智能音箱产业发展研究及信息安全评测分析报告

国家广播电视产品质量监督检验中心

360IoT 安全研究院

二零一九年四月

前言

近年来，随着新一代信息技术的高速发展，以及政策和资本的推动，使得人工智能技术进入到应用阶段，从概念逐渐地走向产品，而智能音箱的有声资源播放、语音交互和智能家居控制等功能促使其成为人工智能领域最火热的话题之一。

智能音箱的普及带来的安全问题也日渐凸显。相较于传统音箱，智能音箱的连接性和功能性使其增加了病毒攻击、数据泄露和漏洞频发等信息安全隐患。由于智能音箱产业还处于发展期，安全技术的滞后和管理措施的欠缺尤为突出。如何明确智能音箱的安全需求，通过技术和管理手段，在推动智能音箱发展的同时保证其安全性，成为广大技术和管理人员亟待解决的问题。

本文从智能音箱产业的发展现状和信息安全问题入手，深度分析了目前市场上主要智能音箱产品的信息安全性能现状，提出智能音箱行业的信息安全发展建议。为切实可靠的针对智能音箱信息安全性能展开分析，我们得到了业内安全厂商的协助，依据国内相关标准以及参照信息安全领域国内国外安全架构广泛认同的安全性指标研究制定了智能音箱信息安全评测规范，选取国内外知名厂商的十款最新智能音箱产品作为测试样本，依据规范对样品进行了评测分析，完成了此次报告。

一、智能音箱产业概述

（一）智能音箱定义与功能

1、智能音箱定义

智能音箱是传统有源音箱智能化升级的产物，是指具备智能语音交互系统、可接入内容服务以及互联网服务，同时可关联更多设备、实现对场景化智能家居控制的智能终端产品。智能音箱集成了人工智能处理能力，能够通过语音识别、语音合成、语义理解等技术完成语音交互。

2、智能音箱产品功能

（1）语音交互体验

语音交互体验一直是智能音箱的核心功能。用户可以通过语音来操控智能音箱，从最基本的语音点歌，到相对比较复杂的上网购物。

目前国内推出的智能音箱也在语音交互方面也进行了更加深入的研究，提升了智能音箱对于自然语义的理解。

（2）有声资源内容分享

智能音箱作为一种播放载体，自然离不开内容的支撑，而对于智能音箱来说，内容不再仅仅只是音乐一种，而是包括各类有声资源。以内容分享为主的智能音箱，将音箱作为音乐、有声读物等流媒体内容载体，让用户有更多的内容可以在智能音箱上进行选择，满足用户对于内容的全方面需求。

（3）智能家居控制

智能音箱一直被看作是未来的家庭智能控制终端，而这也是各大厂商十分看重的一点。

从现阶段的发展情况来看，智能音箱已经能够控制基本的智能家居设备，就像一个万能的语音遥控器，可以控制灯光、窗帘、电视、空调、洗衣机、电饭煲等智能家居设备。

（4）互联网生活服务

互联网生活服务也是智能音箱非常重要的一方面功能，可以通过自身的平台资源或搭建第三方服务资源，实现语音购物，提供查询餐厅、路况、火车、机票、酒店、物流等信息，在不利用手机的情况下，进一步方便人们的生活。

（5）生活小工具

基于家庭的使用场景，智能音箱还开发了一些非常实用的小工具。如有些智能音箱拥有如计算器、单位换算、查限行、星座运势、留言机等小工具，在日常生活中给予用户便利，而且相比智能手机，智能音箱的语音交互方式会显得更加方便。

目前智能音箱已经拥有非常丰富的功能了，但是对于智能音箱整体的行业来说，智能音箱依然处于初级阶段，最常用的功能还是听音乐，其他方面还需要进一步的完善，才能真正应用于日常生活。

（二）智能音箱技术原理

目前的智能音箱多基于语音控制，其基本交互流程可以概括为三步：用户通过自然语言向音箱提出服务请求或问题；音箱拾取用户声音（音箱本地完成）并分析（一般在服务器端完成)；音箱通过语言播报（音箱端）和 APP 推送（关联的手机等）对用户的请求进行反馈。根据智能音箱的主要功能，其工作原理可分为以下两类：

1、智能音箱提供内容和服务的工作原理

假设用户向智能音箱发出“查询 A 到 B 的机票”的指令，智能音箱的语音交互系统通过语音算法本地处理单元和音频解码单元收集语音、降噪、识别唤醒词、将语音信号转为数字信号，之后将处理后的数字信号上传至云端服务器，云端服务器将进行语音数字编码识别和语义理解，随后通过调用机票预订数据库中的信息传递给智能音箱，智能音箱将上述数字信号通过音效单元还原为语音信号并播放出来。

2、智能音箱控制智能家居的工作原理

假设用户向智能音箱发出“关闭电灯”的指令，智能音箱通过语音收集、语音识别后将语音数字编码通过云端服务器进行语义理解，并将得到的信息回馈回到家庭路由器，通过路由器广播这条控制指令，智能家居设备拥有各自唯一的 IP 号，智能家居能够识别指令中是否涉及自身的 IP 号，最终电灯的插座识别完成后，完成关闭电灯的指令。

（三）智能音箱发展历程

2011 年美国亚马逊开始智能音箱的研发，至 2014 年 11 月发布了 Echo 智能音箱，内测半年后于 2015 年正式发售，由此掀开了智能音箱产业爆发式增长的大幕。亚马逊发布的智能音箱 Echo 受到市场强烈反响以后，谷歌在 2016 年 5 月发布 Google home，苹果在 2017 年 WWDC 发布智能音箱 HomePod。国内方面 2015 年京东联合科大讯飞推出叮咚智能音箱，是我国智能音箱产业的先行者；之后阿里巴巴和小米等企业也纷纷加入入口抢夺战。目前为止国内科技巨头 BAT、小米、华为，老牌电器厂商联想、苏宁，传统音箱企业 DOSS，语音技术企业科大讯飞、思必驰，硬件技术创业公司出门问问、若琪等都陆续通过自研或合作的方式入局智能音箱领域。

自此，每月都有一两家科技公司发布智能音箱新产品或二代、三代产品。国内外互联网和硬件行业巨头纷纷加入战局，争夺语音交互流量入口，带动了 AI 落地的一轮热潮。

（三）智能音箱核心技术分析

1、智能音箱核心技术概况

智能音箱将声学设计、无线技术、语音识别、远场拾音、语义分析等众多技术融合在一起，使得技术更为复杂，因此相较于普通蓝牙音箱，无论在硬件或软件系统上都采用了更先进的技术作为支撑。其中主要包括硬件层面的芯片技术、麦克风阵列技术和软件层面的智能语音技术。

2、芯片技术

智能音箱需要将识别到的自然界模拟信号转成数字信号，上传云端服务器分析后将接收到的数字信号处理成模拟信号再进行放大，因此额外需要应用处理器芯片和音频编解码芯片，这也是初代智能音箱的语音芯片架构。

相较于其他智能硬件，智能音箱只需要音频信号处理，不需要 4G 通信、 GPU 图形处理等功能，为了提升智能音箱性能，其核心技术由普通芯片慢慢转变为智能语音专用芯片，解决对麦克风阵列支持不好，算法不成熟等问题。智能语音专用芯片更加具备高集成度、低功耗、低成本、可定制化等特点。

3、麦克风阵列技术

麦克风阵列是由一定数目的麦克风组成，用来对声场的空间特性进行采样并处理的系统。麦克风阵列技术相对于单麦克风系统的优势在于当用户距离音箱较远或音箱设备处于复杂的环境中时，依然能够正常的收听用户的语音指令。麦克风阵列方案主要受成本和算法两个因素限制。一方面，虽然麦克风本身成本并不是特别高，但增加麦克风数量需要配套的增加采样等后续硬件的投入，会大大增加成本。另一方面，麦克风阵列涉及一系列算法，算法设计难度和计算复杂度都会随着麦克风数量的增加而加大。在选择麦克风时，除了指向性、灵敏度、信噪比、频响范围、失真度等常规的

参数要求，其安放位置、开口设计也要考虑 ID 设计和扬声器的位置、功放等，需要全盘考虑。

4、智能语音技术

目前智能音箱应用的智能语音助手的工作流程大致可以分为语音识别（ASR）、自然语言处理（NLP）和文语转换（TTS）三个步骤。智能音箱的智能语音交互系统是实现其智能化的关键技术。

（1）语音识别（Automatic Speech Recognition, ASR）

语音识别的目的是将语音信号转化为文本。语音识别技术相对成熟。目前，基于近场信号的、受控环境（低噪声、低混响）下的标准音语音识别能够达到很的水平。然而在智能音箱开放性的真实环境，语音识别依然是一个不小的挑战，需要接合前端信号处理一起来优化。

（2）自然语言处理（Natural Language Processing, NLP）

自然语言处理（NLP）就是把人的语言形式转化成机器能够理解的、结构化的、完整的语义表示，并回复响应的语言。

只有自然语言理解能够接近人类的理解了，机器的语音交互，才真的能让用户正常对话。NLP 是 AI 领域的最大瓶颈。但结合良好的产品设计，目前还是能够利用现有技术，做出实用的智能音箱产品。

（3）文语转换（Text To Speech，TTS）

TTS 是语音合成应用的一种，在内置芯片的支持之下，通过神经网络的设计，把文字智能地转化为自然语音输出。TTS 技术对文本文件进行实时转换，转换时间之短可以秒计算。TTS 文语转换用途很广，包括电子邮件的阅读、IVR（交互式语音应答系统）系统的语音提示等等，

（四）智能音箱产业链分析

1、产业链概况

目前智能音箱的产业链从上游到下游依次为元器件供应商、语音技术服务商、OEM/ODM 供应商、内容供应商以及终端厂商（如图 1 所示）。产业链上游的元器件供应商与软件服务商为产业链中游的 OEM/ODM 供应商提供基础硬件零部件以及软件系统，OEM/ODM 供应商提供解决方案并生产制造智能音箱，搭载内容服务商的提供的有声资源，通过产业链下游的终端厂商、品牌渠道商将智能音箱提供给消费者。



图 1 智能音箱产业链

2、元器件供应商

从生产制造的角度来看，智能音箱产业链上游包括硬件的芯片、麦克风阵列、基础零部件等供应商。智能音箱的火热，使得包括高通、联发科、英特尔、全志科技等芯片厂商纷纷积极备货并推出新品；楼氏电子、歌尔股份、瑞声科技、ST、BSE、芯奥微、Hosiden、Sanico、博世、敏芯微 MEMS 等麦克风厂商也陆续推出一体化解决方案。目前在芯片环节亚马逊 Echo 主要采用 TI 的芯片以及三星的内存，苹果 Homepod 主要采用自主设计的 A8 芯片，阿里的天猫精灵 X1 采用了联发科的芯片，咕咚音箱和叮咚音箱的芯片主要由北京君正和全志科技提供。

3、软件服务商

智能音箱产业链上的软件服务商主要提供语音技术和操作系统解决方案。在语音技术服务环节，目前主要有科大讯飞、云知声、思必驰等提供技术支持。京东叮咚由科大讯飞提供语音技术支持，天猫精灵、小米小爱音箱（第一代）由思必驰提供全套的语音交互技术。目前国内已经形成较丰富的语音服务商方阵，厂商之间相互对接形成包括语音交互、内容、服务等全套解决方案。因此各家智能音箱的用户体验、使用感受从本质上看，差异不是特别大。

4、OEM/ODM 供应商

传统音响厂商利用在硬件研发上的积淀，从产业布局的角度切入智能音箱产业，如富士康、漫步者、国光、哈曼等。

5、内容供应商

智能音箱的内容与服务的载体，主要搭载音乐、天气、新闻资源等第三方内容。第三方内容供应商占有独特的 IP 资源并开始与众厂商开展合作模式，代表有喜马拉雅、酷我、虾米等。

6、品牌渠道商

目前渠道商主要包括线上（淘宝、京东等电商平台）、线下（商超、门店）、生态链（互联网生态和家电厂商固有资源）和房地产商。京东通过京东智能打造智能生态体系，建立京东 Alpha 智能服务平台，以京东微联为平台接入多种智能硬件产品，最终实现叮咚和京东微联智能家居的打通，目前叮咚拥有 150 多项服务并且拥有自主的开发者平台。阿里巴巴依托电商平台建立相对完善的生态体系，在内容、技术、O2O 服务等方向上都有所布局，但硬件产品较少，硬件实力相对弱。

二、国内外智能音箱产业发展概述

（一）国际智能音箱产业发展现状

1、国际智能音箱产业市场规模

据德勤发布的报告显示，2018 年智能音箱产业共计收入 43 亿美元；预计在 2019 年智能音箱总共将售出 1．64 亿部，

平均售价为 43 美元，收入将增长 63%，智能音箱市场达到 70 亿美元。智能音箱作为价值增长最快的互联设备，正处于快速扩张期。

根据对 Strategy Analytics 发布的公开信息的整理，2016 年和 2017 年智能音箱出货量分别达到了 650 万台和 3220 万台；2018 年前三季度全球智能音箱出货量为 4360 万台，值得一提的是 2018 年第四季度，全球智能音箱出货量增长了 95%，达到 3850 万台，超过了 2017 年的总出货量，并使 2018 年的总出货量达到 8620 万台，预计 2019 年智能音箱出货量将突破 1 亿台。同样 Canalys 预测智能音箱的出货量将达到 1 亿台，到 2020 年，市场将增长一倍以上，达到 2.25 亿台。据 Global Market Insights 称，到 2024 年，全球智能音箱市场的价值可能高达 300 亿美元。

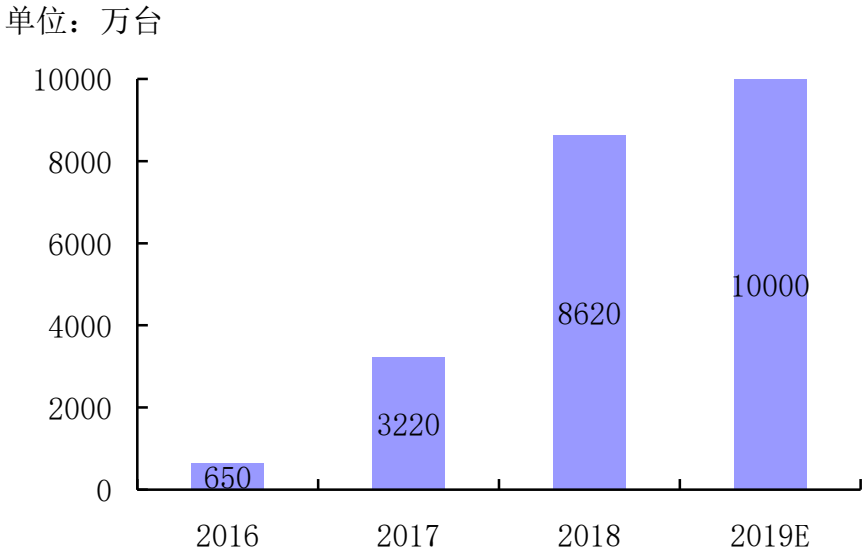


图 2 全球智能音箱出货量统计

通过总结这些预测结果，我们不难得出智能音箱的市场规模将在 2020 年达到百亿美元量级，2025 年有望达到近千亿美元量级。

2、国际智能音箱市场竞争格局

2014 年 11 月亚马逊发布智能音箱 Echo，并于 2015 年正式发售，当年销量为 250 万台，2016 年销量 520 万台，在细分的智能音箱市场占据了 99%的市场份额，谷歌随即快速反应，在 2016 年推出了多种外观设计、多种价位的产品，打破亚马逊的垄断局面，一度占据 20%的市场份额。巨头企业亚马逊、谷歌的先发优势和大规模投入，是美国保持领先地位的主因。另外，在关于噪声抑制、混响去除等最为基础、关键的技术方面，亚马逊的多麦克阵列和谷歌的双麦克阵列也具有先发和领先优势。美国是智能音箱起步最早的国家，也是全球最大的智能音箱市场，占全球过半的市场份额。随后其他国家与品牌陆续加入，近两年中国智能音箱市场增长迅猛，目前已成为全球第二大智能音箱市场，仅次于美国。

根据美国科技市场研究公司 Strategy Analytics 发布的《2018 年第三季度全球智能音箱市场报告》显示，2018 年第三季度全球智能音箱出货量为 2270 万台，同比增长 197%。其中，排名第一的亚马逊 Echo 出货量为 720 万台，市场份额为 32.3%；谷歌出货量为 520 万台，市场占有率高达 22.7%；阿里巴巴、小米和百度也瓜分了不少市场份额，出货量分别

为 220 万台、200 万台和 190 万台。由此可见，目前全球的智能音箱市场由几大巨头型的企业领跑，占据主要大部分市场。

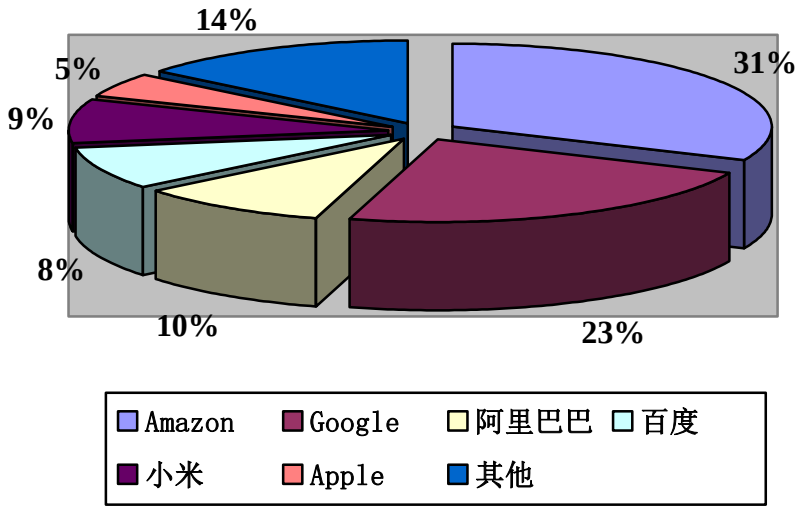


图 3　2018 年第三季度全球智能音箱市场份额（数据来源：Strategy Analytics，中国电子科技集团公司第三研究所整理）

2019 年将继续延续巨头企业瓜分绝大部分市场的态势。预计亚马逊 Echo 将占美国智能音箱市场 63.3%的份额，而 Google Home 将占 31.0%。规模较小的品牌，如 Sonos One 和 Apple HomePod 也将占有一席之地。随着谷歌的不断赶超和更多的品牌进入市场，亚马逊的份额会继续下降。

（二）中国智能音箱产业发展现状

1、中国智能音箱产业市场规模

2016 年，中国智能音箱的销售量仅为 6 万台，而在 2017 年，得益于科技巨头的大规模投入，智能音箱产业开始爆发，销售量突破 150 万台，达到 165 万台，同比增长 2650%，市

场规模达到 4.9 亿元。据奥维云网全渠道推总数据显示，2018 年，中国智能音箱市场零售量为 1625 万台，同比增长 823%，零售额为 36.5 亿元，同比增长 645%，高速增长使得中国已成为全球第二大智能音箱市场。随着各品牌的积极竞争，2019 年中国智能音箱市场仍将保持快速增长。据 Canalys 预测，2019 年中国智能音箱市场出货量将增长至 2960 万台，市场规模将破百亿元。

2、中国智能音箱市场竞争格局

中国智能音箱市场以本土互联网巨头品牌为主，但格局未定、竞争激烈。2016 年，“叮咚”、“飞利浦”、“JBL”等瓜分了全部智能音箱市场。但 2017 智能音箱行业格局大变，小米 AI 音箱和“天猫精灵”强烈冲击市场。2018 年百度、腾讯、华为等互联网巨头也开始布局智能音箱产业，小度、听听等智能音箱登陆市场。以 2018 年 9 月为例，国内智能音箱销量约为 46 万台，天猫精灵以 35%的份额占据 9 月销量冠军，随后则是百度小度的 22%、小米小爱的 20%以及京东叮咚的 20%。

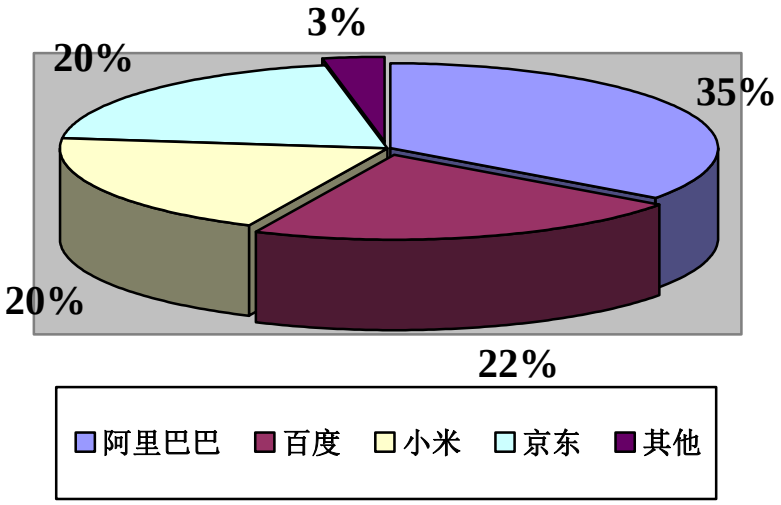


图 4　2018 年 9 月中国智能音箱市场份额（数据来源：Strategy Analytics，中国电子科技集团公司第三研究所整理）

据 Canalys 统计，2018 年第四季度国内智能音箱出货量高达 860 万台，占年度总出货量的 40%。其中，阿里巴巴以 270 万台的出货量领跑市场，占当季出货量的 31%。小米及百度智能音箱产品的出货量都达到了约 250 万台，其中小米以微弱优势排在第二，百度排在第三。百度自 2018 年 3 月进场后，便打破了京东、天猫、小米三足鼎立的局面，成为智能音箱市场最大黑马。

除了互联网巨头以布局生态链的角度切入产业，智能音箱终端企业还包括技术公司、传统音响厂商、内容商以及创业公司几类玩家，分别以扩张产业链或者合作的形式，加入国内智能音箱市场的竞争格局。

表 1 国内智能音箱终端企业参与格局

企业类型	代表厂商	公司特点
互联网巨头	京东、阿里、腾讯、百度、华为	有庞大的业务布局，定位于建立以语音为入口的智能生态，为既有的内容和服务寻找新的入口。
技术公司	科大讯飞、出门问问	在语音技术方面有累积，具有技术优势。
传统音箱厂商	漫步者、JBL、DOSS	在传统印象硬件研发和销售渠道上有累积，倾向于与技术及内容厂商合作。
内容资源商	喜马拉雅、酷狗	在内容上有累积，内容厂家拥有独特的 IP 及内容资源，一般联合技术厂商共同打造音箱载体。
创业公司	Rokid、裴讯	多带有互联网基因，从场景和用户出发，期望打造爆品。

三、智能音箱行业信息安全风险与评价

（一） 智能音箱信息安全风险问题分析

相较于传统音箱，智能音箱集成了人工智能交互处理功能，能够通过语音识别、语义理解、关键词唤醒等技术完成和用户之间的交互，并自主获取来源于互联网的内容播放。然而，正是由于其智能交互功能的获取性与开放性，使得病

毒攻击、数据泄露、漏洞频发成为智能音箱设备的信息安全隐患。

2017 年 12 月，美国消费者保护组织 Consumer Watchdog 出具的一份报告显示，亚马逊、谷歌等 AI 智能音箱存在“偷听”用户的可能，指控此类智能音箱设备违反了相关隐私法案。此外，包括智能音箱在内的智能家居终端，安全性薄弱、利用成本低，首当其冲成为病毒攻击的目标；加之智能设备的弱口令、明文传输、过多权限索取等，造成用户隐私泄露；更有智能家居设备漏洞频发，漏洞影响范围大且修复困难的问题，成为智能产品信息安全的痛点。

（二） 智能音箱信息安全评测体系介绍

为切实可靠的针对智能音箱信息安全性能展开分析，我们依据国内相关标准以及参照信息安全领域国内国外安全架构广泛认同的安全性指标研究制定了智能音箱信息安全评测规范。依照规范，智能音箱设备的信息安全性从设备终端、网络通信、移动设备应用程序、云端四个方面的安全性来进行评测。

1、设备终端安全性

设备终端安全性是指在硬件和固件使用环节存在的信息安全隐患。在对设备终端的评测过程中，选取了固件获取方式、固件系统安全配置、固件升级方式、固件系统对外服务等测试项目。

固件系统可以通过网络、硬件等多种方式获取，安全风险在于固件被获取的可能性大小，所以当固件无法被获取时最为安全。

固件系统安全配置风险在于系统安全配置是否开启，是否使用 SELinux 或者 AppArmor。其中，使用全局安全配置，整体安全性最高。

固件升级可以通过后台自行从官网下载升级或是通过用户点击手动升级等方式，其风险存在于固件升级过程是否会被中间人劫持，故以自动强制升级最为安全。

固件系统对外服务指如 http server 服务、ftp 服务等，风险点在于固件对外的服务是否存在缺陷。原则上无法对外服务最为安全。

2、网络通信安全性

网络通信安全性是指在设备终端和其他端（如云端、手机端）的通信环节存在的信息安全隐患。在对网络通信的评测过程中，选取了通信协议的安全性与通信加密方式作为评测项目。

通信协议的安全性是指是否使用容易被攻击的协议，如 http 协议、UPnP 等通信协议，通信加密方式是指通信过程是否使用加密手段。网络通信的风险在于数据是否会被中间人获取或者篡改。

3、移动设备应用程序安全性

移动设备应用程序的安全性是指在安卓或者IOS系统上的应用程序使用环节存在的信息安全隐患。在对移动设备应用程序的评测过程中，选取了应用程序安全配置、应用程序代码安全规范、非通用安全风险作为安全指标。

应用程序安全配置是指安装时的权限设置，如是否可以调用非必须权限，其安全风险在于应用程序的隐私数据是否会被泄露。

应用程序代码安全规范是指应用程序的代码编写是否符合规范要求，如是否调用易导致漏洞的函数。未按照规范编写的应用程序通信数据，或可被中间人获取或者篡改将存在安全风险。

非通用安全风险指如登录等与逻辑相关联的漏洞，风险在于开发环境的后台信息是否会被泄露。

除此之外，我们依据 GB/T 22239-2008《信息安全技术 信息系统安全等级保护基本要求》对身份鉴别、通信安全做出了评测。

身份鉴别是指应用是否对用户名进行唯一性检查、鉴限制非法登录次数等登录失败处理功能。

通信安全是指是否可以保证通信过程中的完整性和敏感信息的保密性。

依据 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》对数据安全、安装及

卸载安全、运行安全做出了评测。

数据安全要求应用中敏感数据不应以明文形式存储。

安装及卸载安全是指检查软件安装时是否包含签名信息、是否提示使用的资源和数据、不影响终端系统及其他应用软件安全、卸载时是否可以清除安装过程中产生的资源文件、配置文件和用户数据。

运行安全测试包括：身份鉴别机制、APP 权限是否为最小权限、默认组件安全、反编译、抗二次打包、敏感信息清除、抗动态调试、数据存储安全。

4、云端安全性

云端的安全性是指在后台信息服务和管控提供服务的环节中存在的信息安全隐患。在对云端的评测过程中，选取了信息搜集与网站渗透两方面作为安全评测指标。安全风险主要在于服务器端通信数据泄露、服务器数据库泄露、服务器控制权限被远程窃取、服务器网站程序被恶意登录等问题。

信息搜集风险意味着可公开查询信息越少越安全。端口就是云服务器上可访问的端口，一般云端对外部暴露的端口数量越少越好

另一个风险因素是 HTTP server 版本问题，版本越低越不安全，反之最新版本则最安全。

第三个因素是 TLS 版本问题。由于 http 是明文，所以采

用 TLS 防止他人获取中间信息，与 HTTP server 相同，版本越低风险则越高。

第四个因素是中间件使用信息，一般使用的中间件数量越多会有更多安全风险。

（三） 智能音箱信息安全评测结果分析

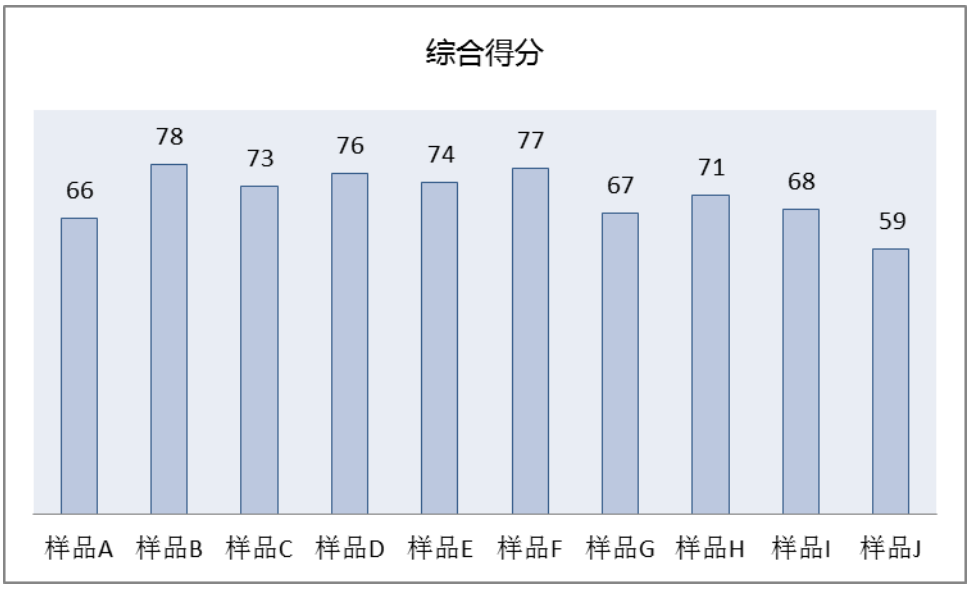
为切实可靠的反映目前市场上智能音箱产品的信息安全性能水平，我们选取了国内外知名厂商的十款最新智能音箱产品进行评测。其中包括了苹果、亚马逊、华为、百度、小米等品牌，覆盖了国内外智能产品巨头和新兴互联网企业。产品清单如下所示：

表 2 测试样品信息

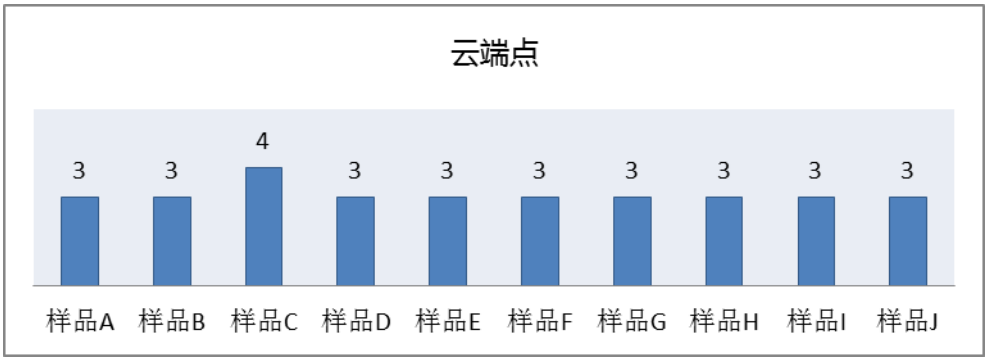
音箱型号	固件版本	APP 版本
阿里-天猫精灵方糖	1.10.4-S-20180928.1315	3.8.1
苹果-HomePod	无	无
华为-AI 智能音箱	9.0.1.8（H100SP9C00）	9.0.3.315
百度-小度智能音箱	1.1.0.201811101655	3.3
亚马逊-Echo1	618622220	2.2.250163.0
亚马逊-Echo2	592452720	2.2.250163.0
小米-AI 音箱	1.26.53	2.0.7
腾讯-听听音箱 T1	无	3.5.0.34
京东-叮咚 mini2 智能音箱	无	3.5.8.805
喜马拉雅-小雅 AI	1.3.47	1.8.23

评测从设备终端（硬件和固件）、网络通信、移动应用程序、云端四个层面开展安全测试，共 30 个测试项目，覆盖了更新、数据通信、配置规范、代码规范等产品体系中的多个脆弱环节。评测过程采用信息安全领域国内国外安全架构广泛认同的安全性指标。

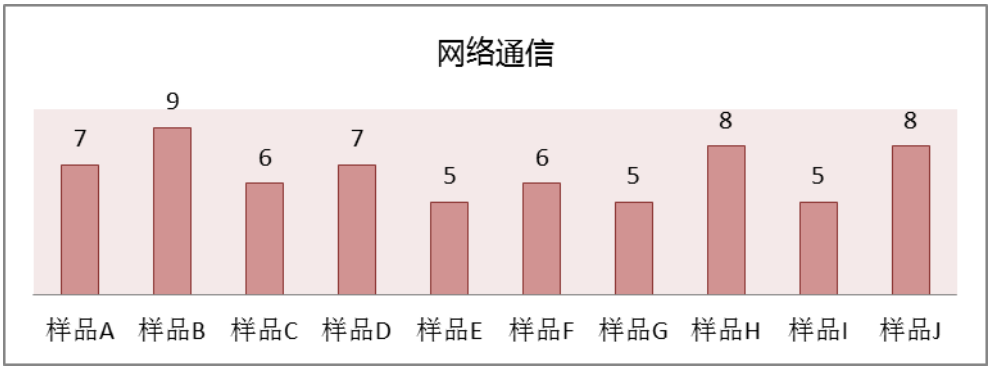
单项评分中的分值表示减分，扣分越多，表示安全性越差。最终得分以百分制显示，分数越高，则表示安全性越好。然后再根据各个产品在每一项安全指标的情况乘以对应安全指标的权重，最后求和得出最终分数。



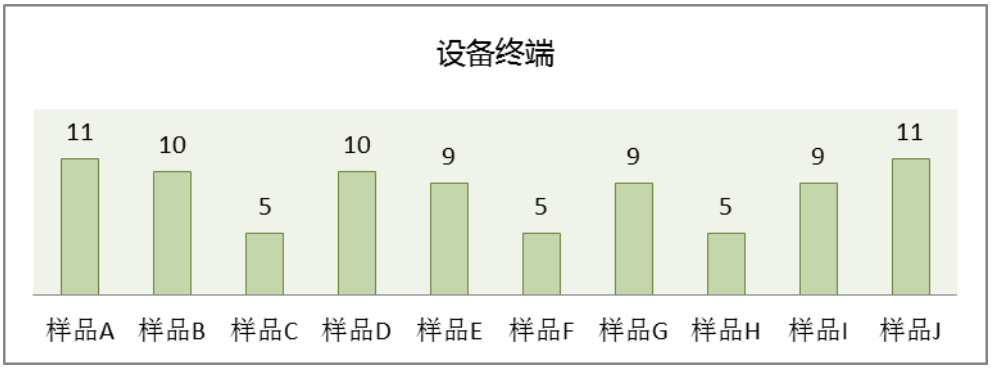
由上图综合得分可见，十款样品的整体信息安全情况一般，存在不同程度的风险机会，个别样品风险机会犹大，需要相关研发企业提高信息安全风险防范意识，加大产品信息安全相关研发投入，提高信息安全保障能力。



由上图可见，10 款产品在云端点信息搜集风险水平较为一致，需要特别说明的是，由于未取得被测方的授权，云端服务器渗透测试项目无法进行测试，故此项目数据默认无分数扣减。

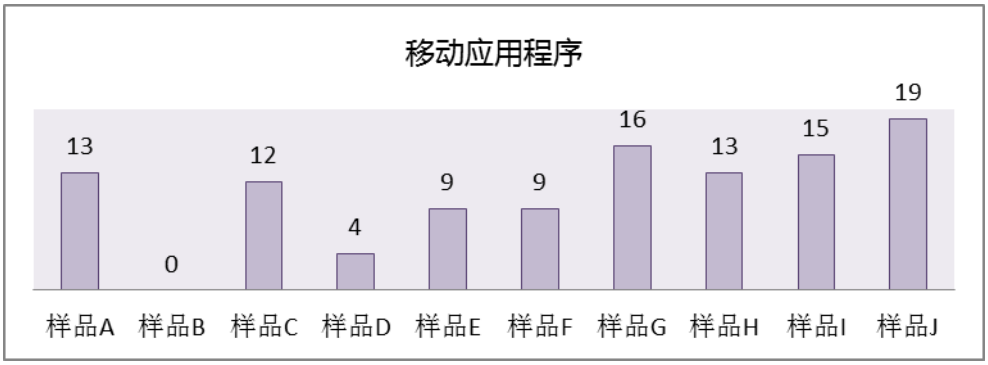


网络通信方面，均存在 http 方式传输数据，并采用部分明文通信，但都是非敏感数据，因此属于低危。其中，样品 I 智能音箱安全水平较高，另有 4 款产品使用了较低版本的 NTP 服务提高了风险机会。



设备终端方面，整体安全水平不足。除一款样品外，其

余 9 款产品都可以被通过物理方式获取到固件；除样品 C 与样品 H 外，其他 8 款产品均未进行固件加密。



在移动应用程序方面，由于样品 B 的应用程序为 iOS 系统的内置程序，无法导出测试，故而只对其余 9 款产品进行了测试。整体风险低，但 9 款产品都存在不符合安全规范的情况，样品 G 与样品 J 相对风险较高。

具体测试数据如附表一。

四、智能音箱信息安全发展趋势与建议

（一） 我国信息安全发展趋势分析

1、信息安全投入有望提高，行业还将保持快速增长

从所有互联网终端设备来看，我国企业信息安全投入不足，经济损失位居全球第一。2017 年，大约 3.52 亿的中国消费者曾成为网络犯罪的受害者,经济损失达到 663 亿美元，过去 4 年复合增长 15.7%。持续增长的网络威胁促进我国信息安全产品的快速发展。2016 年，中国的网络信息安全市场达到 336.2 亿元，同比增长 21.5%，高于全球增长率 12.05%。随着国家战略的逐步落地，我国信息安全投入比例将逐渐向成熟市场看齐，且相关政策的持续推动，国内信息安全市场

前景可观。预计 2019 年国内网络信息安全市场将持续高速增长，增长率约可保持在 20%以上。

2、市场布局转换，安全服务市场加速

目前我国信息安全市场仍是以硬件为主，占比 51.3%，其次是安全软件和安全服务分别占 37.5%和 11.2%，其中安全服务中安全集成和安全咨询占 90%的市场份额。随着我国信息产业和网络技术的发展，传统的网络信息安全产品难以满足日益变化的复杂的网络空间，我国的信息安全产品行业必将向国际看齐，由硬件为主转换为以服务为主，安全服务是长期发展方向。新形势下，产品和服务的联动更加紧密，安全服务逐渐从配合产品的辅助角色，转变成为安全产品发挥最佳效用的必要条件。

（二） 智能音箱信息安全发展建议

1、以监管为核心，打通新型智能终端产业链

由于智能音箱终端产品的应用广泛性、需求多样性、功能复杂性，需要政府加大投入监管力度。智能音箱作为家庭伴读的重要工具和智能家居的控制窗口，不仅需要从产品质量、信息安全等方面加强监管，还需要约束智能音箱自动提取的信息所涉及的基本伦理道德法律内容，从多方面、多维度监管，制定相关法规、政策，为使用者提供一个积极、健康、安全的环境。

此外，还应加强政府与企业、企业与市场、企业上下游

的协作，打通新型智能终端产业链。在助力优质企业成长的同时，打击黑色产业链，大幅度降低安全事件的发生概率，发展新型智能终端良性生态系统，构建网络空间命运共同体。

2、加强信息安全核心技术研发

随着智能音箱产业链条逐渐复杂，信息安全需要整个行业来维护，共建安全生态。建立以终端厂商、安全厂商、高校专家和科研机构为主体，产学研用相结合的技术攻关体系，推动核心安全技术真正落地，保障用户在智能时代的人身安全、数据安全与隐私安全。

具体来说，加强智能音箱产业信息安全核心技术应重点发展包括对终端设备硬件部分设计安全接口，加强固件加密能力，加强设备通信的加密能力，减少云端公共信息，减少云端对外暴露的风险点，加强移动设备应用程序的隐私保护能力。

3、积极制定信息安全标准规范，完善评价体系

目前市场上智能音箱产品种类众多。企业硬件平台参差不齐，软件厂商维护成本高，垂直行业多样且复杂，使得市场碎片化现象严重，产品信息安全水平更是良莠不齐。

智能音箱终端安全标准是提升行业安全水准的重要技术依据，要根据技术发展和应用情况及时制定完善的终端安全标准，明确其在保护用户数据、保障业务安全方面的技术

要求，引导产品研发和产业发展。结合智能音箱自身特点，定制安全技术框架与具体要求、管理指南以及测试方法和流程，明确各标准之间的相互关系，形成标准架构体系。

在制定技术标准和管理规定时，应从需求出发，定义不同的防护强度。针对智能音箱终端在隐私信息保护、访问控制等方面面临的风险开展研究，细化数据安全保护级别，按照重要性和敏感程度分级分类，重视各种用户信息的安全性和隐私性，制定完善多角度多层次的新型智能终端安全标准。技术标准和管理规定也应考虑到对产品生命周期的全覆盖。包括针对产品设计阶段的安全需求分析指南，贯穿开发实施和运营阶段的技术要求、接口规范等，测试阶段的检测标准和具体操作流程，以及运营和反馈阶段的安全事件响应及恢复流程。这些标准互相配合，既保持标准的一致性，又各有重点，可以灵活实施。

4、搭建技术测试平台和威胁情报平台

构造公平、完备、有效的技术验证服务体系和规模化测试环境，是贯彻标准执行的有效措施。可以适当形成评级方法，定义指标，将各种强度的安全防护能力量化呈现。并公示评测结果，为行业自律提供依据。

同时，将监测与检测联动，打造新型智能终端威胁情报平台，提供第一时间信息分享，控制安全事件的波及面。威胁情报包括僵尸网络地址、0day 漏洞、恶意 URL 地址等各

类信息。通过众测平台和厂家协作等渠道，广泛捕捉威胁情报，缩短信息系统发现威胁的时间并迅速响应，保证“防护时间> 检测时间+响应时间”，从而实现对威胁的快速遏制，构建安全互联生态系统。

5、发挥协会和龙头企业作用，指引发展方向

增加企业话语权，发挥龙头企业带头作用。在安全方面，国有企业的国际话语权尤为重要，直接关系到国家安全的保障。要加强我国在信息领域中的国际话语权，参与网络安全国际规则的制定，才能在更高的层面保障国家安全。一些国内的互联网公司既涉足新型智能终端的研发和生产，又对安全有深入研究，同时还具备一定的国际影响力。以这样的企业为代表，牵头参与国际安全规则的制定，有利于被国际市场所接纳。

支持协会推广，打破行业壁垒，优化产业结构。避免各自为政、重复安全标准建设、安全技术和检测碎片化。

附表一：

设备危险类别	风险规则	评分规则	样品 A	样品 B	样品 C	样品 D	样品 E	样品 F	样品 G	样品 H	样品 I	样品 J
云端点（40分）	1.信息搜集（4分）	1.端口（1分）	1	1	1	1	1	1	1	1	1	1
		2.HttpServer 类型版本（1分）	1	1	1	1	1	1	1	1	1	1
		3.TLS 版本（1分）	0	0	1	0	0	0	0	0	0	0
		4.中间件信息（1分）	1	1	1	1	1	1	1	1	1	1
	2.网站渗透（未授权）	1.heartbleed 漏洞（3分	/	/	/	/	/	/	/	/	/	/
		2.sql 注入（5分）	/	/	/	/	/	/	/	/	/	/
		3.xss（3分）	/	/	/	/	/	/	/	/	/	/
		4.csrf（3分）	/	/	/	/	/	/	/	/	/	/
		5.ssrf（2分）	/	/	/	/	/	/	/	/	/	/
		6.文件上传（5分）	/	/	/	/	/	/	/	/	/	/

		7.源码下载（5 分	/	/	/	/	/	/	/	/	/	/	/
		8.弱口令（5 分）	/	/	/	/	/	/	/	/	/	/	/
		9.敏感目录泄露（5 分）	/	/	/	/	/	/	/	/	/	/	/
网络通信（16 分）设备和云端之间的交互的安全性，还有设备到手机端	脆弱协议（4）通信协议是否有协议，https 等就比较安全，高版本的 ntpv3	1.使用非标准自定义协议通信（1 分）	0	1	0	0	0	0	0	0	0	0	0
		2.使用 UPnP 通信（1 分）	0	1	0	0	0	0	0	0	0	0	0
		3.使用 HTTP 通信（1 分）	1	1	1	1	1	1	1	1	1	1	1
		4.使用版本 3 或更低版本的 NTPv3（1 分）	0	0	1	0	0	1	0	1	0	1	1
	网络加密（12 分）通信过程是否内容加密	1.设备到云完全使用明文通信（4 分），部分明文通信（2 分），无明文通信（0 分）	2	2	2	2	2	2	2	2	2	2	2
		2.移动应用程序到云完全使用明文通信（4 分），部分明文通信（2 分），无明文通信（0 分）	2	2	2	2	2	2	2	2	2	2	2

		3.移动应用程序到设备完全使用明文通信（4 分），部分明文通信（2 分），无明文通信（0 分）	2	2	0	2	0	0	0	2	0	2
设备终端（硬件 -- 外壳和电路板 & 固件 -- 软件）（ 20 分）	固件获取方式（9 分）因为对固件进行分析，需要各种途径获取固件。如果获取不到才是最安全的	通过互联网获取(官网获取--提供下载、升级 IP 获取...)（2 分如果通信加密，就无法获取	2	2	0	0	0	0	0	0	2	0
		物理串口获取（2 分）	0	0	0	0	2	0	0	0	0	2
		可通过物理芯片读取（2 分）	2	0	2	2	2	2	2	2	2	2
		固件未加密（3 分	3	3	0	3	3	3	3	0	3	3
	固件系统安全配置（4 分）操作系统	未使用 SELinux 或者 AppArmor（4 分）	2	2	2	2	2	0	2	2	2	2
	固件升级方式（3 分）（自动强制升级最安全）	手动升级（2 分）	2	0	0	2	0	0	0	0	0	0
		官方未推送升级包（1 分）	0	0	0	0	0	0	0	1	0	0
	固件系统对外服务（4 分）（无对外服务最安全）	每项服务 1 分（4 分）	0	3	1	1	0	0	2	0	0	2

移动应用程序（ 24 分）	配置规范（3 分）	webview 组件存在忽略证书校验错误的情况（1.5 分）	1	homepoad 的应用程序为 iOS 系统的内置程序，无法导出测试，但整体风险低	1	1	1	1	1	1	1	0
		webview 组件存在未注册 Java 类函数（1 分）	0		0	0	0	0	1	0	0	0
		HTTPS 未校验服务器证书（2 分）	1		1	0	0	0	0	0	1	0
	代码规范（8 分）	apk 未对组件调用者进行校验（1.5 分）	0		0	0	0	0	1.5	1.5	0	1.5
		敏感函数调用（1 分）	1		0	0	1	1	0	0	1	1
		内网段测试信息残留（1 分）	0		0	0	0	0	0	0	0	0
		敏感的调试日志（1.5 分）	0		0	0	0	0	0	0	0	0
		webview 组件存在忽略证书校验错误的情况（1.5 分）	1		1	0	1	1	1	1	1	1
		webview 组件存在未注册 Java 类函数（1 分）	0		0	0	0	0	0	0	1	0
	安全风险（1 分）	HTTPS 未校验服务器证书（2 分）	0		1.5	0	1.5	1.5	1.5	1.5	1.5	1.5

	身份鉴别（2 分）	用户标识唯一性	0		0	0	0	0	1	0	0	1
		登录失败处理功能										
	通信安全（2 分）	通信保密性	0		0	0	0	0	0	0	0	2
		通信完整性										
	数据安全（2 分）	加密传输	1		0	0	0	0	0	0	0	1
		加密存储										
	安装及卸载安全（1 分）	安装	0		0	0	0	0	0	0	0	0
		卸载										
	运行安全（5 分）	默认组件安全	5		4	3	1	1	4	4	3	5
		反编译										
		抗二次打包										
		抗动态调试										
		敏感信息清除										
		数据存储安全										
智能设备综合得分			**69**	**78**	**76.5**	**76**	**77.5**	**80.5**	**72**	**75**	**73.5**	**64**