

CAICT 中国信通院

**互联网设备
智能音箱安全白皮书
(2019 年)**

中国泰尔实验室
电信终端产业协会
2019年12月

版权声明

本白皮书版权属于中国信息通信研究院中国泰尔实验室，并受法律保护。转载、摘编或利用其它方式使用本白皮书文字或者观点的，应注明“来源：中国泰尔实验室”。违反上述声明者，本实验室将追究其相关法律责任。

前 言

当前，世界正处于新一轮科技革命和产业革命的变革浪潮中，以智能终端为代表的互联网产业已成为“互联网+”的基础设施，是推动经济社会变革的重要力量。近年来，智能音箱发展迅猛，出货数量出现井喷式增长。智能音箱作为具有智能语音交互系统、互联网服务内容，同时可扩展更多设备和内容接入的互联网终端产品，可为家庭消费者提供随时享受互联网时代的便利。随着产业的蓬勃发展，智能音箱产业未来会进一步走向信息化、智能化。

但与此同时，频繁曝光的智能家居设备入侵、用户隐私数据窃取等事件表明智能音箱生态安全存在一定的安全风险。为研究该风险具体情况和应对措施，中国泰尔实验室通过对主流智能音箱设备抽样检测和分析，制定了《2019年互联网设备-智能音箱安全白皮书》。本白皮书着眼于智能音箱产业新的发展阶段，阐述了智能音箱当前的安全态势和安全风险，基于业界最佳实践，在智能音箱产品网络安全防护和用户个人信息保护等方面提出建议。希望为智能音箱生态各参与方提供参考，并通过各方通力合作，加强行业自律，强化产业协作体系，为用户提供更安全放心的智能音箱服务。

目 录

一、智能音箱产业安全现状.....	1
二、2019 智能音箱安全评测报告.....	6
(一) 智能音箱安全行业标准.....	7
(二) 硬件安全评测.....	8
(三) 操作系统安全评测.....	10
(四) 应用安全评测.....	12
(五) 无线通信安全评测.....	13
(六) 用户个人信息安全评测.....	15
三、2019 智能音箱十大安全风险.....	18
(一) 个人信息收集处理规则模糊，存在过度收集和使用风险.....	18
(二) 个人信息明文传输，存在数据泄露风险.....	19
(三) 个人信息不安全存储，存在未授权访问风险.....	19
(四) 设备硬件调试接口暴露，存在固件及敏感信息提取风险.....	20
(五) 设备系统更新不及时，存在高危漏洞利用风险.....	20
(六) 设备系统更新机制不安全，存在更新包篡改或替换风险.....	20
(七) 设备系统防护不足，存在恶意应用静默安装风险.....	21
(八) 身份认证机制缺陷，存在会话劫持风险.....	21
(九) 移动应用安全防护不足，存在恶意代码植入风险.....	21
(十) 设备漏洞引发跳板攻击，影响互联设备安全.....	21

四、智能音箱用户个人信息保护的分析和建议.....	22
(一) 规范用户个人信息收集使用规则.....	22
(二) 落实用户信息收集使用告知同意原则.....	24
(三) 重点加强音频等用户个人敏感信息全生命周期安全防护.....	25
(四) 明确预置应用用户个人信息收集使用规则及责任归属.....	27
(五) 加强预置应用权限调用可知可控力度.....	28
五、智能音箱网络安全防护的分析和建议.....	28
(一) 设备出厂前关闭（非必要）调试接口且去掉敏感信息.....	28
(二) 采用最新的操作系统及外部代码库.....	29
(三) 对设备系统及应用进行安全加固.....	29
(四) 采用安全存储技术保障敏感信息安全.....	29
(五) 完善身份认证机制保障通信过程安全.....	30
六、智能音箱产业安全防护行动倡议.....	31
(一) 加强音箱行业自律，明确企业主体责任.....	31
(二) 推进标准规范制定，促进行业健康发展.....	31
(三) 依托社会公众监督，加强安全监管力度.....	32
(四) 鼓励各方合作共享，协作提高安全水平.....	32

一、智能音箱产业安全现状

（一）智能音箱设备安全现状

智能音箱设备快速应用发展的同时，其信息安全问题也日益突显，并逐渐成为制约智能音箱设备发展的关键问题之一。智能音箱设备的广泛应用为人们的生活带来了诸多便利，然而，庞大的终端数量、复杂的传输协议、海量的数据传输，也使其面临巨大的信息安全风险。近几年智能音箱安全事件频发，新型攻击方式不断涌现，用户个人信息泄露和终端远程恶意操控等风险突显，用户的合法权益受到严重侵害。智能音箱设备安全已经成为关系广大人民群众切身利益的重要问题。

（二）智能音箱安全事件

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。据组织内部人员表示，事件的起因是发现来自亚马逊和谷歌的专利中包含可能被用作收集用户信息和广告推广的设备。该组织经研究宣称，从这两大巨头的专利申请可以看出，这些设备可能被用于收集大量信息和广告推广，并警示：在不远的将来，智能音箱可以监听到用户的一切，从一些机密对话，到主人冲厕所的习惯，无所不包。而智能家居产品的新

版本可能会收集用户数据并向其推销相应产品。该组织研究发现，即使用户认为智能音箱在“休眠”状态，它们也可以被“唤醒”。实际上，这些设备只要开着，就一直都在收听声音。而亚马逊设想用语音助手 Alexa 收集信息，并为房间内所有人设立档案，依此向其推销相应产品。2018 年 8 月，在拉斯维加斯举行的全球黑客大会 DEFCON 上，技术人员展示了全世界畅销的智能音箱——亚马逊智能音箱 AmazonEcho 被破解的全过程，全程仅需 26 秒。通过控制智能音箱，不仅能够远程控制进行录音，还能够发送录音文件。亚马逊智能音箱在美国市场占有率达到 70%，由于市场的普及性，亚马逊为这款智能设备设置了高安全系数。显然，一直处在安全研究人员的“高难度黑名单”上的亚马逊智能设备也难以阻挡住黑客的破解。2019 年 11 月，网络安全研究员 Takeshi Suguwara、Fu 和一组密歇根大学的研究人员一起将正弦波的形式随时间改变激光强度的光声现象变成了某种更令人不安的事情。他们可以使用激光以静默方式向任何接收语音命令的计算机“说话”，包括智能手机、Amazon Echo 音箱、Google Homes 和 Facebook 的 Portal 视频聊天设备。这种类似间谍的技巧使他们可以从数百英尺远的地方发送“轻指令”。他们可以打开车库，在线购买商品，或者做出各种恶作剧或恶意行为。当设备的所有者不在家里时，攻击者可以轻松地通过窗户，让目标设备进行响应。

国内有专家表示，智能家居设备通过终端收集相应语音数据，并传输到服务器，供语音 AI 程序分析使用。智能音箱会收集用户说话，这涉及到语音识别和指令执行。从隐私保护角度来看，应该避免服务端收集的数据逆推到具体个人。也就是说，服务器收集了很多语音片段，人工智能程序会分析处理这些语音，识别语音中的内容，并根据用户需要的结果反馈给音箱。但如果从智能设备逆推回去，能够确定用户身份及个人信息，就会存在很大隐私风险。

由此可见，无论攻击者从何种角度攻击，目的无非两种，一是远程控制音箱，以音箱为翘板实现对所关联设备的控制；二是窃取用户隐私，无论是窃听用户生活日常、窃取用户录音，还是收集用户信息和日常生活习惯，皆可将收集信息作于不法用途。

1) 远程控制

攻击者通过对音箱系统进行分析，利用其薄弱环节，对其进行攻击以达到远程控制目的，例如通过破解音箱系统升级流程，下发恶意代码以控制音箱，流程如图 1 所示。

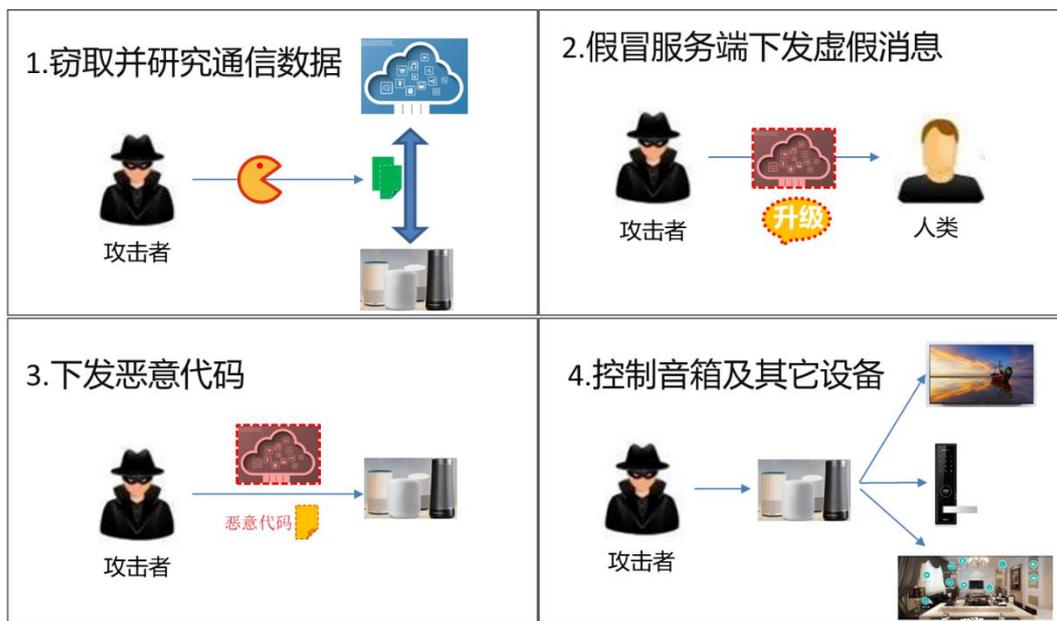
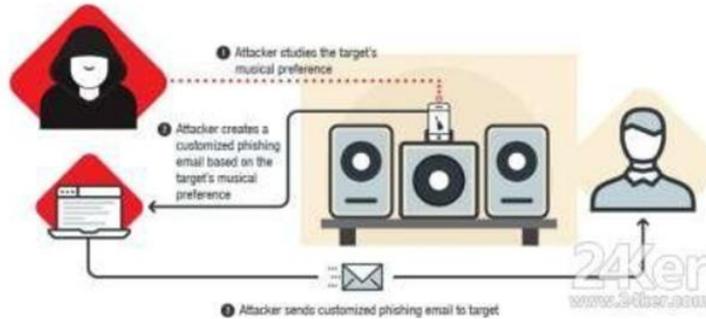


图 1 远程控制流程

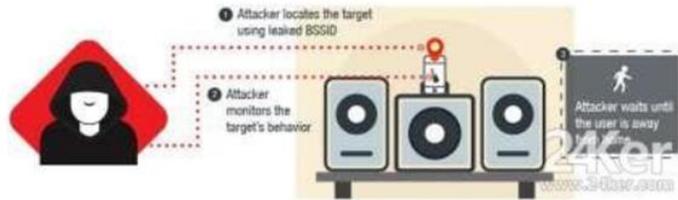
2) 泄漏用户身份数据

用户隐私泄露已成为智能音箱安全的痛点，例如利用 BSSID 请求获取 AP 的大致位置，可以被黑客用来发起精确攻击，例如利用 URI 通道远程控制音箱播放指定音乐，如图 2 所示。

一、黑客研究目标对象音乐喜好，撰写并投放成功率更高的钓鱼邮件。



二、黑客通过泄露的BSSID锁定目标的物理位置，进而监控（窃听）目标行为，等目标离开家门后进入房间作案。



三、黑客通过音箱播放虚假的消息推送提醒，诱使目标打开包含恶意软件的邮件或信息。

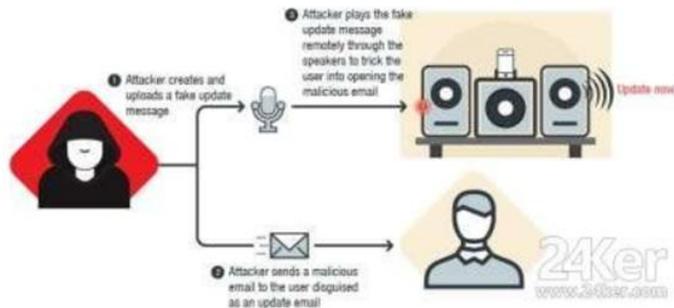


图 2 隐私泄漏

（三）智能音箱安全威胁发展趋势

根据智能音箱终端应用的固有特征，目前针对音箱系统的攻击已呈现出几大的威胁趋势：

首先，针对数据的攻击逐渐趋多，两个方面：首先是隐私泄露问题，另一方面是数据污染问题，由于故意的或偶然的行為造成的对原始数据的完整性和真实性的损害，进而影响最终的决策过程。

其次，拒绝服务攻击频次和破坏性更大，由于弱口令等原因，智能音箱设备僵尸网络正成为令人难以置信的高容量 DDoS 攻击源。大规模的攻击已经不再需要利用反弹/放大技术。它们只需依靠设备的数量即可，伴随而来的是攻击的规模、频度、复杂性和带来的影响、损失都在日益快速增长，在僵尸大军面前所有被盯上的机构都难以抵抗。

再次，音箱终端还容易遭受劫持攻击，勒索所劫持设备，正成为黑客钟爱的新型攻击手段。设备与现实世界紧密连接，攻击效果对黑客的吸引力更大。

另外，音箱终端还易沦为攻击的跳板。入侵单一设备或许不能造成太大安全威胁，但通过设备进入其他目标系统情况就大不相同。过去网络连接方式单一，存在的网络攻击面有限。网络“融合”导致能够被攻击的脆弱点激增，设备间的“跨越式”攻击变得容易。

二、2019 智能音箱安全评测报告

中国泰尔实验室依据 TAF 标准《智能音箱产品安全能力技术要求 and 测试方法》（征求意见稿），按照行业销售量排名，此次对 11

个品牌的智能音箱产品进行安全抽测。

（一）智能音箱安全行业标准

1. 标准编制情况

为规范智能音箱设备的安全防护能力，通过提高智能音箱自身的安全防护水平，防范各类安全威胁。由中国信息通信研究院牵头，联合北京百度网讯科技有限公司、北京奇虎科技有限公司、北京小米移动软件有限公司和北京京东世纪贸易有限公司制定了TAF协会WG4组协会标准《智能音箱产品安全能力技术要求和测试方法》（征求意见稿），该标准旨在为智能音箱采购者、生产厂商、评估机构提供一个多方认可的、通用的安全要求，产品厂商可参考本标准进行设计、开发。

2. 标准内容

标准的基本内容包括安全能力框架、安全能力技术要求、安全能力分级和安全测试方法。安全能力框架主要包括：根据智能音箱可能面临的安全风险，提出安全功能架构，包括硬件安全、操作系统安全、AI模型安全、应用能力安全、扩展能力安全和用户隐私保护等。安全能力技术要求从基本功能（声音采集、语音唤醒、内容满足、网络接入）、扩展功能（如支付功能、家居控制功能）、操作系统及硬件等方面对智能音箱终端应具备的安全能力提出要求。安全能力分级是基

于基本的安全保障、实现难度、特殊安全能力等层面对智能电视音箱能力进行分级，以便于产品具有特定品质，便于消费者选择。安全测试方法中提供针对智能音箱的测试方法，测试方法与安全要求中所描述的智能音箱安全能力具有对应性。

(二) 硬件安全评测

1. 评测内容

由于安全性设计考虑不足，大部分终端硬件均保留测试接口或其他可利用接口信息。导致可直接基于硬件获取其超级权限。并且由于成本原因，无法嵌入具有安全性能的 MCU 或安全芯片，只能选用不具备安全防护芯片，使得关键信息或敏感数据极易被获取。

因此本次主要对主板和物理接口进行分析，发现其可能存在调试入口及未加密存储数据。

2. 评测结论

对抽取产品进行硬件测试，测试发现 70% 的被测产品主板存留敏感丝印信息以及暴露 Test PIN。例如 JTAG、SWID、UART 等硬件接口用于设计时的前期调试，程序烧录，以及诊断测试。我们发现 70% 的设备的硬件上都保留了调试接口，攻击者通过这些接口获取到大量实现上的细节信息。

测试发现 90% 的产品硬件存储芯片采用没有加密功能的芯片，

可基于不同的方式提取其中的关键信息。

3. 典型问题

基于调试接口获取固件信息：智能设备在出厂后为了方便业务侧进行远程设备调试，多数设备不会移除调试串口或关闭调试端口。在实际的检测中发现很多设备都存在此类漏洞：例如某款智能音箱同时存在未移除调试串口和调试端口未关闭的情况，如图 3 所示。

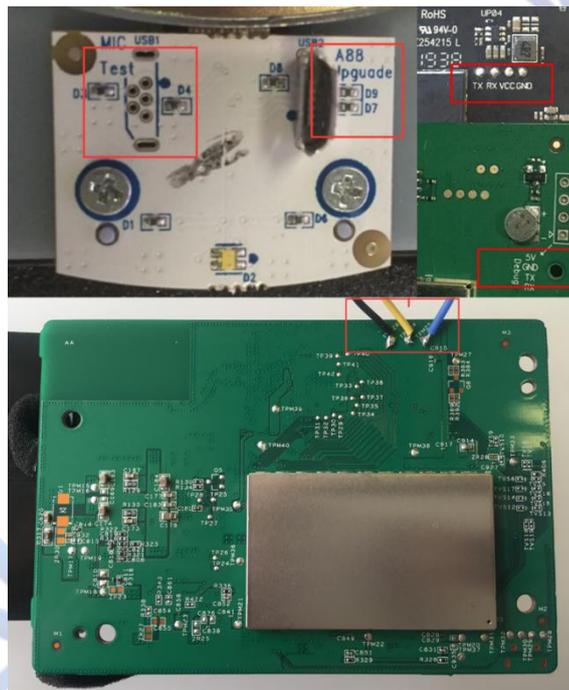


图 3 调试接口暴露

基于暴露接口，通过物理接触获取 shell，然后提权获取 ROOT。如图 4 所示。

```
[00:00:19.194] SpotifyUserCmd return err = 0
[00:00:19.847] on_online_status: old[21] new[11] last_status[-1]
[00:00:20.371] >> binder uin[1481931789], nick_name[克]
[00:00:20.371] on_binder_list_change: error = 0, nCount = , ota_force = 1
[00:00:20.372] on_binder_list_change: tx_query_ota_update_ex 8888
[00:00:20.426] NTPDATE sync successful with tag 0

[00:00:20.426] <<<<<TIME_BASE>>>>>> SNTP===== 2019-11-27 08:27:41 =====
[00:00:20.426] A0lcontroller rcv_buf NTPSyncOffset:1574843244 ++++++
[00:00:20.426] A0lcontroller rcv_buf -----
[00:00:20.427] MW_I0GUARD rcv:GNOTIFY-SETNEXTALARM:-1 +++
[00:00:20.427] MW_I0GUARD rcv:---
[00:00:20.824] !!!!!!!!!!!!!!!-----on_login_complete | code[0]
[00:00:21.803] on_online_status: old[21] new[11] last_status[11]
[00:00:21.879] Snd_Ctrl 1 to volume 100
[00:00:21.229] Snd_Ctrl 1 to mute 1
WMUtil_check_Mute_PA 2668
WMUtil_check_Mute_PA mute flag changed!0 to:1
[00:00:21.232] UART real_write
AXXS1
AXX+MUT+001
is_alib_0a820fa88(0x1eb)
HARMANDSPLIB alsalib Deallocate success
pid= 0x000001eb, before release mFileWatchThread = 0xb608d450
pid= 0x000001eb, quit from file watch
pid= 0x000001eb, after release mFileWatchThread = 0x00000000
stopFileWatch success
dsp release success
[00:00:21.557] smplayer -----
[00:00:21.560] Guard rcv_buf AlexaLoginSuccess+++++
[00:00:21.915] UART real_write AXX+VIS+IDL

# whoami
root
```

图 4 ROOT 权限获取

(三) 操作系统安全评测

1. 评测内容

终端软件包含或其系统以及系统安装应用，由于自身问题，或者由于缺乏相应的更新机制导致其存在大量漏洞，攻击者可以利用终端或节点的漏洞进行木马、病毒的攻击，导致终端节点被非法控制或不可用。同时，物联网 API 接口开放性、逻辑多样性，使得流程实现没有考虑全部可能的情况，尤其异常情况，导致攻击者可以绕过或篡改业务流程，比如绕过认证环节远程对设备进行控制。

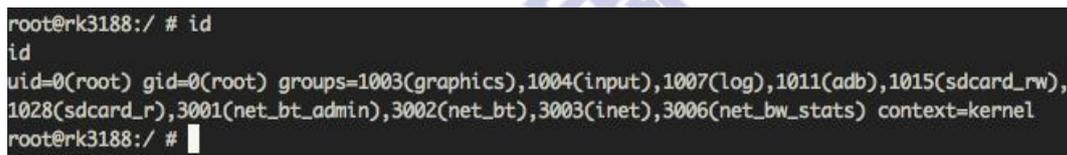
本次操作系统安全测评利用固件逆向和自动化分析工具，对固件进行逆向分析，发现其密钥存储及业务实现所存在的逻辑漏洞。

2. 评测结论

测试人员对被测产品系统进行漏洞扫描和人工排查发现，部分系统存在大量高危漏洞，且漏洞修复比例较低。一些产品甚至存在未修复高危已知漏洞，攻击者可能利用已知漏洞，提权并对系统进行破坏或窃取用户账户信息等。尤其在固件更新层面，90%以上的固件升级更新机制实现不安全，大量升级操作存在固件不加密，没有对固件进行签名校验等漏洞。

3. 典型问题

系统更新不全，漏洞修复比例低，利用系统漏洞获取Root权限，如图 5 所示：



```
root@rk3188:/ # id
id
uid=0(root) gid=0(root) groups=1003(graphics),1004(input),1007(log),1011(adb),1015(sdcard_rw),
1028(sdcard_r),3001(net_bt_admin),3002(net_bt),3003(inet),3006(net_bw_stats) context=kernel
root@rk3188:/ #
```

图 5 系统漏洞利用

被测某款产品关键性程序和脚本未进行混淆和加固，通过逆向发现了远程代码执行漏洞，流程如下：

- 通过按静音按钮和复位按钮 2 到 3 秒进入工程模式（实现在内核里）。
- 设备将启动一个名为 xxxxSmartAssistant_xxxxxxx 的 ssid 热点。
- 热点没有密码，任何人都可以连接。
- /usr/sbin/factoryTestServer.py 将作为 Web 服务在端口

8765 上以 root 权限运行。

- 其 Web 服务模块中存在代码注入漏洞，可能会将攻击者的远程 root shell 授予设备。

（四）应用安全评测

1. 评测内容

在智能音箱系统中，移动应用一般可以用来监测设备终端状态和控制设备终端。移动端威胁可分为应用安装前风险、安装风险、运行风险以及更新风险。其中应用在开发或打包前，未使用有效加固手段或未进行安全检测，导致移动应用被反编译或存在高危漏洞；

安装时，如未进行完整性校验或签名校验，可导致安装带有恶意行为应用；应用在运行时，如未增加有效防调试手段，黑客可读取内存信息获取应用运行逻辑或关键信息如密钥等；应用在更新时，未对更新包进行有效校验，导致安装带有恶意行为应用。以上任意阶段均可成为黑客攻击目标，以实现其远程控制或窃取隐私的目的。

针对以上安全风险，本次应用安全测评利用 App 漏洞扫描、反编译等工具，对智能音箱 App 进行安全性测试，发现存在的漏洞，验证其是否存在密钥泄露、代码逻辑漏洞、业务逻辑泄露等风险。

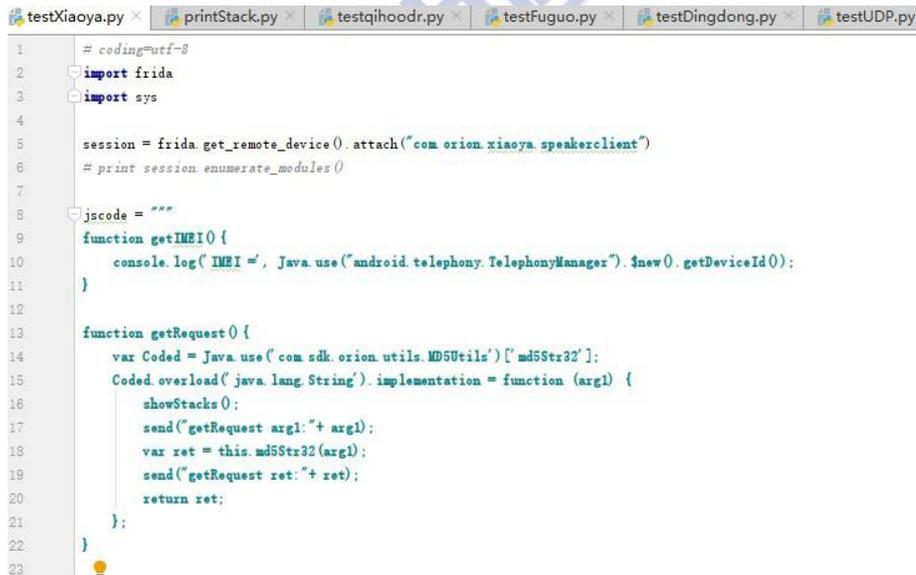
2. 评测结论

对被测产品对应客户端 APP 应用进行批量检测后，发现 80%应

用未进行过安全加固，也无防重打包和代码注入的能力。黑客能够通过反编译，在程序中植入木马、恶意代码及广告等，并可对其重编译二次打包，重打包后程序依然可正常运行。被恶意篡改后的程序可能导致用户隐私泄露，用户账户窃取等风险。与此同时，测试发现部分应用更新未对更新包进行版本号、哈希值、签名和文件大小校验，导致可通过篡改更新包植入恶意代码。

3. 典型问题

应用逆向篡改其运行逻辑：通过 JEB 查看某产品移动 APP 运行逻辑后，基于 Frida 进行 hook、调试，篡改其运行逻辑，在其中插入恶意代码，可实现对应用可控制设备的非法控制，如图 6 所示。



```
testXiaoya.py x printStack.py x testqihodr.py x testFuguo.py x testDingdong.py x testUDP.py
1 # coding=utf-8
2 import frida
3 import sys
4
5 session = frida.get_remote_device().attach("com.orion.xiaoya.speakerclient")
6 # print session.enumerate_modules()
7
8
9 jscode = """
10 function getIMEI() {
11     console.log('IMEI =', Java.use("android.telephony.TelephonyManager").$new().getDeviceId());
12 }
13
14 function getRequest() {
15     var Coded = Java.use('com.sdk.orion.utils.MD5Utils')['md5Str32'];
16     Coded.overload('java.lang.String').implementation = function (arg1) {
17         showStacks();
18         send("getRequest arg1:" + arg1);
19         var ret = this.md5Str32(arg1);
20         send("getRequest ret:" + ret);
21         return ret;
22     };
23 }
24 """
```

图 6 应用逆向

（五）无线通信安全评测

1. 评测内容

音箱系统通信网络环境相对复杂，包括终端与移动端互联、终端与服务端互联、移动端与服务端互联，同时应用多种通信协议包括蓝牙、wifi、蜂窝网络等。通信过程很多仅采用弱身份认证，甚至无身份认证。于此同时，大量设备在传输过程部分或全部明文传输，缺乏加密通信机制。无论弱身份认证或是明文传输，都会导致被非法攻击，后果既非法访问、数据丢失，数据篡改，更有甚者会被下达非法控制操作。

本次无线通信安全评测利用网络抓包、SSL 中间人攻击等方法，对通信进行监控，对通信协议安全性、数据传输保密性和完整性进行测试，验证是否有用户名密码泄漏、数据流地址泄漏、其他信息泄露等风险。

2. 评测结论

通过测试发现,60%音箱采用不安全传输协议通过公网网络或局域网络传输用户数据，导致传输信息易于窃取和替换。

3. 典型问题

对传输数据进行抓包获取其传输内容：通过测试发现，某音箱采用不安全传输协议通过公网网络或局域网络传输用户数据，导致传输信息易于窃取和替换。其 OTA 升级包地址通过明文传输，通过中间人攻击截获其传输信息，通过分析后，得到对应 OTA 升级包下载地址，更改地址后，可任意下发恶意程序，如图 7 所示。

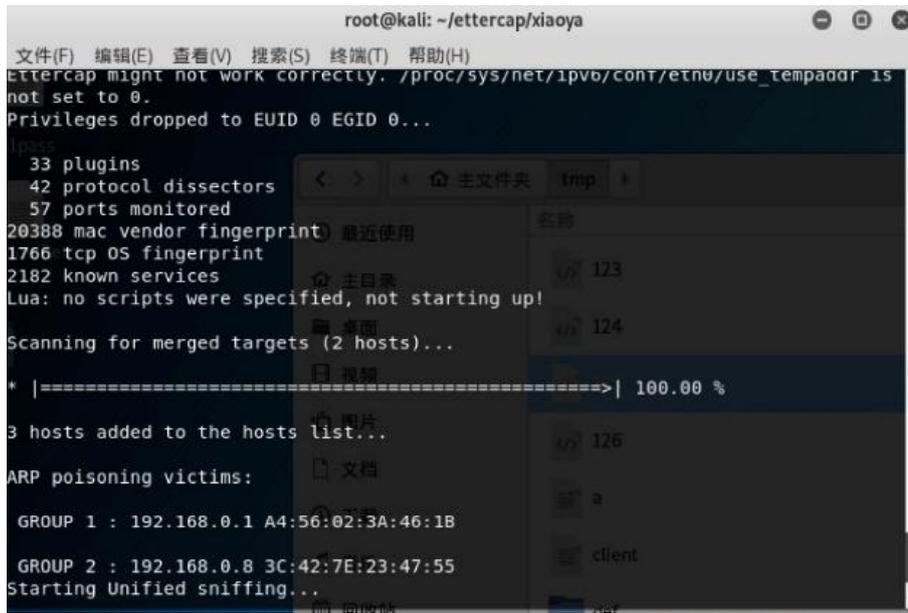


图 7 数据明文传输

替换升级包植入恶意行为:某音箱升级过程中只采用 MD5 校验,无签名校验,对其进行篡改后,通过中间人攻击使该音箱使用篡改后存在恶意行为的升级包升级,从而获取远程控制权限,如图 8 所示。

```

"data": {
  "rom": {
    "forced_update": false,
    "hash_code": "b00c1ad89767c0d7a0904d07558c4482",
    "os_version": "1.2.22",
    "update_desc": "",
    "url":
      "http://dlbcdn.update.aiirobot.com/rom/td_speaker_nano_1604781180_5585123180_1.2.22.zip"
  }
}

```

图 8 升级过程弱身份验证

(六) 用户个人信息安全评测

1. 评测内容

使用抓包工具和流量监控工具对终端以及 APP 数据传输过程抓包和监控,分析其是否上传产品型号、系统版本、序列号、IMEI、

地理位置等信息，以及确认信息内容是否明文传输。同时抓取与音箱对话内容、添加日历等。同时对其进行中间人攻击，验证是否存在用户数据泄露风险。

2. 评测结论

测试发现某些产品上传用户在该 APP 的任何操作、用户详细地理位置以及用户同音箱的详细对话内容。然后该系统应用采用非安全的传输协议，存在明文传输用户信息的行为，用户的操作、语音控制内容可被攻击者窃取或被恶意劫持，并替换诈骗、钓鱼、反动等非法信息。同时发现 70% 以上的产品可被获取 Root 权限，可基于获取权限通过不同方式对用户进行窃听。

3. 典型问题

伪造身份获取后台数据：通过对某产品通信数据进行抓包获取 token 后，就可向后台抓取对应用户与音箱的对话数据等内容，如图 9 所示。

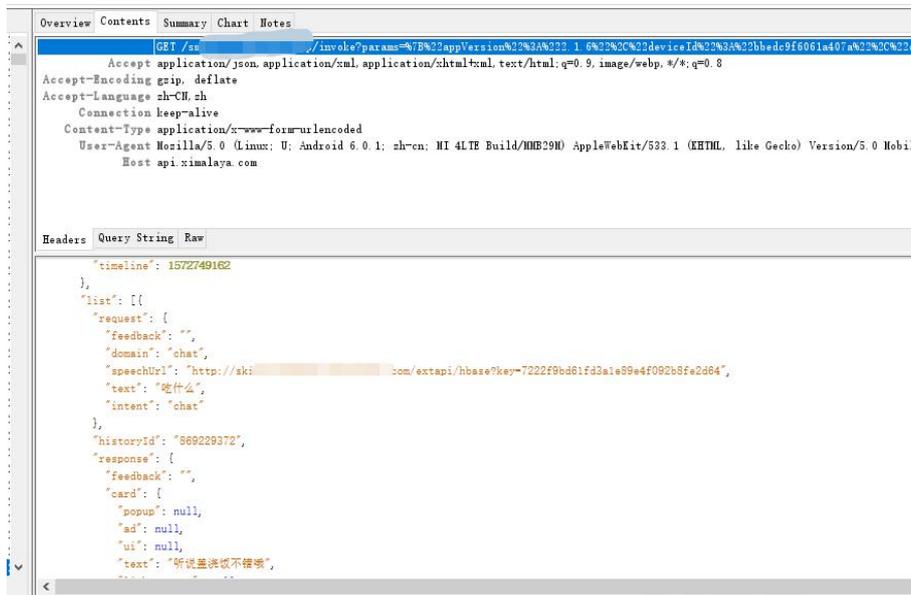


图 9 用户信息抓取

获取超级权限后对用户进行窃听：通过远程控制某音箱可以静默安装录音工具，实现对用户的窃听并上传窃听数据，如图 10 所示。

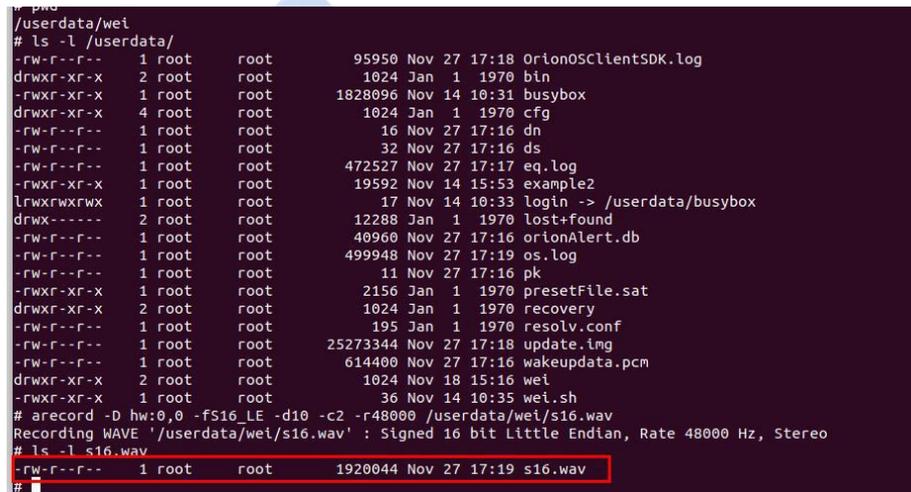


图 10 获取权限后实施窃听

三、2019 智能音箱十大安全风险

（一）个人信息收集处理规则模糊，存在过度收集和使用风险

随着移动互联网的迅速发展，智能音箱产品经历了“野蛮生长”的时代。为提供个性化服务，开展精准投放，智能音箱收集使用了大量用户的个人信息，包括音频信息、位置信息、通讯录等敏感数据。智能音箱在收集使用个人信息的过程中，存在以下现象：

智能音箱在收集处理个人信息时，规则模糊。智能音箱是具有智能语音交互系统、互联网服务内容，同时可扩展更多设备和内容接入的互联网终端产品。作为智能家居中控的存在，用户和智能音箱在进行语音交互时，智能音箱会收集音频信息，音频中包括个人信息中的声纹，而在隐私声明中，往往没有明示声纹、指纹等敏感信息在收集、存储、转移、删除和二次加工等处理的方式，因而收集的音频数据一旦泄露，可造会造成广泛的恶劣影响。

智能音箱在用户不知情的情况下，过度收集和使用个人信息。智能音箱易出现在用户不知情情况下，对用户语音、位置等敏感信息持续收集的现象，尤其是用户语音，用户较多不易感知。一些智能音箱并未通过隐私政策或其他途径明确告知用户收集使用信息的目的、方式、范围和频次，也未向用户提供明确的允许和拒绝的选

择，这种累积性的权益侵害在日常生活中普遍存在，将会引发用户的严重担忧。信息过度收集使用的乱象亟待解决。

预置应用大量收集使用个人信息。智能音箱通常会使用预置应用快速实现业务功能，而预置应用与智能音箱在收集用户信息方面具有同样的能力。鉴于预置应用的不开源性，智能音箱无法完全掌控预置应用的行为。部分智能音箱不清楚预置应用申请权限的目的，难以准确明示预置应用所收集使用的用户信息，通常只能通过协议约束预置应用收集使用用户信息的行为。某些预置应用同时被多家智能音箱集成使用，收集的海量数据一旦泄露，可造成广泛的恶劣影响。

（二）个人信息明文传输，存在数据泄露风险

智能音箱在传输个人信息如操作记录、对话记录等信息时，未采用有效的认证方式，或对传输信息未加密或采用弱加密方式，导致个人信息在传输中被非法获取。

（三）个人信息不安全存储，存在未授权访问风险

无论智能终端或是移动端，在采集到个人信息后，将信息存储至不安全区域，导致信息极易被窃取。即便将信息存储至服务端，也可通过假冒身份方式去获取个人信息。

(四) 设备硬件调试接口暴露，存在固件及敏感信息提取风险

部分厂商由于安全措施考虑不充分，导致用于设计时的前期调试接口暴露。攻击者可利用暴露接口，直接提取固件系统、密钥等信息。通过对固件系统进行静态分析与动态调试，挖掘可能存在的漏洞，并尝试利用发现的漏洞进行攻击。

(五) 设备系统更新不及时，存在高危漏洞利用风险

终端系统在设计开发时，主要以实现功能为主，对安全方面考虑较少，引入大量脆弱点；同时智能音箱系统版本较老，自身存在大量漏洞，甚至高危漏洞。攻击者可基于这些漏洞进行攻击，以获取用户数据或控制终端设备。

(六) 设备系统更新机制不安全，存在更新包篡改或替换风险

设备固件在升级过程中，对下载的固件和软件的签名和完整性没有进行校验，或是当对通信链路进行中间人攻击篡改服务器地址后，会下载存在恶意行为固件程序至终端，攻击者可基于该恶意程序完成对音箱系统的攻击。

（七）设备系统防护不足，存在恶意应用静默安装风险

由于设备安全防护能力不足，攻击者可利用多种方式（物理接触、远程网络接触等）获取系统 Root 权限，基于 Root 权限可预留后门，在用户不知情的情况下，后台静默安装恶意应用，例如录音工具等，获取用户隐私。

（八）身份认证机制缺陷，存在会话劫持风险

身份认证主要用来验证使用者身份，防范非法用户对云端与设备的访问。然而由于音箱系统验证机制存在逻辑漏洞或身份认证采用弱身份认证时，攻击者极易获取其认证信息，截取通话内容；同时可伪造终端同服务端对话，或伪造服务端同终端/移动端对话。

（九）移动应用安全防护不足，存在恶意代码植入风险

移动应用在开发时未引入相应安全措施，而如今移动应用攻击技术已非常成熟且多见。移动应用存在缺少身份鉴别机制、组件不安全、无反编译抗二次打包能力、抗动态调式、数据存储不安全等风险，导致攻击者极易植入恶意代码，以移动应用为切入点，入侵整个音箱系统。

（十）设备漏洞引发跳板攻击，影响互联设备安全

智能音箱多为智能家居网络的中控设备，而音箱设备可能存各个方向安全漏洞，攻击者可利用该漏洞，通过篡改其核心逻辑或添

加控制指令代码，对音箱进行控制，然后基于音箱控制相关的互联设备。

四、智能音箱用户个人信息保护的分析和建议

（一）规范用户个人信息收集使用规则

随着智能音箱功能的不断更新，收集使用的用户个人信息也随之增多。智能音箱设备应具有收集使用用户个人信息的规则，规则内容应包括所收集用户个人信息的内容、目的、方式和范围。智能音箱收集使用的用户个人信息中常会包含但不限于声纹、指纹、人脸等的个人敏感信息，对于这些个人敏感信息，规则中也应明确指出。

在个人信息收集前告知用户，且告知内容易读易获取。智能音箱应以界面或语音交互形式，明示用户个人信息收集使用规则。用户首次使用时，智能音箱设备应在开机向导的隐私政策或用户协议中，展现信息收集使用的内容，明确告知此设备将收集的详细信息。在使用智能音箱功能或服务过程中，需收集个人敏感信息时，应在每次收集前进行告知。当收集信息的内容、使用目的、收集方式与频率、存放地域与期限、保护方式、信息共享和个人信息控制权等发生变更时，应重新告知用户。在智能音箱界面中，应增加可供用户随时查看的隐私政策或用户协议入口。在个人敏感信息收集时，

应通过询问、弹窗等二次增强的告知方式，将收集的个人敏感信息告知用户，并由用户选择同意或拒绝。

明确用户音频信息收集使用方式。用户在操作智能音箱时，主要涉及用户音频信息，用户音频信息包括但不限于原始音频数据、经本地分析处理后的提取数据等。在语音交互中，智能音箱应明示本地收集、处理、存储、删除、转移共享音频信息的目的、类型、范围、方式、频次等（包括唤醒前、唤醒后）。在语音交互中，智能音箱应该明示云端收集、处理、存储、删除、转移共享音频信息的目的、类型、范围、方式、频次等。

告知内容应足够全面且易读。智能音箱明示于用户的个人信息收集使用规则应至少包含服务提供者的基本信息；收集使用的用户个人信息及收集使用的目的、方式、数量、范围、时机、频度、精度等内容，并显著标示个人敏感信息；保存地点、期限以及到期后的处理方式；是否会向第三方、境外提供以及向第三方、境外提供的用户个人信息的目的、方式、数量、范围、时机、频度、精度、第三方/境外接收方类型；用户撤销同意，以及查询、更正、删除个人信息的渠道和方法；投诉、举报渠道和方法等；用户个人信息保护措施；收集、使用规则的版本、发布时间；其他有利于保护用户知情权的事项。

(二) 落实用户信息收集使用告知同意原则

智能音箱设备在收集使用个人信息时，用户应具有知情权与选择权。智能音箱应详细告知所收集用户个人信息的内容、目的、方式和范围，仅当用户同意后方可收集。

用户确认方式应简单且明确。在智能音箱收集使用用户音频信息时，应具备用户主动确认的方式，包括但不限于语音确认和按键确认。智能音箱收集使用的音频信息，可能会涉及用户的敏感信息，如声纹、位置、指纹、人脸等信息，智能音箱应具备用户主动确认的方式，包括但不限于语音确认和按键确认。

用户确认方式应全面且可选择。智能音箱在收集和使用用户个人信息前，应主动告知用户，并获得用户同意后，方可收集使用用户个人信息，在提供用户确认时，应包括同意和拒绝选项，用户可通过按键选择同意或拒绝选项。智能音箱在收集使用用户个人敏感信息前，应告知主动告知用户，并获得用户同意后，方可收集使用用户个人敏感信息，在提供用户确认时，应包括同意和拒绝选项，用户可通过按键选择同意或拒绝选项。

收集使用行为应易于感知。在智能音箱界面中，应增加可供用户随时查看的用户敏感信息收集情况的入口，用户敏感信息包括但不限于指纹、声纹、位置等信息。在智能音箱使用用户个人敏感信息时，应增加可供用户随时查看的用户敏感信息使用的入口，用户

敏感信息包括但不限于指纹、声纹、位置等信息。

（三）重点加强音频等用户个人敏感信息全链条全生命周期安全防护

智能音箱收集使用的音频信息中的用户个人敏感信息直接关系到用户的切身利益，用户的音频信息、位置信息、生物识别信息等必须得到有效的安全防护。智能音箱设备厂商应健全生物特征数据保护架构，采用生物特征数据加密存储、生物特征数据加密传输等措施，保障用户切身权益。

收集方式应安全可控。智能音箱在收集用户个人信息时会涉及较多的音频、位置、个人习惯等敏感信息。在收集前，智能音箱应提供主动确认和授权的方式，待用户确认和授权后，方可进行收集。

存储方式应加密处理。智能音箱在存储个人敏感信息时，应采用加密等安全措施，例如用户位置、个人习惯等信息；存储个人生物识别信息时，应采用技术措施处理后再进行存储，例如用户声纹、指纹等个人生物识别信息。在控制端存储用户个人敏感信息时，应采用加密等安全措施，例如用户位置、个人习惯等信息；存储个人生物识别信息时，应采用技术措施处理后再进行存储，例如用户声纹、指纹等个人生物识别信息。在云服务端存储用户个人敏感信息时，应采用加密等安全措施，例如用户位置、个人习惯等信息；云服务端不应存储用户个人生物识别信息，例如用户声纹、指纹等个

人生物识别信息。

转移方式应加密处理。用户个人信息的转移即为用户个人信息的传输，在传输之前，应明示传输的范围且传输应可控，在传输用户个人敏感信息时，不应直接传输原始数据，应提炼关键词，进行处理，方可传输。智能音箱在转移用户敏感信息时，应采用加密传输等安全措施，例如用户位置、个人习惯等信息；智能音箱不应转移个人生物识别信息时，例如用户声纹、指纹等个人生物识别信息。在控制端转移个人敏感信息时，应采用加密传输等安全措施，例如用户位置、个人习惯等信息；控制端不应转移个人生物识别信息时，例如用户声纹、指纹等个人生物识别信息。在云服务端转移用户个人敏感信息时，应采用加密传输等安全措施，例如用户位置、个人习惯等信息。

删除方式应安全可控。智能音箱、控制端和云服务器均应提供删除用户个人信息的功能。个人信息主体要求删除的，应及时删除个人信息。智能音箱、控制端和云服务器应及时删除个人信息控制者违反法律法规规定，收集使用个人信息的；应及时删除个人信息控制者违反与个人信息主体的约定，收集使用个人信息的。智能音箱、控制端和云服务器应及时删除个人信息控制者违反法律法规规定或违反与个人信息主体的约定向第三方共享、转让个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止共享、转让

的行为，并通知第三方及时删除。智能音箱、控制端和云服务器应及时删除个人信息控制者违反法律法规规定或与个人信息主体的约定，公开披露个人信息，且个人信息主体要求删除的，个人信息控制者应立即停止公开披露的行为，并发布通知要求相关接收方删除相应的信息。

（四）明确预置应用用户个人信息收集使用规则及责任归属

智能音箱设备厂商应加强预置应用收集使用用户个人信息的防护，避免在用户不知情的情况下，用户个人信息被随意收集使用。

预置应用应明确收集使用用户个人信息规则。智能音箱设备应明确自身收集使用用户个人信息规则的适用范围和规范，如果智能音箱设备收集使用个人信息的规则不能包含预置应用收集使用用户个人信息的规则，需要预置应用单独明示收集使用用户个人信息的规则。

预置应用收集使用用户个人信息应可控。当用户通过智能音箱设备使用预置应用时，需要用户授权，智能音箱方可将用户个人信息提供给预置应用，包括但不限于用户的身份信息和位置信息。如果用户拒绝预置应用收集使用用户个人信息，需要用户在授权弹窗中选择拒绝授权，智能音箱设备将不会把用户个人信息提供给预置应用，且不会影响对智能音箱核心业务的使用。

(五) 加强预置应用权限调用可知可控力度

预置应用应遵循行为与用户意愿一致的基本原则，设计完善的权限管控机制，提升用户可知可控的能力，避免用户个人信息泄露。

用户对预置应用权限调用应可知。预置应用应通过给用户提示的方式来防范安全威胁，给用户的提示可以是图标、文字或其他明显的方式。在操作执行期间，提示应足够引起用户注意，且提示信息易于理解。

用户对预置应用权限调用应可控。预置应用应通过让用户确认的方式来防范安全威胁，用户应具有选择权，即用户能确认也能取消。预置应用应提供可配置操作，用户可以根据需要配置应用收集使用用户个人信息的权限、范围、频次等。当用户授权预置应用收集使用用户个人信息时，预置应用才可以收集使用用户个人信息；如果用户未授权给预置应用，预置应用不可收集使用用户个人信息。

五、智能音箱网络安全防护的分析和建议

(一) 设备出厂前关闭调试接口且去掉敏感信息

关闭调试接口。经过分析测试，调试接口极易成为攻击者攻击点，但是在生产和测试过程又需要基于该接口对产品进行调试或更新，因此建议产品量产后关闭所有调试接口 如需要调试或升级建议采用 TESTPIN 方式，并分散布置。

（二）采用最新的操作系统及外部代码库

及时适配操作系统最新稳定版本。应用开发者进行软件开发时，应及时适配操作系统最新稳定版本，给用户带来较好的使用体验和较强的个人信息保护机制，避免旧版本的遗留问题影响应用使用，侵犯用户权益。对于集成第三方代码的移动应用，在采用新版本操作系统后，需适配相应第三方代码库，避免旧版本代码的兼容性引入新问题。

充分利用终端和操作系统新特性。在应用开发时，开发者应充分利用终端和操作系统新特性，例如生物识别认证方式等。

（三）对设备系统及应用进行安全加固

对设备系统进行加固。智能音箱系统在烧录前，应进行相应的加固措施。例如对系统源码进行混淆，对固件中的so文件、可执行文件等进行加固，增加系统的防止逆向工程的能力。同时对带有资源文件、数据文件的系统，应对其相应文件加密，防止关键信息泄露。

对管控端的移动应用进行加固。在移动应用上架前，应对应用采取加固措施，包括但不限于加壳、数据加密、签名校验、防内存修改、完整性校验、应用安全检测等。防止应用被恶意破解、反编译、二次打包，内存抓取等攻击。

（四）采用安全存储技术保障敏感信息安全

采用硬安全区存储关键信息。智能音箱在硬件设计时，有能力者可集成安全芯片，存储密钥、身份、关键数据等信息。防止攻击者直接读取芯片内数据，

采用软安全区存在关键信息。由于成本以及设备体积原因，部分音箱无法集成带有安全功能的存储芯片。此类设备可加入软安全区，用来存储密钥、身份等关键信息。保证系统在运行过程中，全程不出现密钥等关键信息的明文，以防止攻击者通过对系统运行时调试获取关键信息。

（五）完善身份认证机制保障通信过程安全

建立端到端的双向身份认证机制。智能音箱系统应建立包括音箱与云平台、音箱与控制端、控制端与云平台、音箱与控制设备之间的双向身份认证机制。

建立安全身份认证过程。智能音箱通信过程应采用安全证书进行身份认证，校验并锁定安全证书，避免攻击者通过中间人攻击与通信两端建立联系。安全证书应与设备特征绑定，达到一机一密，防止身份被盗用，保证攻击者无法通过破解单个设备实现对批量设备的攻击。

六、智能音箱产业安全防护行动倡议

提升智能音箱产业安全防护能力，加强用户权益保护，离不开全行业的共同努力。我们倡议：

（一）加强音箱行业自律，明确企业主体责任

在行业协会的组织下，全面加强行业自律。行业自律是智能音箱安全防护的关键，也是企业可持续发展的内在基础。鼓励在行业协会的组织下，积极开展自律工作。芯片厂商、设备厂商、应用厂商、安全厂商等相关厂商积极落实主体责任，主动适应智能音箱设备产业新形势新要求，严格遵守法律法规，积极配合主管部门的监管要求，切实有效维护好用户合法权益。同时配合行业协会在智能音箱设备产业自治方面加大创新力度，积极探索自律新思路、新方法、新途径。

（二）推进标准规范制定，促进行业健康发展

在行业协会的带领下，大力推进标准规范制定。智能音箱的标准规范，是推动行业健康可持续发展的外在基础。在行业协会的组织推荐下，芯片厂商、设备厂商、应用厂商、安全厂商积极配合，在用户个人信息保护、硬件安全、操作系统安全等多方面加强协作，制定行业标准规范，研制技术方案，研究检测方法。在检测认证、监测处置等方面协调统一行动，强化产业协作体系，提升智能音箱

设备产业的安全防护能力，全民加强用户权益保护。

（三）依托社会公众监督，加强安全监管力度

高度重视用户权益保障，为用户举报监督创造便利条件。公众监督既是手段，也是目的。智能音箱厂商应以用户为中心，促进公众监督，为用户举报投诉设置便捷的方式和渠道，健全公众参与监督的机制，时刻关注用户感受和体验，尊重并保障用户的知情权和选择权，积极向行业主管部门移交公众举报信息。

（四）鼓励各方合作共享，协作提高安全水平

针对焦点和难点问题，产业界齐心协力联手行动。针对当前用户普遍关注的智能音箱用户个人信息安全、网络安全防护等问题，积极响应产业诉求，加强芯片厂商、设备厂商、应用厂商、安全厂商等多环节的沟通协调，在用户个人信息保护、硬件安全、操作系统安全等多方面加强协作，共享技术经验，创新安全技术，开发检测手段，提升智能音箱设备产业的安全防护能力，保护公众的合法权益。

中国泰尔实验室

地址：北京市海淀区花园北路 52 号

邮政编码：100191

联系电话：010-62300345

传真：010-62300536

网址：www.chinattl.com

