文献引用格式：韩志军，胡华鹏，孙凯．智能家居设备安全分析技术综述[J]．信息安全与通信保密，2022(6):144-153.
HAN Zhijun,HU Huapeng,SUN Kai.A Survey for Sercurity Analysis Technologies of Smart Home Devices[J].Information Security and Communications Privacy,2022(6):144-153.

智能家居设备安全分析技术综述*

韩志军，胡华鹏，孙　凯
（中国电子科技集团公司第三十研究所，四川 成都 610041）

摘　要：随着智能家居技术的广泛应用，智能家居作为物联网技术在家居领域的典型应用得到了迅速的发展。然而，智能家居设备中存在的安全缺陷将直接威胁用户的隐私安全甚至是生命财产安全，因此，针对智能家居的安全分析技术逐渐成为当前研究热点。在介绍了智能家居概念及其系统组成的基础上，分析了智能家居系统安全需求、安全风险以及风险来源，从固件获取及解析、静态分析、动态分析以及同源性分析等方面介绍了智能家居设备安全分析常规的流程及方法。

关键词：物联网；智能家居设备；安全缺陷；固件；安全分析
中图分类号：TN915.08　　**文献标志码：**A　　**文章编号：**1009-8054(2022)06-0144-10

A Survey for Sercurity Analysis Technologies of Smart Home Devices

HAN Zhijun, HU Huapeng, SUN Kai
（No.30 Institute of CETC, Chengdu Sichuan 610041, China）

Abstract: With the wide application of smart home technology, smart home, as a typical application of Internet of things technology in the field of home, develops rapidly. However, the security defects existing in smart home devices will directly threaten the privacy security of users and even the safety of life and property. Therefore, the security analysis technology for smart home has gradually become a hot issue. Based on the introduction of the concept of smart home and its system composition, this paper analyzes the security requirements, security risks and risk sources of smart home system. Finally, it describes the conventional processes and methods of security analysis of smart home devices from the aspects of firmware acquisition and analysis, static analysis, dynamic analysis and homology analysis.

Key words: IoT; smart home device; security vulnerability; firmware; security analysis

* 收稿日期：2022-02-14；修回日期：2022-06-03　Received date: 2022-02-14; Revised date: 2022-06-03

0 引 言

2021 年，是我国物联网发展史上具有里程碑意义的一年，据《2020—2021 中国物联网发展年度报告》显示，全球活跃物联网连接设备量首次超越非物联网设备，达到 117 亿台。随着物联网技术的发展以及伴随着的物联网设备量呈井喷式增长，物联网技术逐步向各行各业渗透，产生了一系列新的概念，其中，智能家居作为物联网技术在家庭环境中的典型应用，逐步进入大家的视野并在近几年得到了迅速发展。

智能家居设备的出现，使得人们可以随时随地通过互联网远程控制智能家居设备，了解智能家居设备工作状态，监控居家环境，为大家的居家生活增添了很大的便利，然而，智能家居设备所带来的安全风险同样不容忽视。智能家居设备的广泛应用将互联网中广泛存在的一些安全风险引入到了原本私密且封闭的居家生活环境中，这也意味着智能家居设备将直面来自互联网中的安全风险的挑战。而安全舒适的居家环境作为大家日常生活中最根本的需求，必须得到保障。因此，如何保障智能家居设备的信息安全成为实现智能家居行业长足发展所面临的一个重大障碍和考验。

本文从智能家居设备安全分析以及防御的角度出发，梳理已有的研究工作，并对这一领域新的研究方向和趋势进行初步的归纳和展望。

1 智能家居介绍

在国家标准 GB/T 35134—2017《物联网智能家居 设备描述方法》中，将智能家居定义为：以住宅为平台，融合建筑、网络通信、智能家居设备、服务平台，集系统、服务、管理为一体，其目的是为用户提供高效、舒适、安全、便利的居住环境 [1]。智能家居作为物联网技术在家庭环境中的典型应用，是将物联网技术融入传统家居系统的成果。

从国家标准给出的定义可以看出，网络通信、智能家居设备和服务平台是构成智能家居的重要组成部分。智能家居系统组成如图 1 所示。

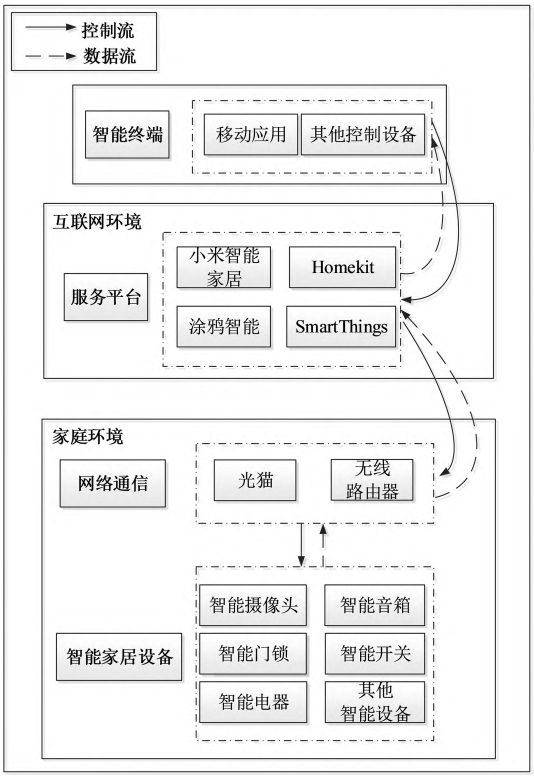

图 1 智能家居系统组成

智能家居主要通过网络等通信技术手段控制智能家居设备，网络的接入打破了传统家居设备封闭的环境，给使用者远程监视家居设备工作状态、控制家居设备提供了通道，同时网络的接入也为智能化的实现奠定了基础。智能家居环境下，目前应用比较广的网络通信方式主要包括有线以及 Wi-Fi、蓝牙、近场通信（Near Field

1.工作频率：NFC的工作频率为13.56MHz，而RFID的工作频率有低频，高频（13.56MHz）及超高频。
2.工作距离：NFC的工作距离理论上为0~20cm，但是在产品的实现上，由于采用了特殊功率抑制技术，使其工作距离只有0~10cm，从而更好地保证业务的安全性。由于RFID具有不同的频率，其工作距离在几厘米到几十米不等。
3.工作模式：NFC同时支持读写模式和卡模式。而在RFID中，读卡器和非接触卡是独立的两个实体，不能切换。
4.点对点通信：NFC支持P2P模式，RFID不支持P2P模式。
5.应用领域：RFID更多的应用在生产，物流，跟踪和资产管理上，而NFC则工作在门禁，公交卡，手机支付等领域。
6.标准协议：NFC的底层通讯协议兼容高频RFID的底层通信标准，即兼容ISO14443/ISO15693标准。NFC技术还定义了比较完整的上层协议，如LLCP，NDEF和RTD等。

Communication，NFC）、4G/5G 等无线通信方式。其中，以 Wi-Fi 为代表的无线通信方式凭借无需布线、接入便捷、技术成熟、兼容性强等优势，成为智能家居中的主要网络通信方式。

智能家居设备包括智能摄像头、智能音箱、智能门锁、智能开关等家居设备，这些设备通过接入网络来实现智能化，最终由智能家居平台进行统一管理[2]。相较于传统家居设备，智能家居设备最显著的区别在于其具备了网络接入能力，可以通过有线或者 Wi-Fi、4G/5G 等无线接入的方式接入互联网。Wi-Fi 的接入需要依赖于无线路由器，无线路由器作为家庭内部网络与互联网的接口，在智能家居中扮演着重要的角色。

智能家居的智能不仅仅体现在远程控制上，数据的分析处理及反馈才是更深层次智能化的体现，而这一功能依托于服务平台实现。智能家居设备作为数据采集和执行的终端，将采集到的数据以及自身的状态信息通过网络上传至服务平台，在服务平台上进行数据分析处理，进而获取智能家居设备的行为模式等信息，控制命令作为智能家居的神经中枢，也是通过云平台下发到智能设备，因此服务平台是智能家居体系中不可或缺且非常重要的一部分[3]。

2 智能家居安全风险分析

随着服务平台的引进、网络的接入以及家居设备功能的扩展，智能的概念被引入到家居领域。然而智能家居设备的大面积应用带来了更高的信息安全风险，限制了智能家居的发展。

2.1 智能家居安全防护需求

区别于其他信息设备，智能家居的应用场景是私密的家庭环境，其目的是为用户提供高效、舒适、安全、便利的居住环境，因此智能家居在信息安全防护方面有着较高的需求。结合信息系统安全层次划分[4]，智能家居安全防护需求主要体现在设备安全需求和数据安全需求两个方面。

设备安全主要体现在设备的稳定性、可靠性、可用性 3 个方面，是智能家居系统安全的物质基础。智能家居环境下的设备安全和家庭环境的物理安全有着紧密的联系，例如智能空调可能会被随意调节温度，智能洗衣机被攻击后连续高速运转，这些都将对使用者的生命财产安全造成威胁，其中最典型的案例是智能门锁，研究人员发现市面上部分智能门锁存在安全漏洞，不通过预设的密码或者指纹就能打开门锁。

数据安全主要体现在数据的秘密性、完整性、可用性 3 个方面，大数据时代的来临，使数据安全扮演着越来越重要的角色。特别是《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》等法律文件的出台，进一步明确了对各类数据的采集利用和全生命周期保护的必要性和迫切性，智能音箱、智能摄像头作为家庭环境中随处可见的数据采集设备，对数据安全保障的需求尤为迫切。

2.2 智能家居安全风险层次分析

作为物联网在家庭环境的典型应用，智能家居系统体系架构和物联网系统相同，自下而上划分为感知层、网络层和应用层 3 个层次。底层的感知层作为物联网系统特有的层次，主要实现数据的感知采集以及数据处理后的反馈执行。网络层主要实现数据、控制命令在设备

间以及设备与服务平台间的交互、传输，是智能家居系统互联互通的管道。应用层的功能分为两个方面，一方面是身份认证、数据存储处理等通用的功能；另一方面与设备的具体业务高度关联，主要实现设备业务数据的分析处理以及业务功能的控制。

（1）感知层安全风险分析。感知层作为智能家居系统与物理世界直接交互的接口，主要面临智能家居设备硬件、操作系统 / 固件方面的威胁。硬件方面，一些智能家居设备暴露在公共场所中，例如智能摄像头、智能门铃等，攻击者可以轻易接触到这些设备，并通过设备上预留的一些硬件接口（如 USB、UART、JTAG 等）窃取设备中所存储的隐私信息，更有甚者能利用这些硬件接口结合设备本身存在的一些缺陷（如弱口令等）篡改存储在 flash 中的固件，植入后门，进而获得设备的控制权。操作系统 / 固件方面，由于固件本身存在一些漏洞，攻击者可以利用这些漏洞并借助网络或者物理接触的方式实现对设备功能的扰乱以及控制权的获取。此外，设备在固件升级过程中缺乏校验机制等一系列措施，使得攻击者在此过程中可以通过网络的方式植入含有木马的固件。

（2）网络层安全风险分析。网络层在智能家居中起到类似神经中枢的作用，设备与设备之间，设备与服务平台之间的互联互通都依赖于网络层的功能实现，因此，网络层主要面临网络协议、认证机制以及通信流量方面的威胁。网络协议方面，许多智能家居设备由于功耗体积的限制采用了一些物联网特有的协议，与在长期的攻防博弈中完善了安全机制的通用互联网协议不同，目前针对这些协议的安全研究还不够充分，因此容易存在一些协议上的漏洞，攻击者可以利用协议漏洞实现非法的网络接入进而窃取、篡改数据，导致隐私数据泄露、控制扰乱。认证机制方面，一些服务平台和设备身份认证机制不完善，采用的安全协议存在缺陷，访问控制机制缺失，攻击者可在较短时间内非法接入到服务平台或者设备。通信流量方面，容易遭受拒绝服务攻击，攻击者通过控制大量的物联网设备向目标设备发送庞大的超过目标设备处理能力的数据流量，导致目标设备网络崩溃进而影响设备的正常使用。

（3）应用层安全风险分析。应用层主要是依靠丰富的应用程序向用户提供相应的服务，因此，应用层主要面临应用程序漏洞的威胁。在公开发布的漏洞中存在着大量与智能家居设备相关的漏洞，其中不乏应用程序方面的漏洞，例如，某款摄像头中提供的实时流传输协议（Real Time Streaming Protocol，RTSP）服务和 Web 服务的主程序名为 ipc_server，研究人员在对 ipc_server 进行分析时发现其中存在多个登录绕过和缓冲区溢出漏洞，攻击者利用这些漏洞可以实现对摄像头的远程控制 [5]。

2.3 智能家居安全风险来源

相较于传统家居设备，智能家居设备具有 3 个最为显著的特征，分别是网络化、智能化和远程控制，网络化和智能化的实现依赖于智能化的设备、网络的接入以及数据的采集处理。

如图 2 所示，智能家居安全风险主要来源于网络通信、服务平台和智能设备 3 个方面。其中，网络通信为网络攻击提供了入口，而网

络攻击的主要目标是智能家居环境中的智能家居设备。服务平台存在隐私数据泄露的风险，而作为数据采集和反馈执行的终端，智能家居设备的安全直接关乎智能家居系统的数据安全。

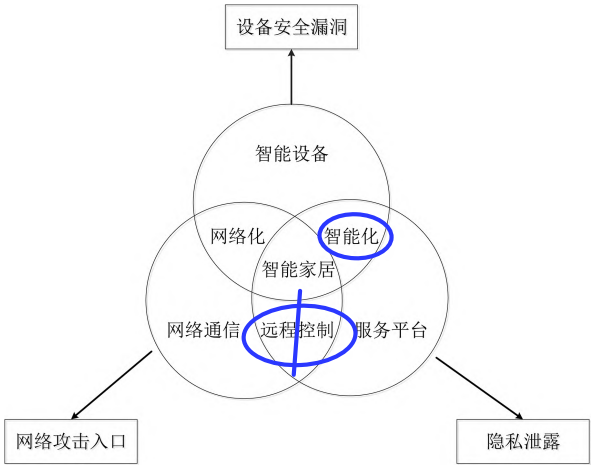

图 2　智能家居安全风险

智能家居设备种类繁多，数量庞大。一方面，智能家居设备的功能多种多样，功能的多样性决定了设备所采用的硬件架构、操作系统以及相关通信控制协议的多样性，因此针对智能家居设备的安全防护没有通用的防护措施或者安全防护软件。另一方面，智能摄像头、无线路由器等智能家居设备通常需要长时间工作，并且很多例如智能扫地机器人等移动的智能家居设备采用电池供电的方式，因此智能家居设备往往有低功耗的需求，这也就导致设备本身计算资源和存储资源极其有限，并且大部分资源及能耗都投入到设备的核心应用功能中，因此智能家居设备在安全防护及隐私保护方面投入的资源就非常有限。此外，智能家居设备上所搭载的嵌入式操作系统在设计之初并未将安全作为最重要的考虑因素，因此在设计层面也缺乏足够多的安全防护方面的考虑。以上诸多原因导致智能家居设备成了安全漏洞的重灾区。

综合对智能家居安全需求、风险分析和风险来源等方面进行分析，如图 3 所示，在安全需求方面，设备安全是智能家居安全的基础，也是数据安全实现的根本保障；在风险分析方面，因为设备的缺陷而引入的安全风险覆盖智能家居系统感知层、网络层、应用层 3 个层次；在风险来源方面，智能设备是安全漏洞的重灾区，安全漏洞数量众多。综上所示，对智能家居设备安全分析的研究焦点主要集中在智能家居设备上。

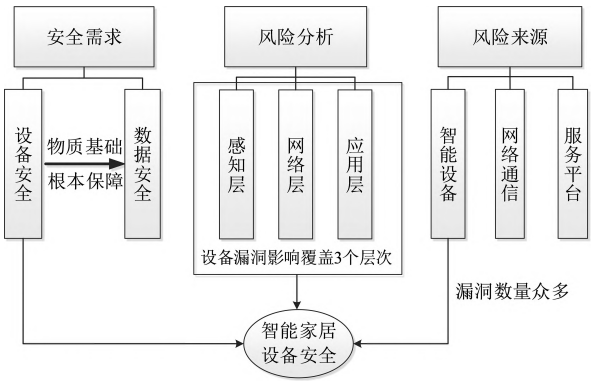

图 3　智能家居安全分析焦点

3　智能家居设备安全分析方法

智能家居设备典型软硬件结构如图 4 所示。智能家居设备核心功能主要依托设备固件实现。因此，智能家居设备安全分析的焦点也集中在针对智能家居设备固件的安全分析上。其安全分析方法和物联网设备安全分析方法类似，可分为静态分析技术、动态分析技术和同源性分析技术 3 种类型 [6]。

3.1　智能家居设备固件及其获取方式

智能家居设备固件是运行在智能家居设备硬件系统上的软件程序，通常烧写在设备的只读存

储器（Erasable Read-Only Memory，EROM）、电可擦除只读存储器（Electrically Erasable rogrammable Read Only Memory，EEPROM）或者闪存（Flash）上，由固件头、固件主体以及其他附属数据组成。

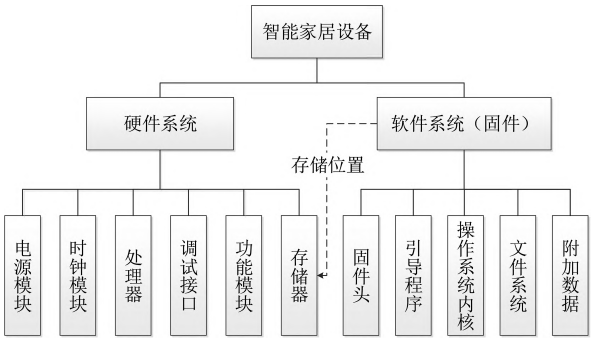

图 4　智能家居设备典型软硬件结构

固件承载了设备的操作系统和相应的应用程序，依据设备搭载的操作系统，物联网设备固件分为通用操作系统固件、实时操作系统固件和无操作系统固件 3 种类型。其中，第一类通用操作系统固件通常搭载裁剪后的 Linux 操作系统，这一类操作系统中通常使用一些轻量化的用户环境，例如 BusyBox 和 uClibc 以节省硬件资源消耗，将更多的硬件资源留给应用程序以实现特定的功能，智能摄像头、路由器以及智能电视机等设备对实时性要求不高，操作系统与硬件交互相对较多的设备通常搭载了这一类固件。第二类实时操作系统固件，搭载这一类固件的设备更加注重程序执行的实时性，通常采用 VxWorks 等实时操作系统。这一类固件通常搭载对运算能力要求较低的、执行单一任务的设备上，例如智能开关、智能灯泡等。第三类无操作系统固件被称为“monolithic firmware”[7]，固件中不存在典型的操作系统结构，搭载这一类固件的设备通常基于一个控制循环以及外设触发的中断对外部事件进行处理。

固件作为智能家居设备安全分析的对象，获取并解析固件是智能家居设备安全分析的第一步。智能家居设备固件一般可以通过以下 3 种方式获取。

（1）通过物理方式直接获取。智能家居设备固件一般存储在设备存储芯片（通常为 flash 芯片）上，因此可以根据相应存储芯片的类型选择对应烧写器将固件读出。这种方式的缺点在于需要将焊接在设备主板上的 flash 芯片取下，读取固件后还需要将存储芯片重新焊接到主板上，设备才能正常工作。由于存储芯片体积较小、管脚较细，拆卸焊接过程中有可能会损坏存储芯片。

相较于直接读取存储芯片的方式，通过调试接口获取固件的方式不需要拆卸存储芯片。由于 flash 芯片一般焊接在主板上，而主板上预留有调试接口，方便开发人员进行调试，并且出厂后多数设备会保留调试接口，其中比较典型的就是通用异步收发传输器（Universal Asynchronous Receiver/Transmitter，UART）接口。通过连接设备 UART 接口可以获取设备的 root 权限，这种方式的缺点在于部分设备连接 UART 接口后需要登录密码方可获取 root shell 权限。为了解决部分设备登录密码无法获取的问题，在设备启动过程中，通过 bootloader 阶段的 shell 获取设备的 root 权限进而将设备固件 dump 出。

（2）通过设备厂商获取。例如一些路由器或者智能摄像头厂商一般会在官网上提供固件下载链接，可以通过 Web 或者文件传输协议（File Transfer Protocol，FTP）的方式下载相应设备固件。针对一些设备厂商官网不提供下载链接的新推

出的设备或者较早版本的固件，可以通过联系售后服务顾问的方式获取固件。

（3）通过伪造空中下载技术（Over-the-Air Technology，OTA）方式获取。许多智能家居设备厂商提供 OTA 升级服务，设备采用一定的数据格式和交互协议向厂商 OTA 服务后台发起 OTA 更新请求，因此，可以通过分析设备与 OTA 服务后台交互的数据格式及交互协议来模拟真实设备的行为，向后台请求更新服务并获取设备固件。

3.2 静态分析技术

静态分析是指在设备程序不运行的情况下，针对静态固件中二进制程序以及相关配置文件等文本文件的结构和功能信息进行分析，挖掘程序及相关文本文件在逻辑上、语法上的缺陷。如图 5 所示，智能家居设备静态分析过程一般包含以下几个步骤。

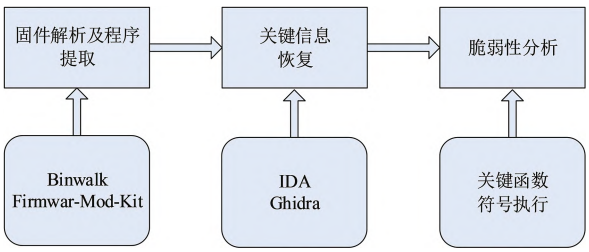

图 5 静态分析步骤

（1）固件解析及程序提取。设备实现各种功能所依赖的全部可执行程序和配置文件信息都包含在文件系统中。这些信息对固件的分析至关重要。然而，不同的设备所使用的文件系统格式和文件系统的压缩算法不尽相同，增加了文件系统提取的难度[8]。从固件中提取文件系统一般有两种方式：手动提取和自动提取。在实际应用中，一般采用自动提取的方式，借助 Binwalk 等自动解析工具，实现固件格式、文件系统和操作系统的识别与分离，以及文件系统解析和提取。此外，研究人员在 Binwalk 的基础上，整合了其他固件解析工具，形成诸如 Firmware-Mod-Kit 等工具集合，借助相应脚本实现了基于 Linux 系统固件的自动化压缩和解析。

（2）关键信息恢复。由于智能家居设备中固件程序通常是商业程序，很少有厂商公开源代码和相关文档，因此安全分析的目标大多是编译后的二进制程序。需要借助交互式反汇编器专业版（Interactive Disassembler Professional，IDA Pro）等反编译工具，将二进制代码转换成统一的中间语言——伪代码。此外，借助 IDA Pro 等反编译工具还能实现程序结构、函数调用关系、字符串引用、地址访问等关键信息的解析和恢复。目前 IDA Pro 可以支持 x86、ARM、MIPS、PowerPC 等多种指令格式二进制汇编代码的转换，涵盖大量智能家居设备的指令集。

美国国家安全局研究部门最近公开了一款名为 Ghidra 的软件逆向工程（Software Reverse Engineering，SRE）框架[9]，其功能和 IDA Pro 类似，优势在于公开提供应用程序接口（Application Programming Interface，API），便于用户开发自己的插件和脚本，并且相较于 IDA Pro，可以在不使用插件的前提下实现 MIPS 架构伪代码的生成。

（3）脆弱性分析。相较于针对通用系统的分析，针对智能家居物联网设备的程序分析更加关注特定的漏洞类型和功能模块。在漏洞类型方面，更加关注验证绕过漏洞、远程代码执行漏洞等能够获取 shell 权限的漏洞。在功能模块方面，更加关注存在人机交互、输入输出的

接口类应用程序，这一类程序中存在远程代码执行漏洞的概率相对较高。针对路由器、IP 摄像头这一类家居设备，其安全缺陷存在的重灾区就在设备的 Web 服务器程序上，在已经公开的漏洞中，例如 CVE-2020-8863、CVE-2018-13313 等漏洞都来自设备的 Web 服务器程序。因此，在关键信息恢复的基础上，对控制流图中的指令进行语法分析和程序指令的语义分析，并聚焦于相关接口程序中输入输出函数以及 system 函数等关键函数，分析其函数功能和执行逻辑，进而发掘存在的缺陷。此外，还可以借助符号执行技术等方式辅助静态分析技术实现设备脆弱性的发掘。

3.3 动态分析技术

模糊测试技术作为一种高效的动态分析技术广泛应用于智能家居设备的安全分析中，模糊测试一般步骤如图 6 所示。

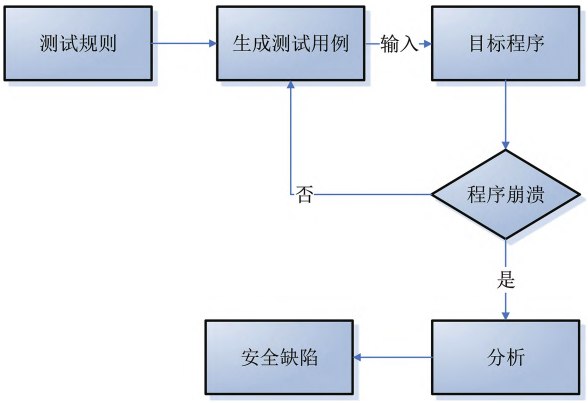

图 6 模糊测试一般步骤

首先依据一定规则，针对特定测试对象自动化或者半自动化生成一系列测试数据，并将其作为目标程序的输入，然后利用监视器监视目标程序运行状况，在测试用例集较为庞大的时候，异常监视往往采用自动化的方法，例如基于调试的方法和插桩的方法。当监视器监测到程序执行异常时，往往需要人工的介入，针对发生异常的位置和原因进行人工分析，确定安全缺陷的存在。

根据程序执行反馈的获取情况，可以将模糊测试分为黑盒测试、白盒测试和灰盒测试[10]。其中，黑盒测试的测试用例按照预先设定的测试规则生成，不受之前测试用例测试结果的影响，这一类测试工具的代表是 boofuzz 和 Peach。白盒测试与黑盒测试相反，测试过程中会对目标程序进行动态污点分析和符号执行以准确获取程序的执行状态，进而指导接下来测试用例的生成，这一类工具的代表是 IoTFuzzer。灰盒测试则介于黑盒测试和白盒测试之间，测试过程中，fuzz 程序会获取部分程序执行的关键特征信息并影响接下来测试用例的生成，相较于完全获取程序执行状态，部分获取关键执行信息的方式提升了模糊测试的效率，这一类工具的代表有 FirmAFL 和 FirmFuzz。

3.4 同源性分析技术

为了节省开发时间，提高产品研发效率，智能家居设备在研发过程中往往会在设备固件程序中复用大量第三方开源框架和组件，例如以 LightHttpd 为代表的轻量化 Web 服务器框架在大量路由器以及智能摄像头中被广泛使用。因此，在智能家居设备中广泛存在这种现象，在不同类型、不同功能、不同硬件架构的设备固件中存在着由相同或相似代码段编译而成的二进制程序。设想一下，如果在复用的这些源码中存在着安全缺陷，那么其影响的覆盖面将会扩大，在存在着相同代码段的不同类型设备中也将存

在相同的缺陷。因此，使用同源性分析技术能够迅速发现在不同设备中存在着因相同缺陷代码所引入的安全漏洞。目前，同源性分析技术主要分为基于二进制文件的粗粒度相似性对比和基于代码片段细粒度相似性对比两大类。具体分类及方法如图 7 所示。

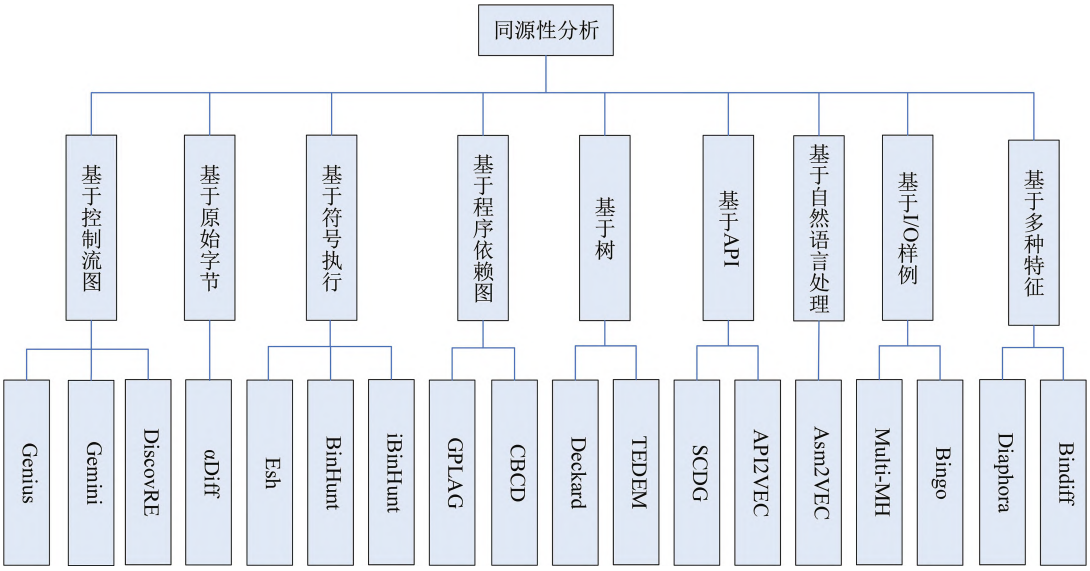

图 7　同源性分析工具分类及方法

4　结　语

随着智能家居设备的广泛应用，越来越多的人享受到了智能家居所带来的便利。与此同时，智能家居的安全也愈发引起了大家的重视，人们对智能家居安全的需求日益增加。本文在综合分析智能家居系统组成及安全风险的基础上总结了智能家居设备安全分析的一般流程及方法。

虽然目前针对智能家居设备安全分析技术的研究取得了一定成果，但是仍受以下 3 个方面因素的制约：智能家居设备种类众多，核心功能各异，设备软硬件架构差异较大，难以通过单一安全分析方法实现；研究工作开展时间较短，且研究目标技术体系更新较快，尚未形成完善的技术体系；现有安全分析方法智能化程度较低，分析效率有待提升。因此，智能家居设备安全分析技术在适应性、准确性和分析效率方面还有待进一步完善。

参考文献：

[1] 国家质量监督检验检疫总局，中国国家标准化管理委员会 . 物联网智能家居 设备描述方法：GB/T 35134—2017[S]. 北京：中国标准出版社 ,2017.

[2] 李意莲 . 物联网智能家居访问控制技术研究 [D]. 西安：西安电子科技大学 ,2020.

[3] 周莹，郑仲凯，谷红霞 . 一种智能家居的云平台系统 [J]. 电子世界 ,2021(16):27-28.

[4] 张焕国，韩文报，来学嘉，等 . 网络空间安全综述 [J]. 中国科学：信息科学 ,2016,46(2):125-164.

[5] Knowsec 知道创宇 . 网络摄像头登录绕过及多个 RCE 漏洞及数据分析报告 [EB/OL].(2018-07-31)[2022-02-04].https://www.freebuf.com/vuls/179155.html,2018.

[6] 郑尧文，文辉，程凯，等 . 物联网设备漏洞挖掘技术

研究综述 [J]. 信息安全学报 .2019,4(5):61-75.

[7] MUENCH M,STIJOHANN J,KARGL F,et al.What You Corrupt is not What You Crash: Challenges in Fuzzing Embedded Devices[C]//Proceedings 2018 Network and Distributed System Security Symposium,2018:30-43.

[8] 李建春 , 谢瑞云 , 张旭博 . 基于固件分析的路由器 Web 页面安全评估技术 [J]. 通信技术 ,2018,51(3):676-681.

[9] Crownless. 全面详解 Ghidra[EB/OL].(2019-03-18)[2022-02-04].https://zhuanlan.zhihu.com/p/59637690.

[10] 于颖超 , 陈左宁 , 甘水滔 , 等 . 嵌入式设备固件安全分析技术研究 [J]. 计算机学报 ,2021,44(5):859-881.

作者简介：

韩志军（1984—），男，硕士，工程师，主要研究方向为网络安全；

胡华鹏（1989—），男，硕士，工程师，主要研究方向为网络安全；

孙　凯（1987—），男，学士，工程师，主要研究方向为网络安全。