ICS 33.050
M 30

中华人民共和国国家标准

GB/T 39575—2020

具有融合功能的移动终端安全能力技术要求

Technical requirements for security capability of mobile terminal with syncretic function

2020-12-14 发布　　2021-07-01 实施

国家市场监督管理总局
国家标准化管理委员会　发布

目　　次

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

请注意本文件的某些内容可能涉及专利。本文件的发布机构不承担识别这些专利的责任。

本标准由中华人民共和国工业和信息化部提出。

本标准由全国通信标准化技术委员会(SAC/TC 485)归口。

本标准起草单位:中国信息通信研究院、高通无线通信技术(中国)有限公司、真珍斑马技术贸易(上海)有限公司、联想移动通信科技有限公司。

本标准主要起草人:姚一楠、陈婉莹、董霁、翟世俊、王宇晓、王嘉义、杜志敏、翁元、李欣。

引　言

随着移动互联网的快速发展，传统智能终端手机、平板电脑等，并不能完全满足用户的使用需求。因此出现了如车载智能终端、可穿戴智能终端、智能家居等，很多具有融合功能的移动终端。用户在享受具有融合功能的移动终端带来的丰富多彩的功能时，却也面临着很多安全风险。近年来，在具有融合功能的移动终端上恶意吸费、隐私泄露等安全事件频发，大大影响到了用户的使用，也制约了其发展。究其原因，融合功能逐渐增多，但是终端设计本身并没有过多的安全考虑，尤其对于数据通信传输没有适当的安全保护，造成了个人信息泄漏、资费损失等安全问题。因此，有必要对具有融合功能的移动终端的硬件、操作系统、外围接口、应用软件及个人信息保护等方面提出一整套安全技术要求。

本标准的制定旨在规范具有融合功能的移动终端安全技术要求，提高其安全防护能力，从而防范终端上的各种安全威胁，避免用户的利益受到损害。

具有融合功能的移动终端安全能力技术要求

1 范围

本标准规定了具有融合功能的移动终端安全能力的技术要求，包括硬件安全能力、操作系统安全能力、应用软件安全能力、通信连接安全能力、个人信息安全保护能力的技术要求。

本标准适用于各种制式的具有融合功能的移动终端，其他终端也可参考使用。

2 规范性引用文件

下列文件对于本文件的应用是必不可少的。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本(包括所有的修改单)适用于本文件。

YD/T 3082—2016 移动智能终端上的个人信息保护技术要求

YD/T 3228—2017 移动应用软件安全评估方法

3 术语和定义、缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

具有融合功能的移动终端 mobile terminal with syncretic function

可对人或物进行信息采集和处理，具备蜂窝网络和互联网络接入功能，支持语音或数据通信，具有融合功能的终端设备。

3.1.2

融合功能 syncretic function

基于终端硬件及软件资源和能力，在终端上承载的除语音和数据通信以外非通信行业功能(例如：数字电视广播、车辆控制、扫码、人体信息采集等)。

3.1.3

脱敏 desensitization

通过模糊化等方法处理原始数据，以实现屏蔽敏感数据且屏蔽后的数据不可逆向恢复的数据保护方式。

3.1.4

个人信息 personal Information

可为信息系统所处理、与特定自然人相关、能够单独或通过与其他信息结合识别该特定自然人的计算机数据。

3.2 缩略语

下列缩略语适用于本文件。

API:应用程序编程接口(Application Programming Interface)
CNVD:国家信息安全漏洞共享平台(China National Vulnerability Database)
CNNVD:中国国家信息安全漏洞库(China National Vulnerability Database of Information Security)
NFC:近场通信(Near Field Communication)
SD:安全数字存储卡(Secure Digital Memory Card)
USB:通用串行总线(Universal Serial Bus)
WLAN:无线局域网(Wireless Local Area Network)

4 具有融合功能的移动终端安全架构

4.1 安全架构概述

图1为具有融合功能的移动终端安全架构,主要包括5个部分:硬件安全、操作系统安全、应用软件安全、通信连接安全、个人信息安全。硬件主要包括基础硬件模块、硬件接口和外设;操作系统主要包括硬件驱动、软件系统内核、各种函数库、基础服务等;应用软件主要包括运行于系统之上的各种本地及Web应用,包括消费类应用、行业应用等各类应用软件;通信连接主要包括网络接入、通信过程、外围接口。

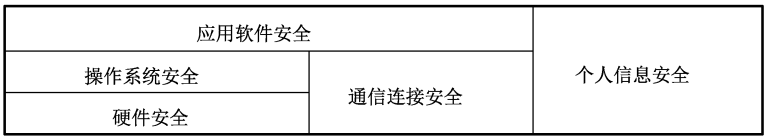

图1 具有融合功能的移动终端安全框架

4.2 硬件安全目标

具有融合功能的移动终端硬件安全目标是保证终端内部芯片数据存储和运算的安全性,能够对抗密码分析、侧信道攻击等破坏数据保密性、完整性的安全威胁。

4.3 操作系统安全目标

操作系统安全目标是保证符合终端使用场景的身份权限管理和访问控制,能够正确地响应授权操作和处理异常行为,保证系统数据的保密性和完整性,保证系统能按照正常预期运行。

4.4 应用软件安全目标

应用软件安全目标是保证运行在操作系统上的应用软件具备来源标识和保密性、完整性防护措施,可以对抗逆向分析,保证敏感行为可以得到控制。

4.5 通信连接安全目标

通信连接安全目标是保证终端所采用的无线或有线传输数据时,采取必要的加密和完整性校验手段,防止认证、标识、口令等业务通信数据在传输过程中被获取甚至篡改。

4.6 个人信息安全目标

个人信息安全目标是保证终端产生的个人信息在收集、使用、传输、删除过程中不被非法获取,不被非法篡改,保证数据在生命周期各环节的安全性。

5 具有融合功能的移动终端安全技术要求

5.1 硬件安全

5.1.1 标识唯一

终端硬件应具备唯一可识别性，硬件标识区不可被改写。

5.1.2 设计安全

芯片应不存在能够使厂商在未获得用户授权的情况下，对芯片内存进行访问或更改芯片功能的隐蔽接口，包括在芯片设计验证阶段使用的调试接口。

加密芯片应采用必要的安全机制保证密钥的产生、分发、使用、存储和销毁的安全性，例如随机数熵值不低于128比特、采用安全区域运行等。

5.1.3 防止物理攻击

具有融合功能的移动终端硬件芯片宜具有防物理攻击的能力，防止信息泄露。攻击手段包括但不限于非侵入式攻击、半侵入式攻击和侵入式攻击。

芯片加密模块应支持防旁路攻击，以及抵抗错误注入攻击。

5.2 操作系统及应用软件安全

5.2.1 安全引导

操作系统应提供安全机制，保证系统启动过程只能加载可信组件，例如：内核、基带固件等。

5.2.2 完整性校验

操作系统应采用完整性校验手段对核心服务、安全网关、权限管理等关键代码或文件进行校验，防止关键文件被篡改。

5.2.3 终端接入认证

应通过数字签名、证书或其他方式保证只有通过认证的终端才可以接入、使用和操作融合功能。避免非法设备接入，从而导致敏感信息泄露、功能异常等。

5.2.4 标识与鉴别

用户在第一次使用时，操作系统应对用户配置标识，且在整个生命周期内实现标识唯一，保证终端所有使用行为可追溯到用户主体。

在用户执行任何与操作系统安全功能相关操作之前应对用户进行鉴别。

鉴别信息应是不可见的，应采用加密方法对鉴别信息的存储进行安全保护。

当用户执行鉴别失败达到操作系统预定义阈值时，系统应采取安全措施执行鉴别失败处理。

5.2.5 访问控制

终端应提供访问控制机制，防止用户或应用软件非授权访问终端应用软件、数据等资源。

文件访问属性应至少包括读、写、执行等；访问方式包括本地和远程两种方式。

访问控制策略应按照预定义方式执行，仅授权用户可以更改，宜采用安全策略模型实现强制访问控制。

5.2.6 权限控制

若终端除预置应用软件外，还可安装其他应用软件，则终端应为授权用户提供权限控制机制，防止非预置应用软件非授权访问终端敏感 API。

权限控制应包括但不限于拨打电话、发送短信、定位、拍照、录音、访问通讯录等，且控制策略应至少包括允许和拒绝，且用户可以更改。

5.2.7 安全域隔离

终端应对系统资源及各类数据进行安全域划分，不同安全域之间应有相应的安全策略，安全域之间的安全策略应通过相应的访问控制机制实现。

5.2.8 日志审计

终端应支持生成审计记录，审计内容应包括日期、对象、描述和结果等。

终端应提供审计记录保护机制，能够生成、维护及保护审计过程，使其免遭修改、非法访问及破坏。

审计记录应仅支持授权管理员访问。

5.2.9 系统安全性

具有融合功能的移动终端应及时修复已知安全漏洞，应不具明显的严重漏洞，宜保证终端不具有 CNVD 或 CNNVD 所公布的 6 个月以前的高危及以上漏洞，防止终端遭受恶意软件攻击。

5.2.10 升级更新

终端应提供升级更新功能，且能够对更新来源进行鉴别，并对更新文件完整性进行校验，防止非授权更新。

应具有原始数据备份能力，且安全属性在升级前后保持一致。

应能够进行必要的回滚操作，避免更新失败导致系统失效。

5.2.11 软件安全

5.2.11.1 应用软件来源

支持融合功能的应用软件应预置于具有融合功能的移动终端内，或仅可从授权渠道实现应用的下载、部署和更新。

5.2.11.2 应用软件签名

应用软件应采用签名认证机制，终端应可识别应用软件签名状态，仅可安装经过用户授权或经过签名认证的应用软件。

5.2.11.3 应用软件安全

支持融合功能的应用软件应采取必要的安全机制，防止软件被逆向分析，应至少包括反编译、反盗版防护，相关要求见 YD/T 3228—2017 中 6.5.1 的内容。

5.2.11.4 身份鉴别认证

支持融合功能的应用软件，操作涉及用户个人信息时，在操作之前应支持必要的身份认证、登陆鉴权环节，防止非授权用户擅自使用融合功能。

在进行高风险敏感业务操作(例如支付类业务)前,宜采用多种认证方式进行多次认证,例如短信验证码、动态口令、生物特征等方式保证业务安全。

5.2.11.5 最小化权限

终端预置应用软件应在业务范围内申请和使用系统权限和资源,防止应用软件权限滥用。

支持融合功能的应用软件应对不同用户可使用的业务进行分权管理,采用权限最小化原则,避免用户权限滥用发生。

5.3 通信连接安全

5.3.1 网络接入安全

具有融合功能的移动终端应支持安全协议在终端侧的实现。支持接入网络中的鉴权和认证、加密传输等安全扩展功能,协议安全性应符合相应国家标准或行业标准。

应支持相应融合功能协议在终端侧的实现,协议安全部分应符合相应国家或行业标准。

5.3.2 外围接口安全

终端不应存在未经声明的外围接口。

当终端外围接口(包括但不限于 WLAN、蓝牙、NFC、USB、SD)建立数据连接及传输时,终端应能够发现并提示用户状态,保证连接的可执性和可控性。

宜禁用或授权使用终端闲置的物理端口,同时应禁用终端的外接存储设备自启动功能。

5.3.3 数据传输完整性

具有融合功能的移动终端与融合功能平台的通信数据应采用完整性检验机制,保证数据传输完整性,且具有通信时延和中断处理机制。

5.3.4 数据传输保密性

具有融合功能的移动终端与融合功能平台的通信数据应提供加密传输功能,所采用的加密算法,应符合国家或行业相关标准规定;与融合功能平台的通信信道宜与公开网络逻辑隔离,保证数据传输通道的保密性。

5.3.5 数据传输健壮性

具有融合功能的移动终端应正确处理融合功能相关信息,当接收到非法信息时应及时响应,并采用相应技术处理,防止拒绝服务攻击等异常情况发生。

5.4 个人信息安全

5.4.1 个人信息采集

具有融合功能的移动终端设备对个人信息的采集应在提供业务服务的同时进行,需要收集个人信息时,应在收集前明示收集的目的和范围,并且只有在用户同意的情况下方可继续。

5.4.2 个人信息存储

当个人信息存储在终端内部时,应为数据文件提供访问控制机制,防止未授权访问。存储账户设置类、传感采集类、金融支付类数据时,应采用密文方式存储。个人信息类型定义见 YD/T 3082—2016。

5.4.3 个人信息加工

具有融合功能的移动终端加工个人信息前，应明示加工数据的目的和范围，并提供访问控制机制，对数据设置适当操作权限，防止未经授权的访问和操作。应对传感采集类数据采取适当的脱敏措施加工后进行存储，避免存储其原始数据。

5.4.4 个人信息转移

具有融合功能的移动终端进行个人信息转移应按照约定目的和用途进行，传输数据之前应对双方进行身份认证和授权。若通过公共网络传输账户设置类、传感采集类、金融支付类个人信息时，应采用数字签名等技术手段保证数据的完整性和抗抵赖性，同时应采用密文方式传输。宜先对个人信息进行脱敏加工，消除能够识别特定个体的所有数据字段后再进行转移。

5.4.5 个人信息删除

具有融合功能的移动终端应提供删除功能，允许授权用户自行删除其在终端内保存的信息通信类、使用记录类、账户设置类、传感采集类、金融支付类信息。对于传感采集类，金融支付类信息应提供彻底删除选项，允许授权用户彻底删除相关信息。

参 考 文 献

[1] GB/T 34976—2017 信息安全技术 移动智能终端操作系统安全技术要求和测试评价方法
[2] GY/T 289—2015 NGB有线智能融合终端总体架构
[3] YD/T 2407 移动智能终端安全能力技术要求
[4] YD/T 2408 移动智能终端安全能力测试方法
[5] YD/T 2674—2013 移动智能终端信息安全设计导则