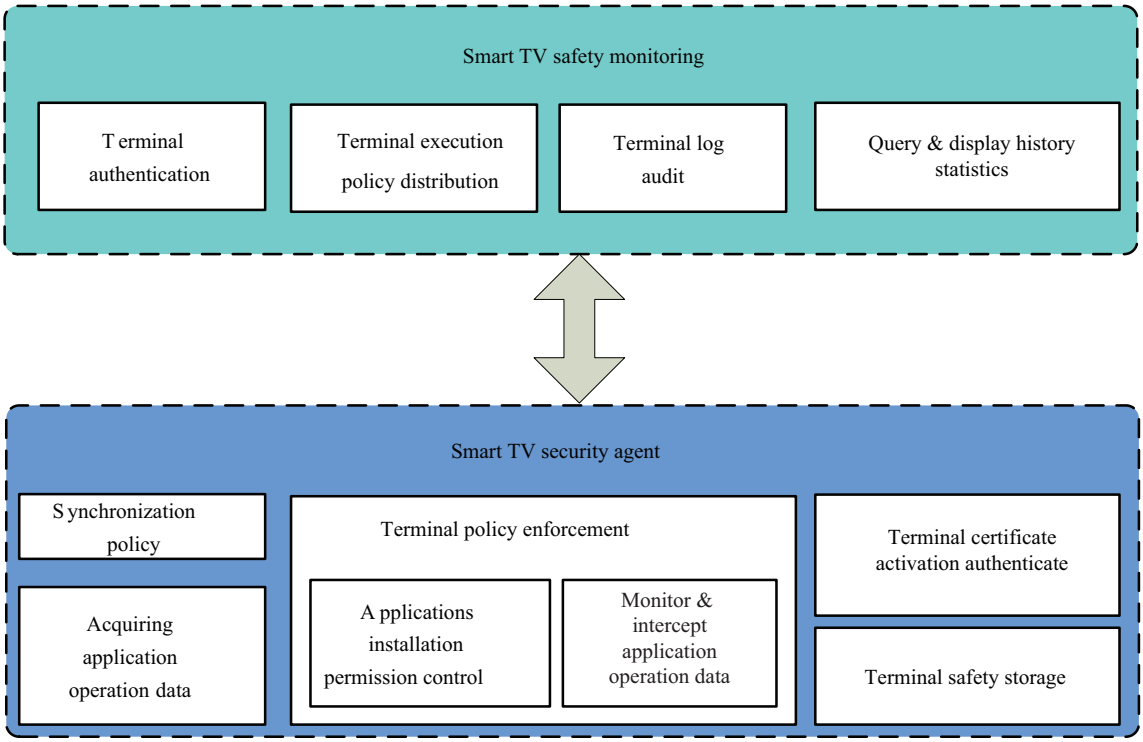

图 5 安全监测架构

Figure 5 The architecture of secure monitoring

4.2.3 基于策略的应用安全管控及数据监测机制

智能电视终端的安全代理 (具体结构如图 7) 分为策略同步、策略执行、证书激活认证、终端安全存储及数据采集上传功能. 终端策略引擎, 用于接收智能电视安全监测中心下发的执行策略. 数据采集上传模块能够实现对底层模块消息的接口, 并提取有效数据上传到监测中心进行分析. 证书激活及认证模块用于对智能电视终端颁发唯一证书并提供扩展应用. 智能电视安全存储用于存储用户隐私数据包括用户账户、私钥等信息. 通过设计实现的隐秘信息存储, 将标准文件系统中的磁盘映像文件, 虚拟并扩展成为一个类文件系统结构, 供上层应用模块访问, 使得上层应用透明的访问底层文件数据. 终端策略执行分为应用安装运行权限调用管控及应用运行数据监视拦截. 应用安装运行权限调用管控, 通过对在 Android 操作系统的内核层及本地库层进行代码注入 [14], 动态修改 System Server 进程的控制流来实现对应用运行权限的管控. 由于 System Server 进程有自己的 dalvik 实例, 所有加载的 Java 类及其方法都会被索引成类对象及方法实例, 而这些实例都会被分配到受 Dalvik 管理的 dalvik-LinearAlloc 内存区域. 每一个方法实例都会指向 System Server 的 Java 接口或本地方法, 所以, 通过在原始的 Java 方法实例中加入一些自定义的本地方法, 就能拦截这些 Java 接口对应的本地方法. 具体流程包括:

(1) 通过调用 attach_to_target 方法将注入代码插入目标进程中 [15];

(2) 通过在目标进程中调用 mmap 函数来获取一段空闲的内存区域;

(3) 通过调用 put_code 方法, 注入代码成功运行在之前申请的空闲内存区域;

(4) 注入代码和被注入的代码具有相同的操作权限.

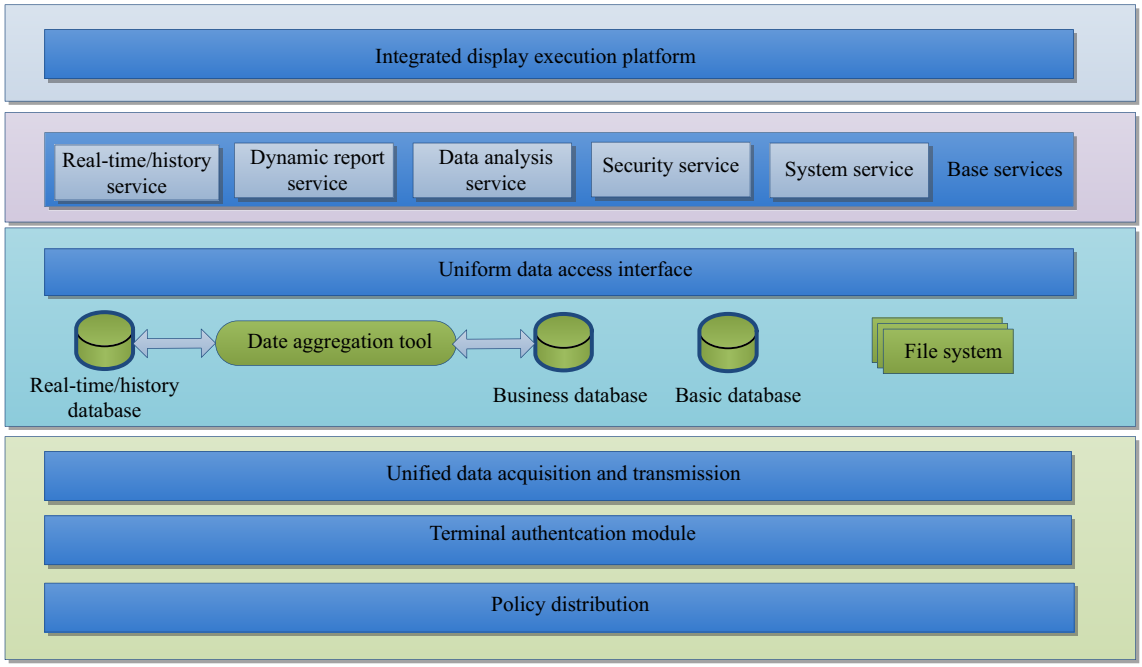

图 6　监测中心内部结构

Figure 6　Inner structure of monitoring center

通过以上方法能够修改系统默认的权限检查机制, 能够根据自定义策略进行应用运行权限管控. 此外, 通过修改 app 的补充组来控制 app 对底层关键驱动的访问 [16,17]. 应用运行数据拦截监视通过对应用程序数据细粒度的监视来实现对关键数据或行为的拦截. 该模块通过监视所有的系统服务远程调用, 监视所有系统资源访问传输数据, 及对 binder 驱动传输的 data 数据结构进行解析, 实现对传输数据的细粒度匹配过滤 [18].

4.3　安全评测中心

智能电视应用安全测评目标是建立智能电视应用多维综合风险评估能力, 为智能电视厂商和电视应用商城的用户提供第三方应用安全风险评估服务, 其涉及的关键技术主要包括海量电视应用检测调度平台技术、应用静态代码安全分析、动态行为监控分析、隐私泄露行为检测以及二次签名管控技术等.

海量电视应用检测调度平台, 是基于分布式云计算, 结合智能电视应用特点所开发的自动化检测任务调度平台. 该平台基于远程消息队列及 Thrift 远程传输协议进行多语言跨平台通信, 结合静态代码安全分析引擎、动态行为监控引擎、隐私泄露行为检测引擎, 实现智能电视应用的自动化检测, 具备高可靠性、高容错性、高效、高扩展性、跨平台等特点, 能够应对海量数据的并发处理和调度, 同时满足负载均衡的要求, 实现平台任务的高效处理和回收. 海量电视应用检测平台分为平台客户端、中心调度节点、检测引擎子节点、数据存储 4 大模块, 其中平台客户端使用多种设计模式, 实现检测任务的接收、组装并下发, 同时使用开源工具 apktool 实现对智能电视应用的预处理; 中心调度节点采用自研发负载均衡算法 [19] 实现海量并发检测任务的高效调度; 检测引擎子节点基于优先级任务队列实现任务自调度 [20,21]; 数据存储采用关系型数据库、非关系型数据库、文件数据存储等多种数据库相结合

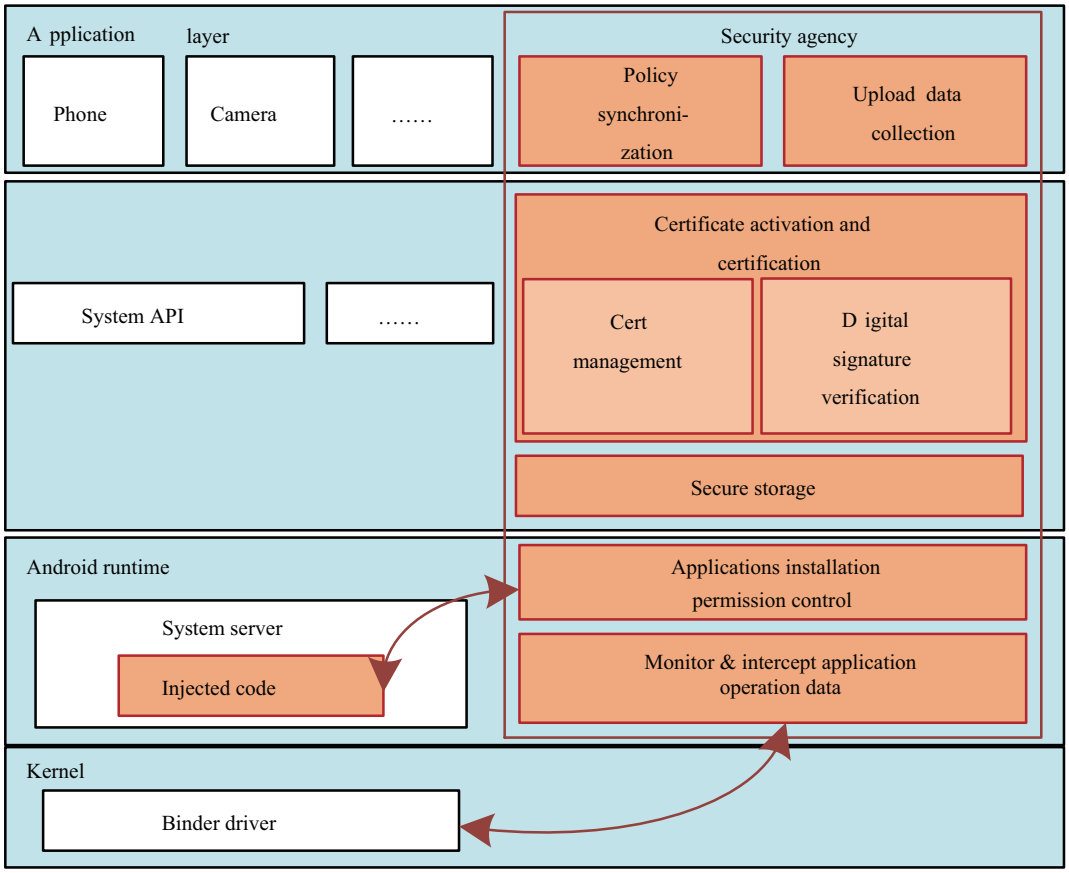

图 7 安全代理结构

Figure 7 The structure of security agent

的方式, 保证平台运行中的历史任务和历史检测结果的稳定存储和快速查询. 同时, 为了提高平台扩展性, 以低耦合高内聚为原则, 添加第三方检测引擎接口, 实现任意第三方检测引擎的实时快速挂载. 如图 8 所示.

4.3.1 静态代码安全分析技术

静态代码安全分析技术通过分析或检查源程序或者反汇编后的程序的语法、结构、过程、接口等来检查分析程序的恶意行为 [22]. 静态测试结果可用于进一步的查错, 并为动态测试流程设计提供指导. 如图 9(a) 所示, 静态测试关键技术如下:

中间代码解析 根据应用可执行文件的反编译得到的中间文件, 生成该应用的抽象语法树. 抽象语法树的逻辑结构就是可执行应用程序的逻辑结构, 包括根节点、类节点、函数节点、参数节点等层次, 从抽象语法树中, 可以得到整个工程的逻辑结构, 已知类和函数关系.

程序堆栈分析 根据生成的抽象语法树, 从主函数入口初始化函数开始, 根据函数调用、对象的实例化等关系, 递归追踪该应用中包含的类和接口、类中的函数参数和内部类信息. 获取程序调用堆栈信息.

代码质量审查 在代码解析、堆栈分析的基础上, 对每一次的追踪信息进行合理的安全分析. 主要通过检查程序中是否使用了过时或者不安全的 API 等危险行为.

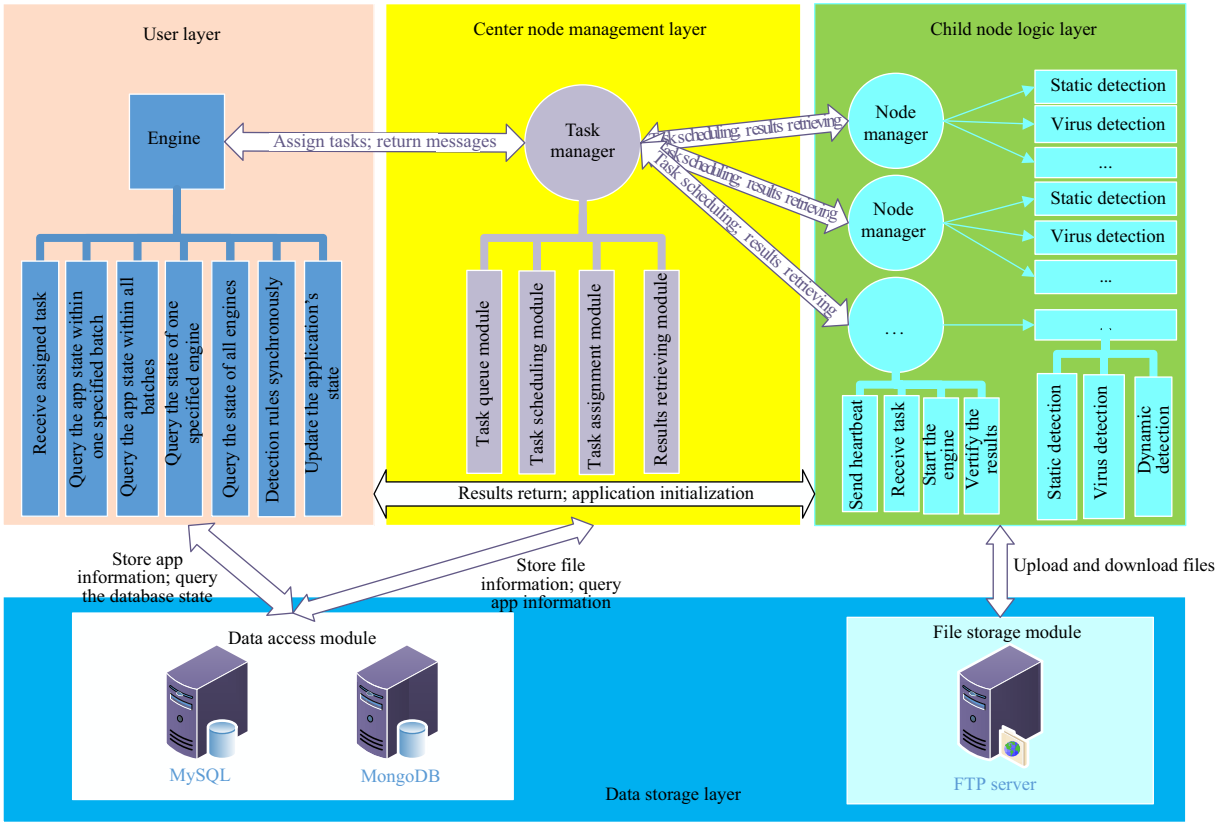

图 8　海量电视应用检测调度平台示意图

Figure 8　Huge TV apps detecting schedule platform

敏感 API 审查与形式化检测　敏感 API 调用, 主要指的是对网络调用、硬件访问、文件读写等电视 API 的调用情况 [23]. 静态检测模块会分析通过反编译代码得到的语法树, 从中查找出是否存在对敏感 API 的调用; 通过追踪信息对其进行形式化分析, 判断是否是用户发起的行为, 并根据基于距离算法的相似度匹配 [24], 进行特征分析.

应用程序恶意代码形式化检测　在检测的样本应用程序中, 对敏感 API 的调用并非是不允许的. 在许多应用程序中, 需要进行网络连接, 或者对其他敏感 API 的调用. 因此并不能把所有对敏感 API 的调用都认为是恶意行为. 应用程序恶意行为审查对中间代码语法树进行分析, 判定敏感 API 是否为用户调用. 若为用户调用则认为是合理的行为; 反之, 如果敏感 API 是在样本应用程序初始化过程中或者执行过程中利用其他线程来执行的, 那么就有可能是恶意行为, 具体情况需要进行进一步的分析.

4.3.2　动态行为检测技术

动态行为检测技术为应用程序的安全性评估提供原始数据, 具有重要意义. 动态检测工具通过在智能电视部署应用程序运行时行为检测模块, 对程序运行时行为进行监测, 发现恶意程序对智能电视的恶意操作, 以及访问软硬件系统进行恶意操控和破坏. 在监测过程中记录待测程序的各项运行时行为, 一方面, 可利用统计数据对程序的安全性进行评估, 评估结果可为静态安全分析技术中对恶意程序的威胁定义提供依据; 另一方面, 监测程序运行时行为使得恶意行为的快速发现和防御成为可能, 提高时效性, 可进一步加强和巩固程序的安全性评估体系. 如图 9(b) 所示, 动态测试关键技术如下:

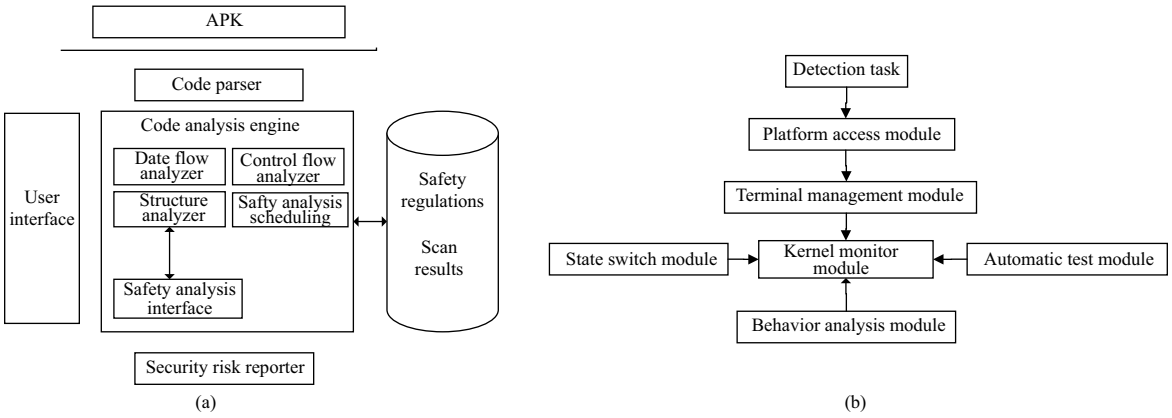

图 9 (a) 静态代码安全分析流程; (b) 动态行为监控分析流程

Figure 9 (a) Static code secure analysis flow; (b) dynamic behavior monitoring analysis flow

应用自动化安装、运行与卸载 动态检测模块通过调度程序接收到应用动态检测任务, 将在智能电视上自动执行安装、运行、卸载等操作 [23].

应用行为自动触发 应用在自动运行过程中, 采用 hierarchyviewer 和深度遍历算法遍历应用界面按钮和事件, 由动态脚本编写与执行程序动态生成 monkeyrunner 脚本, 模拟遥控器输入, 语音输入等用户输入, 触发按钮和事件, 用以模拟用户的真实操作.

应用行为自动监控与分析 动态安全分析指对程序的运行时行为特征进行监测, 并依照监测结果对程序做出安全性评估. 动态扫描通过在智能电视, 或者终端模拟器安装程序行为检测工具来检查应用行为, 动态检测引擎采用基于 Xposed 框架[4)]的动态监控系统, 并参考国标 8 项定义的应用软件恶意行为 [25]. 检测报告生成: 从应用自动运行状态检测的日志中, 分析提取出有效信息, 生成分析报告.

4.3.3 二次签名管控技术

二次签名管控技术在原开发者签过名的应用程序基础上, 使用权威机构 (如第三方应用安全测评机构, 智能电视应用商城, 智能电视终端厂商等) 的私钥证书进行不破坏其完整性和可用性的二次签名; 而在智能电视终端上, 通过预装权威机构公钥证书以及二次签名验签, 验证应用程序完整性未被原开发者以及权威机构以外的第三方破坏, 同时阻止未经权威机构认可签名的应用被安装入安卓终端. 技术如下:

二次签名 应用文件本身是一个压缩文件, 已经被开发者签过名. 首先将其解压到临时文件夹 temp 中, 计算其摘要后, 使用权威机构私钥签名, 将该签名注入应用中, 不破坏其可安装性.

二次验签 首先对应用文件解包并计算各个文件摘要值, 利用软件安全测评服务中心的公钥对已签名应用头部签名内容进行验签.

安装管控 待安装的应用被激活安装时, 安装器接收到其安装请求. 安装器接收到其安装请求后调用由管控程序从本地公钥证书存储区获取权威机构公钥证书路径, 调用内部验签接口对应用进行二次验签, 并给出验签结果. 验签模块将验签结果依次通过安全代理返回给安装器. 安装器对验签结果进行判断, 若结果为验签通过则安装此应用, 若验签失败表明此应用没有可信机构的签名, 则拒绝此应用安装.

4) Xposed, http://repo.xposed.info/.

5 云电视公共安全服务平台技术成果

该部分依次展示云电视公共服务平台总体架构, 分别展示证书认证服务子系统、安全代理及安全监测中心系统、智能电视安全测评子系统 3 项技术成果.

5.1 证书认证服务子系统

证书认证服务子系统利用 PKI 机制建立面向智能电视行业可信身份标识的安全基础设施, 采用行业级中心 CA 和厂商子 CA 的两级主从架构信任管理模式, 为行业内电视终端、制造商、开发者建立身份信任体系, 并为依赖身份信任的应用服务商提供信任源.

智能电视数字证书认证服务子系统主要包括智能电视数字证书中心、统一身份认证中心和厂商子 CA 等 3 部分, 具体取得成果包括:

(1) 设计并实现智能电视终端设备证书在线激活安全协议及其关键技术, 基于两级主从架构信任结构, 形成面向智能电视的行业级 PKI CA 系统平台, 主要负责提供终端数字证书和其他类型证书的生产、运营、管理等基础安全服务. 目前已完成根 CA、二级运行 CA、密钥管理系统、RA 系统、OCSP 和 LDAP 服务系统等子系统的建设部署, 支持百万级电视终端身份管理, 初步形成智能电视行业级的身份管理基础设施, 可为上层各种业务应用开展基于证书标识的电子认证服务提供平台支撑.

(2) 基于已部署的统一身份认证系统在公共服务平台和云服务提供商之间建立信任关系和身份联合服务, 为电视终端使用各制造商资源、公共平台资源、其他云服务资源提供基于终端证书的身份认证服务. 为用户的跨云应用提供良好的单点登录体验, 简化用户管理并提高身份认证效率, 并具备以下认证处理能力: SM2+SM3 签名效率 ⩾10000 次/秒、SM2+SM3 签名验证效率 ⩾8000 次/秒、RSA+SHA1 签名效率 ⩾12000 次/秒、RSA+SHA1 签名验证效率 ⩾18000 次/秒. 已部署的统一身份认证中心性能界面, 如图 9 所示.

(3) 针对智能电视行业内证书管理的特点和多类型实体的证书格式规范和命名规则, 结合智能电视设备证书激活、证书同步、基于设备证书的身份认证与身份绑定等安全业务的特点, 形成《智能云电视证书管理与服务技术规范》草案 v1.0.

5.2 安全监测系统现有进展

5.2.1 安全监测中心现有界面展示

目前安全监测中心能够监测到智能电视终端应用运行、安装、卸载、异常崩溃和系统资源占用等状态信息并提供数据处理分析、报表统计等多样化展示和报警功能. 支持百万级终端实时报警信息并发处理, 十万级终端信息处理延迟 <3 秒.

5.2.2 安全代理现有进展

通过在智能电视中使用 ptrace 实现智能电视系统进程注入等关键技术, 能够对关键敏感权限调用进行拦截, 无需修改系统源代码. 安全代理能够分 3 个层次实现对应用权限及数据访问权限的管控, 提供用管控三级管理模式, 供用户进行切换, 包括一级模式 —— 只提示用户, 不做管控, 此种模式下, 用户能够在电视屏幕右上角滚动窗实时看到应用权限调用行为及数据访问行为; 二级模式 —— 用户对单个应用可以访问的权限, 及某权限可以调用的应用进行高效个性化控制; 三级模式 —— 强制切断所有敏感权限的调用权限.

5.3 智能电视安全测评子系统

智能电视应用软件安全测评子系统面向多家智能电视应用商店, 提供应用软件自动化安全测评及测评过程全周期的信息化管理, 严格依据安全测评的技术、方法、标准和流程, 将测评实施与技术研发相结合, 通过采用静态源码分析、动态样本行为分析、恶意样本检测, 以及引入多家第三方检测引擎综合分析的方法, 实现全方位高效率的安全检测; 全面检查待测程序中可能存在的病毒、木马等各种恶意代码片断, 恶意行为表征, 安全漏洞库等安全风险; 能够应对海量数据的并发处理和调度, 同时满足负载均衡的要求, 实现检测任务的高效处理和回收, 并对检测结果进行风险评估, 根据评估的结果对非安全应用软件进行系统复检和人工复检, 保证了检测结果准确性和权威性. 系统中利用了二次签名技术对应用程序进行签名和验签, 确保发布的应用程序来源的真实性和内容的完整性; 同时, 系统还支持检测结果数据图形化统计, 可生成相应的统计报表, 便于数据的上报和分析. 智能电视应用安全测评系统具体服务能力包括:

(1) 安全测评能力

i) 病毒检测. 在已知病毒检测方面, 集成了 50 多家国内外知名病毒检测引擎, 对目前已知的智能电视应用病毒进行快速、全方位的查杀, 快速高效的保证智能电视及应用的安全性. 目前日病毒检测能力超过 300 款应用程序.

ii) 静态检测. 在研究 Android 智能电视应用程序各种安全威胁的特征基础上, 通过对已知恶意类软件和病毒类软件行为特征的收集和整理, 研究各种安全威胁的形式化描述, 建立安全威胁模式, 归纳总结并抽象出各种智能电视应用程序中安全威胁的本质, 并在此基础上进一步生成针对 Android 智能电视应用程序的安全规则; 利用 Android 应用程序的逆向反编译技术, 对智能电视应用进行逆向分析, 在词法、语法分析的基础上, 抽象出必要的信息并转换成中间表示, 根据需要生成特定的语法树结构, 进而分析应用程序的控制流和数据流, 构建控制依赖关系和数据依赖关系, 在依赖关系的基础上, 使用安全检测规则对应用程序中存在的行为进行匹配分析, 发现应用程序中存在的非用户触发敏感行为.

iii) 动态检测. 对于动态检测技术, 结合 Android 应用程序静态检测技术, 对智能电视应用程序的运行时结构进行分析, 深入研究 Android 智能电视的自动化动态测试技术, 实现 Android 智能电视应用的自动安装、启动、运行测试、卸载, 并将该动态测试的全部过程截图保存; 深入研究并利用 Android 智能终端动态行为激活技术, 在可控的真实及虚拟执行环境中, 自动化生成测试脚本, 动态触发应用程序中的控件信息, 模拟真实操作, 以获取恶意行为的触发条件; 对智能电视操作系统关键行为 API 进行 Hook, 监控记录程序运行时的系统调用和指令执行信息, 跟踪记录程序对网络数据处理的流程, 分析提取程序行为语义, 形成程序系统调用序列, 实现对 Android 智能电视安全的实时监控, 捕获恶意应用程序后台自动联网、窃取隐私文件等恶意行为. 目前在动态检测引擎关键技术方面已取得突破, 并完成原型系统开发, 下一步将实施产品级研发和部署.

iv) 有害行为检测. 在有害行为检测方面, 本平台主要也使用静态检测引擎和动态检测引擎. 检测内容主要包括违反国家相关规定信息散布、反动言论及出版物以及部分翻墙穿透类应用的检测. 在静态检测过程中, 通过对逆向后中间代码及资源的深度分析, 发现应用程序中存在的敏感内容及敏感信息来源等, 构建有害行为规则库, 对应用程序中使用的有害行为 API 进行检测分析; 在动态检测过程中, 通过程序运行过程中的图片识别技术, 对应用程序运行过程中出现的敏感信息进行捕获识别分析.

(2) 安全测评业务管理系统

智能电视应用软件 Web 安全测评管理系统采用 SOA 的软件架构风格, 系统按其功能分为应用

层、服务层、接口层和数据层四层架构, 每一层之间可独立部署. 应用层采用了模块化开发和跨浏览器技术, 为客户提供更友好的操作界面和业务操作流程; 服务层采用 “责任链” 的设计模式进行开发, 提供对工作流程的统一定义和对业务能力的扩展; 接口层则对第三方引擎提供接口定义和说明; 数据层采用 mybatis 引擎使用面向对象的方式进行对数据库的调用封装和展现, 实现数据存储与数据提取.

(3) 电视应用安全态势分析

面向智能电视应用生态圈, 对接应用商城获取应用入库, 分析识别恶意行为特征并进行分类, 定期分析和监控样本库和恶意样本库数量, 种类等属性数据变化趋势, 采用纵向和横向多维度相结合的应用特征统计分析, 协助向外提供实时安全态势分析报告与大规模安全事件爆发预警. 横向维度的统计属性包括: 应用商城来源、开发者、应用种类、上架时间段、下载安装量级等. 纵向维度的统计属性包括: 病毒主类 (如蠕虫、木马、间谍软件、Virus 等)、病毒种类、恶意行为国标八项分类 (恶意扣费、隐私窃取、远程控制、恶意传播、资费消耗、系统破坏、诱骗欺诈、流氓行为)、单项恶意行为内部细分子类 (如隐私窃取进一步分为媒体信息窃取、系统配置信息窃取、账号信息窃取、地理位置信息窃取等), 访问网址分类 (广告地址、恶意网址、应用下载网址等)、程序界面包含敏感词、程序稳定性等. 统计结果采用饼图、散列图、区域图、柱状图、曲线图、3D 图等形式可视化呈现, 以展示电视应用安全态势变化.

6 总结与展望

随着三网融合的推进, 智能电视行业发展迅速, 智能云电视以其开放性、可扩展性、新型人机操控以及丰富 App 应用等特点, 成为了新型的复杂生态系统门户, 也是信息安全问题的交互点. 目前, 智能云电视的推广及应用仍然面临着对 Android 系统依赖度过高、信息内容及用户隐私安全问题、企业间私有云难以互通、公共软件服务错位、缺少统一规范的管控等诸多限制. 为此, 2013 年, 中国科学院作为牵头单位, 与国内 6 大彩电制造商及百度共同推动了工信部智能云电视技术改造专项项目群的立项, 并承担了其中 “智能云电视产业链公共服务平台” 项目的建设工作, 中国科学院信息工程研究所在项目中负责云电视公共安全服务平台建设, 旨在保证产业链各方资源交换和控制、公共数据的采集与分发, 实现云服务与电视服务的融合以及电视企业间的资源聚合协同, 从而加速形成更加完整、健康、有序的云电视生态产业链. 本文就整个智能云电视公共安全服务平台的建设工作做了详细的介绍, 着重介绍了证书认证子系统、安全代理及安全检测中心系统、智能电视安全评测系统的构建工作, 并展示了相关技术成果.

在未来, 随着整个信息产业经历从传统的互联网到移动互联网的转变, 智能终端的功能和形态更加多样化, 人与人、人与物、物与物都能彼此连接, 我们将进入万物互联的时代. 届时, 消费类电子设备将全面融入互联网, 成为互联网的主要数据来源和重要生态入口, 从而带动相关产业链结构的重大调整和转型升级. 与此同时, 互联网化的消费类电子产品与其传统形态相比, 也将面临前所未有的信息安全威胁和挑战. 智能云电视仅仅是众多消费类电子产品之一, 建立智能电视公共安全服务平台是一种尝试, 也终将为消费类电子产品的公共服务平台建设奠定基础、开路导航.

参考文献

1 China Academy of Telecommunication Research (CATR). White Paper of Mobile-Internet. Beijing: China Academy of Telecommunication Research (CATR), 2013 [工业和信息化部电信研究院. 移动互联网白皮书. 北京: 工业和信息化部电信研究院, 2013]

2 He Y. The situation and development of smart community. Chinese Common Secur, 2014, Z2: 70–75 [何遥. 智慧社区的现状与发展. 中国公共安全, 2014, Z2: 70–75]
3 Egele M, Kruegel C, Kirda E, et al. PiOS: detecting privacy leaks in iOS applications. In: Proceedings of the 17th Annual Network and Distributed System Security Symposium. San Diego: NDSS, 2011
4 Anupam D, Nikita B, Matthew C. Do you hear what I hear? Fingerprinting smart devices through embedded acoustic components. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Scottsdale: ACM, 2014. 441–452
5 Zhou Z, Diao W R, Liu X Y, et al. Acoustic fingerprinting revisited: generate stable device ID stealthily with inaudible sound. In: Proceedings of the ACM SIGSAC Conference on Computer and Communications Security. Scottsdale: ACM, 2014. 429–440
6 Dey S, Roy N, Xu W, et al. AccelPrint: imperfections of accelerometers make smartphones trackable. In: Proceedings of the 20th Network and Distributed System Security Symposium. San Diego: NDSS, 2014. 1–16
7 Felt A P, Ha E, Egelman S, et al. Android permissions: user attention, comprehension, and behavior. In: Proceedings of the 8th Symposium on Usable Privacy and Security. Washington: ACM, 2012: 3, 1–14
8 Pang J, Greenstein B, Gummadi R, et al. 802.11 user fingerprinting. In: Proceedings of the 13th Annual International Conference on Mobile Computing and Networking. Montreal: ACM, 2007. 99–110
9 Brik V, Banerjee S, Gruteser M, et al. Wireless device identification with radiometric signatures. In: Proceedings of the 14th ACM International Conference on Mobile Computing and Networking. San Francisco: ACM, 2008. 116–127
10 Kohno T, Broido A, Claffy K C. Remote physical device fingerprinting. IEEE Trans Dependable Secure Comput, 2005, 2: 93–108
11 Gerdes R M, Daniels T E, Mina M, et al. Device identification via analog signal fingerprinting: a matched filter approach. In: Proceedings of the 13th Annual Network and Distributed System Security Symposium. San Diego: NDSS, 2006
12 Nabney I T. Netlab: Algorithms for Pattern Recognition. Berlin: Springer, 2014
13 Clarkson W B. Breaking assumptions: distinguishing between seemingly identical items using cheap sensors. Dissertation for Ph.D. Degree. Princeton: Princeton University, 2012
14 Conti M, Nguyen V T N, Crispo B. CRePE: contextrelated policy enforcement for android. In: Proceedings of the 13th International Conference on Information Security. Berlin: Springer, 2011. 331–345
15 Zhou Y J, Zhang X W, Jiang X X, et al. Taming information-stealing smartphone applications (on Android). In: Proceedings of Trust and Trustworthy Computing. Berlin: Springer, 2011. 93–107
16 Backes M, Gerling S, Hammer C, et al. AppGuard: enforcing user requirements on android apps. In: Proceedings of the 19th International Conference on Tools and Algorithms for the Construction and Analysis of Systems. Berlin: Springer, 2013. 543–548
17 Xu R, Saidi H, Anderson R. Aurasium: practical policy enforcement for android applications. In: Proceedings of the 21st USENIX Conference on Security Symposium, Bellevue, 2012. 539–552
18 Wang Y, Hariharan S, Zhao C, et al. Compac: enforce component-level access control in android. In: Proceedings of the 4th ACM Conference on Data and Application Security and Privacy. Scottsdale: ACM, 2014. 25–36
19 Wu S X. A research on multi-tasks scheduling of multi-level distributed command system. Dissertation for Master Degree. Harbin: Harbin Engineering Universeity, 2011 [吴绍欣. 分布式指挥系统分层多任务调度研究. 硕士学位论文. 哈尔滨: 哈尔滨工程大学, 2011]
20 Hong J, Wang H A, Wang Q, et al. A comprehensive design method of task priority. J Softw, 2003, 14: 376–382 [金

宏, 王宏安, 王强, 等. 一种任务优先级的综合设计方法. 软件学报, 2003, 14: 376–382]

21 Wang Y Y, Wang Q, Wang H A, et al. Design and implementation of a realtime scheduling algorithm based on priority table. J Softw, 2004, 15: 360–370 [王永炎, 王强, 王宏安, 等. 基于优先级表的实时调度算法及其实现. 软件学报, 2004, 15: 360–370]

22 Aho A V. Compilers: Principles, Techniques and Tools (for Anna University). India: Pearson Education, 2003

23 Han L S, Gao K L, Zhao B H, et al. Malware behavior detection based on the API function and its parameters combination. Appl Res Comput, 2013, 30: 3407–3410 [韩兰胜, 高昆仑, 赵宝华, 等. 基于 API 函数及其参数相结合的恶意软件行为检测. 计算机应用研究, 2013, 30: 3407–3410]

24 Hang D, He N, Ge H U, et al. Malware detection method of android application based on simplification instructions. J China Univ Posts Telecommun, 2014, 21: 94–100

25 Network and Information Security Working Committee of the Internet Society of China. Specification for Mobile Internet Malicious Code. Beijing: Anti Network-Virus Alliance of China, 2011 [中国互联网协会网络与信息安全工作委员会. 移动互联网恶意代码描述规范. 北京: 中国反网络病毒联盟, 2011]

Building a public security service platform for Smart cloud TV

WANG YaZhe, XU Zhen, WANG Yu, YAN Min, ZHANG Yan & LIU Tong*

State Key Laboratory of Information Security, Institute of information engineering, Chinese Academy of Sciences, Beijing 100093*, China*
*E-mail: liutong@iie.ac.cn

Abstract With the development of tri-networks, there has been a growing trend in the Smart TV industry. In particular, cloud TV has reached its highest level with widespread cloud service access. However, this has raised important security issues pertaining to Smart TV ecosystems including hardware platforms, operating systems, software applications, cloud services, etc. In this paper, we propose a Smart cloud TV public security service platform to address the lack of unified security management in the Smart TV industry. Our platform solves the content security problem when unifying resources from different parties and protects user privacy at the same time. Our platform has four implemented sub-systems, including a digital certificate authentication system, device security agent system, security monitor system, and security measurement system. Evaluation shows that our platform can provide a cutting-edge Smart TV ecosystem as well as a trusted business environment.

Keywords Smart cloud TV, security, public service platform, device certificate activation, secure agent, secure assessments

WANG YaZhe was born in 1979. He received his Ph.D. degree from the Software Institute at the Chinese Academy of Sciences in 2009. Currently, he is Associate Professor at the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. His research interests include authentication and authorization of distributed computation, security of smart connected devices, and Internet of Things.

LIU Tong was born in 1990. Currently, he is a master's student at the Institute of information Engineering, Chinese Academy of Sciences. His research interests include authentication and authorization of cloud computing and the security of the IOT.

XU Zhen was born in 1976. He received his Ph.D. degree from the Software Institute at the Chinese Academy of Sciences in 2005. Currently, he is Professor at the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences. His research interests include cloud computing security, and the security of networks and systems.