



中华人民共和国国家标准

GB/T 35278—2026

代替 GB/T 35278—2017

网络安全技术 移动终端安全技术规范

Cybersecurity technology—Technical specifications for mobile terminal security

2026-07-30 发布

2027-02-01 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.....Ⅲ

1 范围.....1

2 规范性引用文件.....1

3 术语、定义和缩略语.....1

 3.1 术语和定义.....1

 3.2 缩略语2

4 概述.....3

 4.1 TOE 介绍.....3

 4.2 TOE 安全特性.....5

5 安全问题.....5

 5.1 资产.....5

 5.2 威胁主体.....6

 5.3 安全威胁.....6

 5.4 组织安全策略.....7

 5.5 假设.....7

6 安全目的.....7

 6.1 移动终端安全目的.....7

 6.2 环境安全目的.....8

7 扩展组件.....8

 7.1 族 FCS_CKH_EXT.....8

 7.2 族 FCS_CKM_EXT.....9

 7.3 族 FPT_AEX_EXT.....10

 7.4 族 FPT_JTA_EXT.....11

 7.5 族 FPT_SEE_EXT.....12

 7.6 族 FPT_STG_EXT.....12

 7.7 族 FPT_TST_EXT.....13

 7.8 族 FPT_TUD_EXT.....14

8 安全要求.....15

 8.1 安全功能要求.....15

 8.2 安全保障要求.....37

9 测试评估方法.....39

 9.1 安全功能要求的测试方法.....39

 9.2 安全保障要求的评估方法58

9.3 脆弱性评估测试细则60

10 基本原理.....74

10.1 安全目的基本原理.....74

10.2 安全要求的基本原理.....77

10.3 组件依赖关系.....80

附录 A（资料性） 用户数据保护和密钥层次结构.....85

A.1 用户数据保护.....85

A.2 密钥层次结构85

参考文献.....87

前 言

本文件按照 GB/T 1.1—2020《标准化工作导则 第 1 部分：标准化文件的结构和起草规则》的规定起草。

本文件代替 GB/T 35278—2017《信息安全技术 移动终端安全保护技术要求》，与 GB/T 35278—2017 相比，除结构调整和编辑性改动外，主要技术变化如下：

- a) 更改了“概述”，明确了评估对象 TOE 的范围及 TOE 所处的网络环境(见第 4 章,2017 年版的第 4 章)；
- b) 增加了“资产”“威胁主体”“组织安全策略”相关内容(见 5.1、5.2、5.4)；
- c) 增加了“安全威胁”中的“非授权访问(T.UNAUTHACCESS)”“授权用户的恶意行为(T.ACCESSMALICIOUS)”“残余信息利用(T.RESIDUALDATA)”“完整性破坏(T.INTDESTROY)”“设备仿冒(T.DEVSPLOOF)”相关内容(见 5.3.1、5.3.2、5.3.5、5.3.6、5.3.8)；
- d) 更改了“安全威胁”中的“数据传输窃听(T.EAVESDROP)”“物理访问(T.PHYSICAL)”“恶意应用软件(T.MALICIOUSAPP)”相关内容(见 5.3.3、5.3.4、5.3.7,2017 年版的 5.2.1、5.2.3、5.2.4)；
- e) 更改了“假设”相关内容(见 5.5,2017 年版的 5.1.1、5.1.2)；
- f) 增加了“安全目的”中的“事件审计(O.AUDIT)”“访问控制(O.ACTROL)”“加密保护(O.ENCRYPTO)”“安全擦除(O.INFOERASE)”“会话管理(O.SESSIONMANAG)”“设备鉴别(O.DEVAUTH)”“隐私保护(O.PRIVACY)”等相关内容(见 6.1.1、6.1.3~6.1.5、6.1.7、6.1.9、6.1.10)；
- g) 更改了“安全目的”中的“身份鉴别(O.AUTH)”“安全通信(O.SECCOM)”“完整性保护(O.INTEGRITY)”相关内容(见 6.1.2、6.1.6、6.1.8,2017 年版的 6.1.1、6.1.4、6.1.5)；
- h) 更改了“环境安全目的”中的“物理安全(OE.PHYSICAL)”“人员(OE.PERSONNEL)”“远程设备安全(OE.REMOTE)”相关内容(见 6.2.1、6.2.2、6.2.3,2017 年版的 6.2.1、6.2.2)；
- i) 增加了“扩展组件”相关内容，包括“族 FCS_CKH_EXT”“族 FCS_CKM_EXT”“族 FPT_AEX_EXT”“族 FPT_JTA_EXT”“族 FPT_SEE_EXT”“族 FPT_STG_EXT”“族 FPT_TST_EXT”“族 FPT_TUD_EXT”等相关内容(见第 7 章)；
- j) 更改了“安全功能要求”中的“概述”“FAU 类：安全审计”“FCS 类：密码支持”“FDP 类：用户数据保护”“FIA 类：标识和鉴别”“FMT 类：安全管理”“FPT 类：TSF 保护”“FTA 类：TOE 访问”“FTP 类：可信路径/信道”相关内容(见 8.1.1~8.1.6、8.1.8~8.1.10,2017 年版的第 7 章)；
- k) 增加了“安全功能要求”中的“FPR 类：隐私”相关内容(见 8.1.7)；
- l) 更改了“安全保障要求”中的“概述”“ADV 类”“AGD 类”“ALC 类”“ASE 类”“ATE 类”“AVA 类”(见 8.2,2017 年版的第 8 章)；
- m) 增加了“测试评估方法”(见第 9 章)；
- n) 更改了“基本原理”中的“安全目的基本原理”“安全要求的基本原理”相关内容(见 10.1、10.2,2017 年版的第 9 章)；
- o) 增加了“组件依赖关系”(见 10.3)。

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专利的责任。

本文件由全国信息安全标准化技术委员会(SAC/TC 260)提出并归口。

本文件起草单位：中国信息通信研究院、中国网络安全审查认证和市场监管大数据中心、北京邮电大学、中国移动通信集团有限公司、嘉兴嘉赛信息技术有限公司、华为终端有限公司、维沃移动通信有限公司、北京小米移动软件有限公司、高通无线通信技术(中国)有限公司、OPPO 广东移动通信有限公司、荣耀终端股份有限公司、中讯邮电咨询设计院有限公司。

本文件主要起草人：袁琦、田琛、邹仕洪、王峰、莊敏、刘小丽、张宏星、邱勤、衣强、翟世俊、王键、贾科、姚一楠、吴越、杜志敏、郑琛、安媛媛、徐思嘉、王江胜、李腾、李根、赵晓娜、侯玉华、宁静。

本文件及其所代替文件的历次版本发布情况为：

——2017 年首次发布为 GB/T 35278—2017；

——本次为第一次修订。

网络安全技术 移动终端安全技术规范

1 范围

本文件给出了移动终端的安全问题、安全目的和扩展组件,规定了移动终端的安全要求,并描述了对应的测试评估方法。

本文件适用于移动终端产品的设计、开发、制造、应用和测试。

2 规范性引用文件

下列文件中的内容通过文中的规范性引用而构成本文件必不可少的条款。其中,注日期的引用文件,仅该日期对应的版本适用于本文件;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。

GB/T 18336.3—2024 网络安全技术 信息技术安全评估准则 第3部分:安全保障组件

GB/T 32915—2016 信息安全技术 二元序列随机性检测方法

3 术语、定义和缩略语

3.1 术语和定义

下列术语和定义适用于本文件。

3.1.1

移动终端 mobile terminal

可移动的便携式计算设备。

注:移动终端包括带有无线上网功能的智能移动通信终端、平板式计算机、便携式计算机。

[来源:GB/T 25069—2022,3.7.19]

3.1.2

应用软件 application software

移动终端操作系统之外,向用户提供服务功能的软件。

[来源:GB/T 30284—2020,3.1.2]。

3.1.3

鉴别数据 authentication data

用于验证用户所声称身份的信息。

[来源:GB/T 30284—2020,3.1.3]。

3.1.4

授权用户 authorized user

依据安全策略可执行某项操作的用户。

[来源:GB/T 30284—2020,3.1.4]。

3.1.5

数字签名 digital signature

附加在数据单元上的一些数据,或是对数据单元做密码变换,这种附加数据或密码变换被数据单

元的接收者用以确认数据单元的来源和完整性,达到保护数据,防止被人(例如接收者)伪造的目的。

[来源:GB/T 25069—2022,3.576,有修改]

3.1.6

资源 resource

一组有限的逻辑或物理实体。

注:操作系统为用户、主体和客体分配或管理资源,如存储空间、电源、CPU、无线通信设备等。

[来源:GB/T 30284—2020,3.1.5]

3.1.7

会话 session

用户与 TSF 的一段交互。

注:会话建立受控于多种因素,如用户鉴别、对 TOE 访问的时间和方法及允许建立会话的最大数等。

[来源:GB/T 30284—2020,3.1.6]

3.1.8

TOE 安全功能 TOE security functionality

正确执行安全功能要求所依赖的 TOE 的所有硬件、软件和固件的组合功能。

[来源:GB/T 30284—2020,3.1.8,有修改]

3.1.9

可信信道 trusted channel

TSF 同远程可信 IT 产品能在必要的信任基础上进行通信的一种通信手段。

[来源:GB/T 30284—2020,3.1.9]

3.1.10

TSF 数据 TSF data

实施移动终端操作系统安全功能所依赖的数据。

[来源:GB/T 30284—2020,3.1.11]

3.1.11

用户数据 user data

由用户产生或为用户服务的数据。

[来源:GB/T 25069—2022,3.736]

3.2 缩略语

下列缩略语适用于本文件。

AES:高级加密标准(advanced encryption standard)

ARM:高级精简指令集机器[advanced RISC(reduced instruction set computer) machine]

CPU:中央处理器(central processing unit)

DRAM:动态随机存取存储器(dynamic random access memory)

DRBG:确定性随机位生成器(deterministic random bit generator)

EAL:评估保障级(evaluation assurance level)

ECDSA:椭圆曲线数字签名算法(elliptic curve digital signature algorithm)

FAR:错误接受率(false acceptance rate)

FRR:错误拒绝率(false rejection rate)

HKDF:基于 HMAC 的密钥派生函数(HMAC-based key derivation function)

HMAC-SHA2:基于散列的消息认证码-安全散列算法(hash-based message authentication code-se-

cure hash algorithm 2)

IMEI:国际移动设备识别码(international mobile equipment identity)

ID:身份标识(identity)

JOP:面向跳转的编程(jump-oriented programming)

JTAG:联合测试行动组(joint test action group)

KBKDF:基于密钥的密钥派生函数(key-based key derivation function)

MAC:消息认证码(message authentication code)

NFC:近场通信(near field communication)

PBKDF:基于口令的密钥派生函数(password-based key derivation function)

PIN:个人识别码(personal identification number)

REE:富执行环境(rich execution environmen)

ROM:只读存储器(read-only memory)

ROP:面向返回的编程(return-oriented programming)

RSA:RAS 公钥密码算法(rivest-shamir-adleman)

SFP:安全功能策略(security function policy)

SHA2:安全散列算法 2(secure hash algorithm 2)

SHA3:安全散列算法 3(secure hash algorithm 3)

SM:商用密码(shangmi)

SN:序列号(serial number)

SRAM:静态随机存取存储器(static random access memory)

SOC:片上系统(system on a chip)

SQL:结构化查询语言(structured query language)

ST:安全目标(security target)

TLS:传输层安全(transport layer security)

TOE:评估对象(target of evaluation)

TSF:TOE 安全功能(TOE security functionality)

UART:通用异步收发传输器(universal asynchronous receiver/transmitter)

UI:用户界面(user interface)

UID:唯一标识符(unique identifier)

USB:通用串行总线(universal serial bus)

VPN:虚拟专用网(virtual private network)

Web:万维网(world wide web)

XSS:跨站脚本(cross-site scripting)

2D:二维(two-dimensional)

3D:三维(three-dimensional)

4 概述

4.1 TOE 介绍

4.1.1 TOE 组成

TOE 由移动终端中的硬件平台、操作系统及不可卸载预置应用软件组成,见图 1,具体如下:

- a) 硬件平台包括处理器、传感器和各种接口等,不包括用户可移除的任何组件及存储在这些组件上的数据以及与这些组件相关的服务,例如可插拔存储卡等;
- b) 操作系统是移动终端的组成部分,用于控制、管理移动终端上的硬件,如处理器、内存、输入/输出设备和传感器等,同时提供用户操作界面和应用软件开发接口;
- c) 不可卸载预置应用软件指预置在移动终端中实现移动终端基本功能的应用软件。

移动终端中可卸载预置应用软件和用户安装应用软件不属于 TOE 范围,可卸载预置应用软件是指预置在移动终端中的可卸载应用软件,用户安装应用软件指用户使用移动终端过程中安装的应用软件。

TOE 可提供无线连接,可包括提供电子邮件、网络 and VPN 连接功能的软件,用于访问数据、实现服务和与其他移动终端通信。

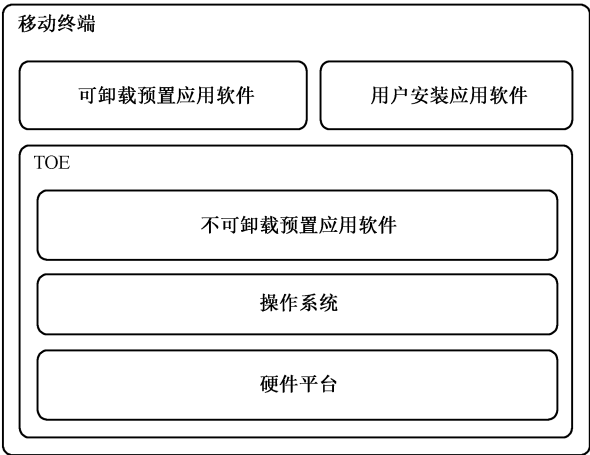


图 1 TOE 组成

4.1.2 TOE 与其他实体的交互关系

TOE 与其他实体的交互关系见图 2,具体如下。

- a) TOE 通过蜂窝网络和/或无线局域网访问远程服务端环境提供的服务,远程服务端环境中的 IT 实体包括系统升级服务器、应用分发平台和其他远程服务平台。
 - 1) 系统升级服务器为 TOE 提供操作系统软件的更新服务,这些系统升级包通常由 TOE 厂商进行签名后部署在系统升级服务器上,由 TOE 进行下载、校验和安装。
 - 2) 应用分发平台负责应用软件的上架审核,以及应用软件的下载和更新等服务。
 - 3) TOE 通过接口实现其他远程服务平台提供的服务,包括数据备份服务、企业服务和游戏服务等。在本地环境中,用户通过 TOE 提供的触摸屏或物理按键与 TOE 进行物理交互。
- b) TOE 可与其他终端设备进行鉴别后建立安全通信连接并进行交互。
- c) TOE 可通过触摸屏或物理按键与用户进行交互。

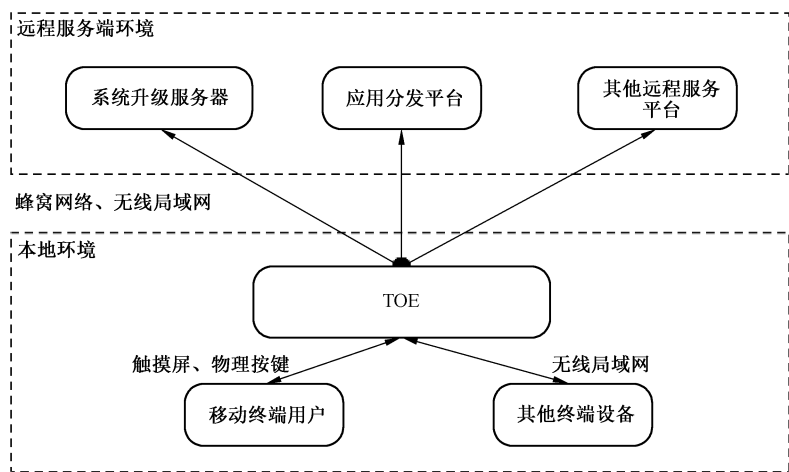


图 2 TOE 与其他实体的交互关系

4.2 TOE 安全特性

针对 TOE 的网络环境,TOE 需要抵御的威胁主要来自非授权用户的访问、授权用户的恶意访问、其他终端设备的非法访问、应用程序的非法访问和互联网非授权实体的访问。TOE 具备以下安全特性。

- a) 用户的身份鉴别:TOE 为用户提供口令鉴别、生物信息鉴别等身份鉴别机制,只有通过身份鉴别的合法用户才能操作或访问 TOE,部分紧急的服务除外,如紧急呼叫。
- b) 设备的身份鉴别:TOE 与其他终端设备(如智能穿戴设备、智能家居设备等)建立连接前,首先对其他终端设备的身份进行鉴别,鉴别通过后才能与其他终端设备建立安全通信。

注:与 TOE 建立连接的其他终端设备为对端设备。

- c) 隐私保护:TOE 提供设备身份脱敏机制,为应用开发者和广告厂商提供可重置设备标识符,防止应用开发者和广告厂商跟踪用户,保护用户隐私安全。
- d) 数据安全:TOE 为数据的存储、传输和使用分别提供加密存储、安全传输和访问控制等安全机制,防止数据被篡改或泄露或非法访问。
- e) 系统安全:TOE 对启动链镜像的完整性和合法性进行校验,实现启动安全;通过强制访问控制、自主访问控制、防漏洞利用和完整保护等安全机制提供 TOE 自身和其他应用软件安全,防止被恶意应用或攻击者入侵,同时对用户的安全操作进行审计,实现运行安全;并通过对系统更新包的完整性和合法性进行验证,以及修复已知漏洞来实现系统更新安全;TOE 支持对应用软件进行完整性验证的系统能力。
- f) 硬件安全:TOE 提供硬件安全机制,保护可信启动根、安全存储根安全,以及用于密钥保护或派生的数据和其他敏感数据不被攻击者物理读取或篡改。

5 安全问题

5.1 资产

应保护的 TOE 资产包括以下内容:

- a) TSF 数据:包括系统镜像、系统升级包、访问控制策略、安全配置数据、预置的签名校验证书、根密钥和加密密钥、审计数据和身份鉴别数据等;
- b) 用户数据:由用户产生或为用户服务的数据,如用户通讯录、通话记录、短信、位置信息、健康

数据、多媒体影音数据和日程表数据等；

- c) 敏感资源:包含敏感应用软件开发接口、网络接口、JTAG 接口、USB 接口、内存和外设资源,如摄像头、位置传感器和传声器等。

注: ST 作者根据具体的应用情况细化对资产的描述。

5.2 威胁主体

威胁主体为根据 TOE 的网络环境,施加不利行为的实体。给出如下威胁主体:

- a) TA.LOCAL:在 TOE 附近的威胁主体,可通过本地无线接口访问 TOE;
- b) TA.REMOTE:可通过广域网接口访问 TOE 的威胁主体;
- c) TA.PHYSAL:对 TOE 具有物理访问权限的威胁主体,如通过物理接口访问 TOE;
- d) TA.FLAWAPP:用户在 TOE 上安装的恶意或编程不良的应用软件,可访问 TOE 的应用软件开发接口,还可访问 TOE 本地无线网络接口和/或广域网络接口。

5.3 安全威胁

5.3.1 非授权访问(T.UNAUTHACCESS)

TA.LOCAL、TA.REMOTE、TA.PHYSAL 或 TA.FLAWAPP 非授权用户或进程访问 TOE 的 TSF 数据、用户数据或敏感资源,并对 TSF 数据、用户数据或敏感资源的数据和安全功能进行恶意操作。

5.3.2 授权用户的恶意行为(T.ACCESSMALICIOUS)

TA.PHYSAL 对 TOE 进行不正确的配置,或恶意利用权限对 TSF 数据、用户数据或敏感资源进行非法操作,使 TOE 安全受到威胁。

5.3.3 数据传输窃听(T.EAVESDROP)

TA.LOCAL、TA.REMOTE 或 TA.FLAWAPP 可能监听或篡改 TOE 与其他实体之间的传输的用户数据和 TSF 数据,造成用户数据和 TSF 数据的泄露或被篡改。

5.3.4 物理访问(T.PHYSICAL)

TA.PHYSAL 尝试通过访问 TOE 的物理接口来访问资产,或尝试通过猜测口令和/或仿冒生物信息技术,从而获得对用户数据资产的访问权限。物理接口包括 JTAG 接口、USB 接口、充电接口以及直接访问 TOE 存储媒体的物理接口。

5.3.5 残余信息利用(T.RESIDUALDATA)

用户出售其 TOE 并尝试事先删除所有用户数据资产,TA.PHYSAL 可能利用 TOE 残留信息的处理缺陷,在执行过程中对未删除的残留信息进行利用,以获取 TSF 数据或用户数据等敏感信息或滥用 TOE 的安全功能。

5.3.6 完整性破坏(T.INTDESTROY)

TA.PHYSAL 通过攻击、篡改 TOE 的 TSF 数据或可执行代码,破坏 TOE 的完整性,导致安全功能对于 TSF 数据或用户数据资产保护的安全机制不再正常工作。

5.3.7 恶意应用软件(T.MALICIOUSAPP)

TA.FLAWAPP 尝试越权访问用户数据和系统敏感资源,窃取用户数据或修改 TOE 的关键

配置。

5.3.8 设备仿冒(T.DEVSPOOF)

TA.LOCAL、TA.REMOTE 或 TA.PHYSAL 创建恶意设备、欺骗 TOE、连接到 TOE,恶意设备伪装成受信任的对端设备访问用户数据,造成 TOE 功能被滥用或用户数据被泄露。

5.4 组织安全策略

移动终端密码的使用应符合国家、行业或组织要求的密码管理相关标准。

5.5 假设

5.5.1 物理安全(A.PHYSICAL)

假设移动终端运行所依赖的运行环境能符合移动终端安全运行的所需的物理保护。

5.5.2 人员(A.PERSONNEL)

假设移动终端的合法用户能按管理员指南管理移动终端的安全功能,对移动终端不存在恶意的破坏企图。

5.5.3 远程设备安全(A.REMOTE)

假设用于管理移动终端的远程 IT 设备和应用设备是安全的。

5.5.4 会话冒用(T.SSIONSPOOF)

TA.PHYSAL 尝试利用不被使用的会话,假冒授权用户对 TOE 的 TSF 数据和用户数据进行恶意操作。

6 安全目的

6.1 移动终端安全目的

6.1.1 事件审计(O.AUDIT)

TOE 应记录安全相关的事件,应对记录的事件进行保护并只限授权用户查看。TOE 应保证审计数据已满的情况下,不影响审计功能和其他安全功能的执行。

6.1.2 身份鉴别(O.AUTH)

TOE 应提供鉴别用户身份的机制,并在用户使用 TOE 功能前对用户身份进行鉴别和标识。TOE 应只提供有限的鉴别反馈信息,并在鉴别失败达到一定次数时限制用户的鉴别行为。

6.1.3 访问控制(O.ACTROL)

TOE 应提供访问控制机制,防止移动终端 TSF 数据、用户数据或敏感资源等在未授权情况下被访问、修改或删除。

6.1.4 加密保护(O.ENCRYPTO)

TOE 应提供加解密机制,利用加密措施对其保护的 TSF 数据和用户数据资产进行安全存储。

6.1.5 安全擦除(O.INFOERASE)

TOE 应保证重要的数据资产在使用完成后会被删除或被安全处理,不应留下可被攻击者利用的残留数据信息。

6.1.6 安全通信(O.SECCOM)

TOE 应提供通过受保护的通道向远程可信 IT 产品提交用户数据的能力,同时也提供受保护的网络通道供可信应用使用。

6.1.7 会话管理(O.SESSIONMANAG)

TOE 应临时暂停不被使用的用户会话,并只有在重新鉴别用户身份后才可恢复已暂停的用户会话。

6.1.8 完整性保护(O.INTEGRITY)

TOE 应提供完整性保护机制,防止系统镜像、升级包、内核等 TOE 关键 TSF 数据被非法篡改以及 TOE 的安全功能被绕过。

6.1.9 设备鉴别(O.DEVAUTH)

TOE 应提供对端设备的身份鉴别机制,在通信连接之前应对对端设备进行身份鉴别,并允许这些设备对 TOE 进行身份鉴别。

6.1.10 隐私保护(O.PRIVACY)

TOE 应提供身份脱敏机制,为应用开发者和广告厂商提供可重置设备标识符,防止应用开发者和广告厂商跟踪用户,使得应用开发者或广告厂商收集的用户数据不能与 TOE 的固定设备标识符绑定,保护用户隐私安全。

6.2 环境安全目的

6.2.1 物理安全(OE.PHYSICAL)

移动终端运行所依赖的运行环境应提供符合移动终端安全运行所需的物理保护。

6.2.2 人员(OE.PERSONNEL)

移动终端的合法用户能按操作指南来管理移动终端的安全功能,对移动终端不存在恶意的破坏企图。

6.2.3 远程设备安全(OE.REMOTE)

移动终端的远程管理设备、应用商店等远程 IT 实体是安全的且其数据和用户信息是被保护的。

7 扩展组件

7.1 族 FCS_CKH_EXT

7.1.1 族行为

本族给出用户数据加密保护的密钥层次,用于描述不同级别用户数据加密保护相关的密钥是如何

派生和保护。密钥层次结构中的某些密钥用作数据加密密钥,其他密钥用于加密和/或派生密钥层次中的其他密钥。

7.1.2 组件层次

本族的组件层次见图 3。

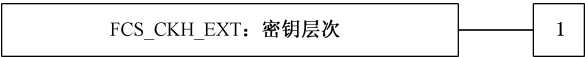


图 3 FCS_CKH_EXT:组件层次

FCS_CKH_EXT.1 密钥层次,应给出用户数据保护的密钥层次结构以及如何派生和/或保护密钥层次结构中的密钥。

7.1.3 管理

尚无预见的管理活动。

7.1.4 审计

尚无预见的可审计事件。

7.1.5 FCS_CKH_EXT.1 密钥层次

从属于:无其他组件。

依赖关系:[FCS_CKM.1/Symmetric 密钥生成或 FCS_CKM.1/Asymmetric,FCS_CKM.5];
FCS.COP.1/ENCRYPT 密码运算。

FCS_CKH_EXT.1.1 TSF 应支持用于【赋值:受密钥层次结构保护的数据资产列表】保护的数据加密密钥的密钥层次结构。

FCS_CKH_EXT.1.2 TSF 应根据【赋值:密钥生成和/或派生算法、密钥长度和标准列表】来派生和/或生成密钥层次中的所有密钥,实现密钥层次结构中的密钥直接或间接使用根密钥和【选择:用户鉴别凭据、无用户鉴别凭据】对【赋值:用户数据资产列表】的数据加密密钥进行保护。

FCS_CKH_EXT.1.3 TSF 应根据【赋值:描述密钥层次中密钥或数据的保护规则】对密钥层次结构中的所有密钥和用于派生密钥层次结构中密钥的所有数据进行保护。

注 1: FCS_CKH_EXT.1.2 中的选择规定了用户鉴别凭证是否参与用户数据资产的保护。设备根密钥用于将密钥层次结构绑定到唯一设备;用户鉴别凭据将用户数据资产数据绑定到用户,将用户鉴别凭据作为密钥层次中密钥派生的一部分,只有在用户进行身份鉴别后才能访问绑定到用户鉴别凭据的用户数据。

注 2: 【】中的内容用于 ST 作者进行选择或赋值的操作。

FCS_CKH_EXT.1.3 中的赋值可使用 FCS_CKH_EXT.1.1 中密钥层次中的密钥和 FCS_COP.1 中的算法对密钥进行加密存储、使用后删除密钥并在需要时重新生成或派生密钥或使用隔离执行环境对密钥进行存储。

7.2 族 FCS_CKM_EXT

7.2.1 族行为

本族给出根密钥保护的要求。

7.2.2 组件层次

本族的组件层次见图 4。

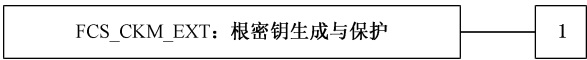


图 4 FCS_CKM_EXT:组件层次

FCS_CKM_EXT.1 根密钥保护,TSF 应支持受硬件保护的根密钥,保存在硬件中无法篡改。

7.2.3 管理

尚无预见的管理活动。

7.2.4 审计

尚无预见的可审计事件。

7.2.5 FCS_CKM_EXT.1 根密钥保护

从属于:无其他组件。

依赖关系:无依赖关系。

FCS_CKM_EXT.1.1 TSF 应支持受硬件保护的根密钥,保存在 TOE 硬件中安全存储区域无法篡改,仅隔离执行环境中的软件可通过硬件密码引擎进行访问。

7.3 族 FPT_AEX_EXT

7.3.1 族行为

本族给出漏洞防利用的要求,用于抵抗常见的漏洞被利用的攻击。

7.3.2 组件层次

本族的组件层次见图 5。

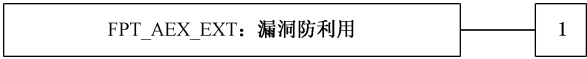


图 5 FPT_AEX_EXT:组件层次

FPT_AEX_EXT.1 地址空间布局随机化,TSF 应支持地址空间布局随机化。

FPT_AEX_EXT.2 内存页权限控制,TSF 应对物理内存执行访问控制。

FPT_AEX_EXT.3 缓冲区溢出保护,TSF 应执行缓冲区溢出保护机制。

FPT_AEX_EXT.4 内核完整性保护,TSF 应提供内核完整性保护机制。

FPT_AEX_EXT.5 控制流完整性保护,TSF 应提供控制流完整性保护机制。

7.3.3 管理

尚无预见的管理活动。

7.3.4 审计

尚无预见的可审计事件。

7.3.5 FPT_AEX_EXT.1 地址空间布局随机化

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_AEX_EXT.1.1 TSF 应为应用软件提供地址空间布局随机化机制。
FPT_AEX_EXT.1.2 TSF 应为内核提供地址空间布局随机化机制。

7.3.6 FPT_AEX_EXT.2 内存页权限控制

从属于:无其他组件。
依赖关系:无依赖关系。

FPT_AEX_EXT.2.1 TSF 应提供以下物理内存保护机制:【选择:数据不可执行、特权模式不可执行、特权模式不可访问、可写内存不可执行、内存只可执行、【赋值:其他内存保护机制】】。

7.3.7 FPT_AEX_EXT.3 缓冲区溢出保护

从属于:无其他组件。
依赖关系:无依赖关系。

FPT_AEX_EXT.3.1 TSF 应提供以下缓冲区溢出保护机制:【选择:基于栈的缓冲区溢出保护、基于堆的缓冲区溢出保护】。

7.3.8 FPT_AEX_EXT.4 内核完整性保护

从属于:无其他组件。
依赖关系:无依赖关系。

FPT_AEX_EXT.4.1 TSF 应提供以下内核完整性保护机制:【选择:内核代码段只读保护、内核数据段不可执行、系统控制寄存器写保护、强制访问控制策略防篡改、【赋值:其他内核完整性保护机制】】。

7.3.9 FPT_AEX_EXT.5 控制流完整性保护

从属于:无其他组件。
依赖关系:无依赖关系。

FPT_AEX_EXT.5.1 TSF 应提供以下控制流完整性保护机制:【选择:前向控制流完整性、后向控制流完整性、指针鉴别、【赋值:其他控制流完整性保护机制】】。

7.4 族 FPT_JTA_EXT

7.4.1 族行为

本族给出 JTAG 接口访问限制的要求。

7.4.2 组件层次

本族的组件层次见图 6。



图 6 FPT_JTA_EXT:组件层次

FPT_JTA_EXT.1 JTAG 接口管控,应指定 TSF 用于限制访问其 JTAG 接口的机制。

7.4.3 管理

尚无预见的管理活动。

7.4.4 审计

尚无预见的可审计事件。

7.4.5 FPT_JTA_EXT.1 JTAG 接口管控

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_JTA_EXT.1 TSF 应支持【选择:通过硬件断开物理连接、通过签名密钥进行接入鉴别】对 JTAG 接口进行访问控制。

7.5 族 FPT_SEE_EXT

7.5.1 族行为

本族给出与操作系统运行环境隔离的执行环境的要求。

7.5.2 组件层次

本族的组件层次见图 7。

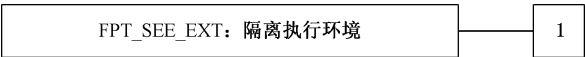


图 7 FPT_SEE_EXT:组件层次

FPT_SEE_EXT.1 隔离执行环境,TSF 应提供隔离的执行环境。

7.5.3 管理

尚无预见的管理活动。

7.5.4 审计

尚无预见的可审计事件。

7.5.5 FPT_SEE_EXT.1 隔离执行环境

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_SEE_EXT.1.1 TSF 应支持与操作系统运行的普通运行环境隔离的隔离执行环境:【赋值:描述隔离执行环境及其安全机制】。

7.6 族 FPT_STG_EXT

7.6.1 族行为

本族给出 TSF 数据存储的要求。

7.6.2 组件层次

本族的组件层次见图 8。



图 8 FPT_STG_EXT:组件层次

FPT_STG_EXT.1 TSF 数据存储,应指定 TSF 数据存储的机制。

7.6.3 管理

尚无预见的管理活动。

7.6.4 审计

尚无预见的可审计事件。

7.6.5 FPT_STG_EXT.1 TSF 数据存储

从属于:无其他组件。

依赖关系:FCS_COP.1 密码运算。

FPT_STG_EXT.1.1 TSF 应为【赋值:其他 TSF 数据列表】的存储提供【选择:隔离执行环境、赋值【其他安全机制】】。

FPT_STG_EXT.1.2 TSF 应使用下述方法对【赋值:TSF 数据列表】进行加密:【赋值:密码算法】【赋值:密钥长度】。

FPT_STG_EXT.1.3 TSF 应使用下述方法对【赋值:TSF 数据列表】的完整性进行保护:【赋值:完整性校验方法】【赋值:密钥长度】。

7.7 族 FPT_TST_EXT

7.7.1 族行为

本族给出 TOE 启动阶段和正常运行阶段完整性校验的要求。

7.7.2 组件层次

本族的组件层次见图 9。

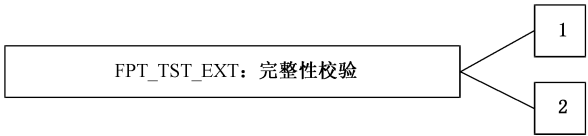


图 9 FPT_TST_EXT:组件层次

FPT_TST_EXT.1 启动完整性校验,TSF 应对启动过程的完整性进行校验。

FPT_TST_EXT.2 运行完整性校验,TSF 应对运行阶段的 TSF 组成部分或 TSF 数据的完整性进行校验。

7.7.3 管理

尚无预见的管理活动。

7.7.4 审计

尚无预见的可审计事件。

7.7.5 FPT_TST_EXT.1 启动完整性校验

从属于:无其他组件。
依赖关系:FCS_COP.1 密码运算。

FPT_TST_EXT.1.1 TSF 应从固化在不可篡改硬件中的启动可信根开始,使用 FCS_COP.1 中规定的密码算法逐级对启动链中的【赋值:启动加载的程序和镜像】进行签名校验,同时【赋值:完整性校验机制及校验公钥保护机制】。

7.7.6 FPT_TST_EXT.2 运行完整性校验

从属于:无其他组件。
依赖关系:FCS_COP.1 密码运算。

FPT_TST_EXT.2.1 TSF 应在正常工作期间周期性地运行自检程序以证明【赋值:TSF 的组成部分或 TSF 数据】能正确运行。

FPT_TST_EXT.2.2 TSF 应将自检程序运行在【选择:基于处理器隔离模式实现的隔离执行环境、基于处理器集成安全处理单元实现的隔离执行环境、基于独立安全处理单元实现的隔离执行环境】,检测到运行错误时应记录审计信息。

7.8 族 FPT_TUD_EXT

7.8.1 族行为

本族给出软件更新机制的相关要求。

7.8.2 组件层次

本族的组件层次见图 10。

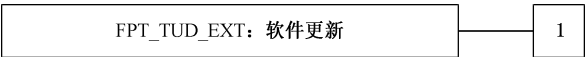


图 10 FPT_TUD_EXT:组件层次

FPT_TUD_EXT.1 软件更新,TSF 应对软件升级包的完整性进行校验。

7.8.3 管理

尚无预见的管理活动。

7.8.4 审计

尚无预见的可审计事件。

7.8.5 FPT_TUD_EXT.1 安全更新

从属于:无。
依赖关系:FCS_COP.1 密码运算。

FPT_TUD_EXT.1.1/OS TSF 应在安装【选择:TOE 系统软件、应用软件】更新包之前使用数字签名机制对【选择:TOE 系统软件、应用软件】更新包的签名进行验证。

FPT_TUD_EXT.1.2/OS TSF 应验证用于校验【选择:TOE 系统软件、应用软件】更新包数字签名的公钥【选择:与首次安装时存储在 TOE 中证书的公钥一致的公钥,为 TOE 中预置的不可篡改证书中的公钥】。

8 安全要求

8.1 安全功能要求

8.1.1 概述

移动终端的安全功能要求由 GB/T 18336.2 规定的组件及第 7 章规定的扩展组件组成,移动终端的安全功能要求组件见表 1。

表 1 安全功能要求组件

序号	组件分类	安全功能要求组件
1	FAU类:安全审计	FAU_GEN.1 审计数据产生
2		FAU_STG.2 受保护的审计数据存储
3		FAU_STG.5 防止审计数据丢失
4	FCS类:密码支持	FCS_CKH_EXT.1/Low 密钥层次
5		FCS_CKH_EXT.1/MediumHigh 密钥层次
6		FCS_CKM.1/Symmetric 密钥生成
7		FCS_CKM.1/Asymmetric 密钥生成
8		FCS_CKM.2 密钥分发
9		FCS_CKM.5 密钥派生
10		FCS_CKM.6 密钥销毁的时间和事件
11		FCS_CKM_EXT.1 根密钥保护
12		FCS_COP.1/SIGN 密码运算
13		FCS_COP.1/ENCRYPT 密码运算
14		FCS_COP.1/HASH 密码运算
15		FCS_COP.1/KEYHMAC 密码运算
16		FCS_RNG.1 随机数生成
17	FDP类:用户数据保护	FDP_ACC.1/MAC 子集访问控制
18		FDP_ACC.1/DAC 子集访问控制
19		FDP_ACC.1/SYSCALL 子集访问控制
20		FDP_ACC.1/Permission 子集访问控制
21		FDP_ACC.1/UserData 子集访问控制
22		FDP_ACC.1/SEE 子集访问控制
23		FDP_ACC.1/DTC 子集访问控制
24		FDP_ACF.1/MAC 基于安全属性的访问控制
25		FDP_ACF.1/DAC 基于安全属性的访问控制
26		FDP_ACF.1/SYSCALL 基于安全属性的访问控制
27		FDP_ACF.1/Permission 基于安全属性的访问控制

表 1 安全功能要求组件（续）

序号	组件分类	安全功能要求组件
28	FDP类:用户数据保护	FDP_ACF.1/UserData 基于安全属性的访问控制
29		FDP_ACF.1/SEE 基于安全属性的访问控制
30		FDP_ACF.1/DTC 基于安全属性的访问控制
31		FDP_RIP.2 完全残余信息保护
32		FDP_SDC.1 存储数据的机密性
33	FIA类:标识和鉴别	FIA_AFL.1 鉴别失败处理
34		FIA_SOS.1 秘密的验证
35		FIA_SOS.2 TSF 生成秘密
36		FIA_UAU.1 鉴别的时机
37		FIA_UAU.5/USER 多重鉴别机制
38		FIA_UAU.5/DEVICE 多重鉴别机制
39		FIA_UAU.5/APP 多重鉴别机制
40		FIA_UAU.6 重鉴别
41		FIA_UAU.7 受保护的鉴别反馈
42		FIA_UID.1 标识的时机
43		FIA_API.1 身份鉴别证明
44	FMT类:安全管理	FMT_MSA.1/Permission 安全属性的管理
45		FMT_MSA.3/Permission 静态属性初始化
46		FMT_SMF.1 管理功能
47	FPR类:隐私	FPR_PSE.1/APPDEV 假名
48		FPR_PSE.1/AD 假名
49	FPT类:TSF保护	FPT_AEX_EXT.1 地址空间布局随机化
50		FPT_AEX_EXT.2 内存页权限控制
51		FPT_AEX_EXT.3 缓冲区溢出保护
52		FPT_AEX_EXT.4 内核完整性保护
53		FPT_AEX_EXT.5 控制流完整性保护
54		FPT_FLS.1 失效即保持安全状态
55		FPT_JTA_EXT.1 JTAG 接口访问控制
56		FPT_PHP.3 物理攻击抵抗
57		FPT_RCV.2 自动恢复
58		FPT_SEE_EXT.1 隔离执行环境
59		FPT_STG_EXT.1 TSF 数据存储
60		FPT_STM.1 可靠的时间戳
61		FPT_TST_EXT.1 启动完整性验证

表 1 安全功能要求组件（续）

序号	组件分类	安全功能要求组件
62	FPT类:TSF保护	FPT_TST_EXT.2 运行完整性验证
63		FPT_TUD_EXT.1/OS 系统软件更新
64		FPT_TUD_EXT.1/APP 应用软件验证
65	FTA类:TOE访问	FTA_SSL.1 TSF 原发会话锁定
66		FTA_SSL.2 用户原发会话锁定
67	FTP类:可信路径/信道	FTP_ITC.1/TLS TSF 间可信信道
68		FTP_ITC.1/DEVICE TSF 间可信信道

8.1.2 FAU类:安全审计

8.1.2.1 FAU_GEN.1 审计数据产生

8.1.2.1.1 从属于:无其他组件。

依赖关系:FPT_STM.1 可信时间戳。

8.1.2.1.2 FAU_GEN.1.1 TSF 应能为下述可审计事件产生审计数据:

- a) 审计功能的开启和关闭;
- b) 系统开机与关机;
- c) 账号相关操作;
- d) 网络相关操作;
- e) 文件相关操作;
- f) 应用相关操作;
- g) 审计日志超限;
- h) 证书相关操作;
- i) 权限相关操作;
- j) 启动链镜像完整性校验结果;
- k) 正常工作过程关键镜像和可信应用完整性校验结果;
- l) 【赋值:其他可审计事件】。

8.1.2.1.3 FAU_GEN.1.2 TSF 应在每个审计记录中至少记录下列信息:

- a) 可审计事件的日期和时间、事件类型、主体身份(如果适用)和事件的结果(成功或失败);
- b) 对每种审计事件类型,基于 ST 中功能组件的可审计事件,【赋值:其他审计相关信息】。

8.1.2.2 FAU_STG.2 受保护的审计数据存储

从属于:无其他组件。

依赖关系:FAU_GEN.1 审计数据产生。

FAU_STG.2.1 TSF 应保护所存储的审计数据,以避免未授权的删除。

FAU_STG.2.2 TSF 应能【防止】审计痕迹中所存储的审计记录的未授权修改。

8.1.2.3 FAU_STG.5 防止审计数据丢失

从属于:FAU_STG.3 审计数据可能丢失时的行为。

依赖关系:FAU_STG.2 受保护的审计数据存储;

FAU_GEN.1 审计数据产生。

FAU_STG.5.1 如果审计数据存储已满,TSF 应【选择:忽略可审计事件、“阻止可审计事件,具有特权的授权用户产生的审计事件除外”、覆盖所存储的最早的审计记录、【赋值:审计存储失效时所采取的其他动作及条件】】。

应用要求:ST 作者给出 TOE 当审计数据溢出时应采取的动作。

8.1.3 FCS类:密码支持

8.1.3.1 FCS_CKH_EXT.1/Low 密钥层次

从属于:无其他组件。

依赖关系:[FCS_CKM.1/Symmetric 密钥生成或 FCS_CKM.1/Asymmetric,FCS_CKM.5];

FCS.COP.1/ENCRYPT 密码运算。

FCS_CKH_EXT.1.1/Low TSF 应支持用于【赋值:低级别用户数据资产列表】保护的数据加密密钥的密钥层次结构。

FCS_CKH_EXT.1.2/Low TSF 应根据【赋值:描述根据 FCS_CKM.1/Symmetric,FCS_CKM.1/Asymmetric 或 FCS_CKM.5 来生成或派生出密钥层次中的所有密钥】来派生和/或生成密钥层次中的所有密钥,实现密钥层次结构中的密钥直接或间接使用根密钥和【无用户鉴别凭据】对【低级别用户数据资产】的数据加密密钥进行保护。

FCS_CKH_EXT.1.3/Low TSF 应根据【选择:使用 FCS_CKH_EXT.1.1/Low 中密钥层次中的密钥和 FCS_COP.1/ENCRYPT 中的算法对【赋值:密钥列表】进行加密存储、使用后删除密钥并在需要时重新生成或派生【赋值:密钥列表】、使用【选择:

- a) 基于处理器隔离模式实现的隔离执行环境;
- b) 基于 SOC 集成安全处理单元实现的隔离执行环境;
- c) 基于独立安全处理单元实现的隔离执行环境

】对【赋值:密钥列表】进行加密存储】对密钥层次结构中的所有密钥和用于派生密钥层次结构中密钥的所有数据进行保护。

应用要求:TOE 可能支持多个密钥层次结构,这些密钥层次结构应通过根密钥来保障其安全性。密钥层次结构关注的是用于数据保护的密钥如何与 TOE 根密钥关联并受 TOE 根密钥保护。

对于申请 EAL2+或 EAL3+级别的 TOE,FCS_CKH_EXT.1.3/Low 中可选择任一隔离执行环境的实现方式对密钥进行加密存储,以保护用于用户数据资产保护密钥的安全。

对于申请 EAL4+或 EAL5+级别的 TOE,FCS_CKH_EXT.1.3/Low 中应选择“使用【基于 SOC 集成安全处理单元实现的隔离执行环境】对【赋值:密钥列表】进行加密存储”或“使用【基于独立安全处理单元实现的隔离执行环境】对【赋值:密钥列表】进行加密存储”,以保护用于用户数据资产保护密钥的安全。

用户数据保护和密钥层次结构见附录 A。

8.1.3.2 FCS_CKH_EXT.1/MediumHigh 密钥层次

从属于:无其他组件。

依赖关系:[FCS_CKM.1/Symmetric 密钥生成或 FCS_CKM.1/Asymmetric,FCS_CKM.5];

FCS.COP.1/ENCRYPT 密码运算。

FCS_CKH_EXT.1.1/MediumHigh TSF 应支持用于【赋值:中高级别用户数据资产列表】保护的数据加密密钥的密钥层次结构。

FCS_CKH_EXT.1.2/MediumHigh TSF 应根据【赋值:描述根据 FCS_CKM.1/Symmetric, FCS_CKM.1/Asymmetric 或 FCS_CKM.5 来生成或派生出密钥层次中的所有密钥】来派生和/或生成密钥层次中的所有密钥,实现密钥层次结构中的密钥直接或间接使用根密钥和【用户鉴别凭据】对【中等级别和高级别用户数据资产】的数据加密密钥进行保护。

注:要求中/高用户数据资产的数据加密密钥是受根密钥和用户鉴别凭据的组合派生的密钥保护,使得中/高级别用户数据资产只能在当前设备中并在用户身份鉴别成功后才能解密。

FCS_CKH_EXT.1.3/MediumHigh TSF 应根据【选择:使用 FCS_CKH_EXT.1.1/MediumHigh 中密钥层次中的密钥和 FCS_COP.1/ENCRYPT 中的算法对【赋值:密钥列表】进行加密存储、使用后删除密钥并在需要时重新生成或派生【赋值:密钥列表】、使用【选择:

- a) 基于处理器隔离模式实现的隔离执行环境;
- b) 基于 SOC 集成安全处理单元实现的隔离执行环境;
- c) 基于独立安全处理单元实现的隔离执行环境

】对【赋值:密钥列表】进行加密存储】对密钥层次结构中的所有密钥和用于派生密钥层次结构中密钥的所有数据进行保护。

应用要求:对于申请 EAL2+或 EAL3+级别的 TOE,FCS_CKH_EXT.1.3/Low 中可选择任一隔离执行环境的实现方式对密钥进行加密存储,以保护用于用户数据资产保护密钥的安全。

对于申请 EAL4+或 EAL5+级别的 TOE,FCS_CKH_EXT.1.3/MediumHigh 中应选择“使用【基于处理器集成安全处理单元实现的隔离执行环境】对【赋值:密钥列表】进行加密存储”或“使用【基于独立安全处理单元实现的隔离执行环境】对【赋值:密钥列表】进行加密存储”,以保护用于用户数据资产保护密钥的安全。

8.1.3.3 FCS_CKM.1/Symmetric 密钥生成

从属于:无其他组件。

依赖关系:[FCS_CKM.2 密钥分发,或 FCS_CKM.5 密钥派生,或 FCS_COP.1/HASH 密码运算];
FCS_RNG.1 随机数生成;
FCS_CKM.6 密钥销毁的时间和事件。

FCS_CKM.1.1/Symmetric TSF 应根据符合【赋值:国家、行业或组织要求的密码管理相关标准】的一个特定的密钥生成算法【选择:使用 FCS_RNG.1 中的随机数生成器,使用 FCS_CKM.5 中指定的密钥派生函数】和规定的密钥长度【赋值:密钥长度,应大于或等于 128 位对称密钥】来生成对称加密密钥。

应用要求:ST 作者应给出 TOE 安全功能用到的对称密钥生成方案,如数据加密存储和密钥加密存储等;若使用 FCS_RNG.1 中的随机数生成器来生成对称密钥,标准可赋值为“无”。

8.1.3.4 FCS_CKM.1/Asymmetric 密钥生成

从属于:无其他组件。

依赖关系:[FCS_CKM.2 密钥分发,或 FCS_CKM.5 密钥派生,或 FCS_COP.1/HASH 密码运算];
FCS_RNG.1 随机数生成;
FCS_CKM.6 密钥销毁的时间和事件。

FCS_CKM.1.1/Asymmetric TSF 应根据符合下列标准【赋值:国家、行业或组织要求的密码管理相关标准】的一个特定的密钥生成算法【赋值:密钥生成算法】和规定的密钥长度【赋值:安全的密钥长度】来生成非对称加密密钥。

应用要求:ST 作者应给出所有用于密钥分发和实体鉴别的非对称密钥生成方案。当用于密钥分发时,非对称密钥生成方案应与密钥分发 FCS_CKM.2 中的方案相匹配;当用于实体鉴别时,非对称密

钥生成方案中的公钥应与 X.509 v3 证书相关联。

8.1.3.5 FCS_CKM.2 密钥分发

从属于:无其他组件。

依赖关系:[FCS_CKM.1/Symmetric 密钥生成,或 FCS_CKM.1/Asymmetric 密钥生成,或 FCS_CKM.5 密钥派生]。

FCS_CKM.2.1 TSF 应根据符合下列标准【赋值:标准列表】的一个特定的密钥分发方法【赋值:密钥分发方法】来分发密钥。

8.1.3.6 FCS_CKM.5 密钥派生

从属于:无其他组件。

依赖关系:[FCS_CKM.2 密钥分发,或 FCS_COP.1/HASH 密码运算];
FCS_CKM.6 密钥销毁的时间和事件。

FCS_CKM.5.1 TSF 应根据符合【赋值:标准列表】的一个特定的密钥派生算法【赋值:密钥派生算法】和规定的密钥长度【赋值:密钥长度列表,密钥长度应大于或等于 128 位】从【赋值:输入参数】中派生出密钥【赋值:密钥类型】。

应用要求:ST 作者应给出 TOE 安全功能,用到的所有密钥派生算法,如口令鉴别、数据加密存储等,密钥派生算法包括 PBKDF、KBKDF、HKDF 或密钥派生函数(Scrypt)等。

8.1.3.7 FCS_CKM.6 密钥销毁的时间和事件

从属于:无其他组件。

依赖关系:FCS_CKM.1/Symmetric 密钥生成,或 FCS_CKM.1/Asymmetric 密钥生成。

FCS_CKM.6.1 当【选择:不再需要,【赋值:密钥或密钥材料销毁的其他情况】】时,TSF 销毁【赋值:密钥(包括密钥材料)列表】。

FCS_CKM.6.2 TSF 应根据符合下列标准【赋值:标准列表】的一个特定的密钥销毁方法【赋值:密钥销毁方法】来销毁 FCS_CKM.6.1 中规定的密钥和密钥材料。

应用要求:ST 作者应给出销毁密钥的列表及销毁方法。

8.1.3.8 FCS_CKM_EXT.1 根密钥保护

从属于:无其他组件。

依赖关系:无依赖关系。

FCS_CKM_EXT.1.1 TSF 应支持受硬件保护的根密钥,保存在 TOE 硬件中安全存储区域无法篡改,仅允许隔离执行环境中的软件通过硬件密码引擎进行访问。

应用要求:ST 作者应给出根密钥的长度,并在 ST 中描述硬件保护根密钥的安全机制。

8.1.3.9 FCS_COP.1/SIGN 密码运算

从属于:无其他组件。

依赖关系:[FCS_CKM.1/Symmetric 密钥生成,或 FCS_CKM.1/Asymmetric 密钥生成,或 FCS_CKM.5 密钥派生]。

FCS_COP.1.1/SIGN TSF 应根据符合【赋值:符合国际标准或国家标准中规定的公开密码标准】的特定的密码算法【赋值:密码算法】和密钥长度【赋值:安全的密钥长度】来执行【加密签名服务(包括生成和验证签名)】。

应用要求:ST 作者应给出 TOE 安全功能用到的所有非对称密码算法,如启动验证、应用软件安装包和更新包,以及系统更新包签名验证、完整性保护等,签名的生成和验证算法包括 RSA、ECDSA 或 SM2 等。

8.1.3.10 FCS_COP.1/ENCRYPT 密码运算

从属于:无其他组件。

依赖关系:[FCS_CKM.1/Symmetric 密钥生成,或 FCS_CKM.1/Asymmetric 密钥生成,或 FCS_CKM.5 密钥派生]。

FCS_COP.1.1/ENCRYPT TSF 应根据符合下列标准【赋值:符合国际标准或国家标准中规定的公开密码标准】的特定的密码算法【赋值:密码算法】和密钥长度【赋值:安全的密钥长度】来执行【对称加密和解密】。

应用要求:ST 作者应给出 TOE 安全功能用到的所有对称密码算法如用户数据加密存储、TSF 数据加密存储,对称密码算法包括 AES、SM4 等。

8.1.3.11 FCS_COP.1/HASH 密码运算

从属于:无其他组件。

依赖关系:无依赖关系。

FCS_COP.1.1/Hash TSF 应根据符合下列标准【赋值:符合国际标准或国家标准中规定的公开密码标准】的特定的密码算法【赋值:密码算法】和消息摘要长度【赋值:消息摘要长度】来执行【散列计算】。

应用要求:ST 作者应给出 TOE 安全功能用到的所有散列算法,如启动验证应用软件安装包和更新包签名验证,以及系统更新包完整性验证等,散列算法包括 SHA2、SHA3 或 SM3 等。

8.1.3.12 FCS_COP.1/KEYHMAC 密码运算

从属于:无其他组件。

依赖关系:[FCS_CKM.1/Symmetric 密钥生成,或 FCS_CKM.1/Asymmetric 密钥生成,或 FCS_CKM.5 密钥派生]。

FCS_COP.1.1/KEYHMAC TSF 应根据符合下列标准【赋值:符合国际标准或国家标准中规定的公开密码标准】的特定的密码算法【赋值:密码算法】和密钥长度【赋值:密钥长度】来执行【基于密钥的散列消息鉴别】。

应用要求:ST 作者应给出 TOE 用到的所有基于密钥的散列消息鉴别算法,基于密钥的散列消息鉴别算法包括 HMAC-SHA2 等。

8.1.3.13 FCS_RNG.1 随机数生成

从属于:无其他组件。

依赖关系:无依赖关系。

FCS_RNG.1.1 TSF 应提供一个【选择:物理、非物理真、确定性、混合物理、混合确定性】随机数生成器,能实现:【赋值:安全能力列表】。

FCS_RNG.1.2 TSF 应提供符合【赋值:指定的质量指标】的【选择:位、八位字节、数字【赋值:数字的格式】】。

应用要求:随机数生成器应具备充分的不可预测性,随机性应符合 GB/T 32915—2016 规定的随机性要求。

8.1.4 FDP类:用户数据保护

8.1.4.1 FDP_ACC.1/MAC 子集访问控制

从属于:无其他组件。

依赖关系:FDP_ACF.1/MAC 基于安全属性的访问控制。

FDP_ACC.1.1/MAC TSF 应对【

- a) 主体:用户态进程;
- b) 客体:【选择:文件、网络对象、套接字、系统参数(如产品型号、处理器型号、版本和功能状态等)、系统服务,【赋值:系统其他对象】】;
- c) 操作:【赋值:操作许可列表】】执行【强制访问控制策略】。

应用要求:ST 作者应给出强制访问控制策略覆盖的客体和操作许可列表。

8.1.4.2 FDP_ACC.1/DAC 子集访问控制

从属于:无其他组件。

依赖关系:FDP_ACF.1/DAC 基于安全属性的访问控制。

FDP_ACC.1.1/DAC TSF 应对【

- a) 主体:用户态进程;
- b) 客体:【选择:目录、普通文件、驱动文件、系统参数(如产品型号、处理器型号、版本和功能状态等),包括【赋值:其他对象列表】】;
- c) 操作:读、写、执行】执行【自主访问控制策略】。

应用要求:ST 作者应给出自主访问控制策略覆盖的客体。

8.1.4.3 FDP_ACC.1/SYSCALL 子集访问控制

从属于:无其他组件。

依赖关系:FDP_ACF.1/SYSCALL 基于安全属性的访问控制。

FDP_ACC.1.1/SYSCALL TSF 应对【

- a) 主体:【赋值:用户态进程列表】;
- b) 客体:【赋值:系统调用接口列表】;
- c) 操作:调用】执行【系统调用管控策略】。

应用要求:ST 作者应给出系统调用管控策略覆盖的用户态进程列表和系统调用接口列表。

8.1.4.4 FDP_ACC.1/Permission 子集访问控制

从属于:无其他组件。

依赖关系:FDP_ACF.1/Permission 基于安全属性的访问控制。

FDP_ACC.1.1/Permission TSF 应对【

- a) 主体:应用软件;
- b) 客体:系统服务(包括【赋值:TOE 提供的系统服务列表】);
- c) 操作:【选择:读、写,【赋值:其他操作列表】】】执行【系统服务访问控制策略】。

应用要求:ST 作者应给出系统服务访问控制策略覆盖的系统服务列表,以及对这些系统服务进行操作的列表。

8.1.4.5 FDP_ACC.1/UserData 子集访问控制

从属于:无其他组件。

依赖关系:FDP_ACF.1/UserData 基于安全属性的访问控制。

FDP_ACC.1.1/UserData TSF 应对【

- a) 主体:TSF;
- b) 客体:【选择:TOE 内部存储,【赋值:其他存储的用户数据】】用户数据资产;
- c) 操作:解密】执行【用户数据解密策略】。

应用要求:ST 作者应给出用户数据资产的范围,以及该范围内用户数据资产分级和存储位置。

8.1.4.6 FDP_ACC.1/SEE 子集访问控制

从属于:无其他组件。

依赖关系:FDP_ACF.1/SEE 基于安全属性的访问控制。

FDP_ACC.1.1/SEE TSF 应对【

- a) 主体:普通运行环境中的应用软件;
- b) 客体:隔离执行环境中的服务;
- c) 操作:读、写、执行】执行【隔离执行环境访问控制策略】。

8.1.4.7 FDP_ACC.1/DTC 子集访问控制

从属于:无其他组件。

依赖关系:FDP_ACF.1/DTC 基于安全属性的访问控制。

FDP_ACC.1.1/DTC TSF 应对【

- a) 主体:TSF;
- b) 客体:【赋值:待传输的用户数据列表】;
- c) 操作:设备间传输】执行【设备间数据传输管控策略】。

应用要求:ST 作者应在 ST 文档中给出设备间数据传输管控方案,对于申请 EAL2+~EAL4+ 级别的 TOE,应在设备间数据传输前告知用户,用户确认后再进行传输;对于申请 EAL5+ 级别的 TOE,应在确认数据的风险等级基础上,结合对端设备类型、安全能力等因素,保障用户数据传输的安全性,若对端设备的类型或安全能力等因素可保障待传输数据安全,允许向对端设备传输并存储,若数据传输存在风险,应告知用户,并在用户确认下传输。

8.1.4.8 FDP_ACF.1/MAC 基于安全属性的访问控制

从属于:无其他组件。

依赖关系:FDP_ACC.1/MAC 子集访问控制。

FDP_ACF.1.1/MAC TSF 应基于【

- a) 主体及其安全属性:
用户态进程:用户态进程标签;
- b) 客体及其安全属性:【选择:
文件系统对象:文件系统对象标签;
网络对象:网络对象标签;
套接字:套接字标签;
系统参数(如产品型号、处理器型号、版本和功能状态等):系统参数标签;
系统服务:系统服务标签;
【赋值:系统其他对象】:【赋值:其他对象标签】】

】对客体执行【强制访问控制策略】。

FDP_ACF.1.2/MAC TSF 应执行以下规则,以决定在受控主体与受控客体间的一个操作是否被允许:【用户态进程标签与客体标签,及主体对客体操作与强制访问控制策略中的规则匹配,则允许用户态进程对客体进行操作】。

FDP_ACF.1.3/MAC TSF 应基于以下附加规则:【无】,明确授权主体访问客体。

FDP_ACF.1.4/MAC TSF 应基于【用户态进程标签与客体标签,及主体对客体操作与强制访问控制策略中的规则不匹配】明确拒绝主体访问客体。

应用要求:ST 作者应给出强制访问控制策略覆盖的客体,及主体和客体的标签,以及强制访问控制的许可规则。

8.1.4.9 FDP_ACF.1/DAC 基于安全属性的访问控制

从属于:无其他组件。

依赖关系:FDP_ACC.1/DAC 子集访问控制。

FDP_ACF.1.1/DAC TSF 应基于【

a) 主体及其安全属性:

用户态进程:用户态进程关联的用户 UID;

b) 客体及其安全属性:【选择:

目录:目录的操作权限位(读、写执行);

普通文件:普通文件的操作权限位(读、写执行);

驱动文件:驱动文件的操作权限位(读、写执行);

系统参数(如产品型号、处理器型号、版本和功能状态等):系统参数的操作权限位(读、写执行);

【赋值:其他对象列表】:【赋值:其他对象的操作权限位(读、写执行)】】对客体执行【自主访问控制策略】。

FDP_ACF.1.2/DAC TSF 应执行以下规则,以决定在受控主体与受控客体间的一个操作是否被允许:【根据用户态进程关联的用户与客体对象属主/属组的关系,并检查应用态进程关联的用户是否有相应的操作权限,如果有则允许应用态进程对客体进行操作】。

FDP_ACF.1.3/DAC TSF 应基于以下附加规则:【赋值:基于安全属性,明确授权主体访问客体的一些规则】,明确授权主体访问客体。

FDP_ACF.1.4/DAC TSF 应基于【用户态进程关联的用户不具有客体对象的操作权限】明确拒绝主体访问客体。

应用要求:自主访问控制机制由客体属主对自己的客体进行管理,并决定是否将自己的客体访问权授予其他主体。ST 作者应给出自主访问控制策略覆盖的客体列表,以及应用态进程的属性 and 客体的属性,同时明确自主访问控制的规则。

8.1.4.10 FDP_ACF.1/SYSCALL 基于安全属性的访问控制

从属于:无其他组件。

依赖关系:FDP_ACC.1/SYSCALL 子集访问控制。

FDP_ACF.1.1/SYSCALL TSF 应基于【

a) 主体及其安全属性:

【赋值:用户态进程列表】:用户态进程 ID;

b) 客体及其安全属性:

【赋值:系统调用接口列表】:系统调用接口名称和参数】对客体执行【系统调用管控策略】。

FDP_ACF.1.2/SYSCALL TSF 应执行以下规则,以决定在受控主体与受控客体间的一个操作是否被允许:【用户态进程调用的系统调用接口名称和参数与系统调用规则一致,则允许用户态进程调用

相应的系统调用接口】。

FDP_ACF.1.3/SYSCAL TSF 应基于以下附加规则:【无】,明确授权主体访问客体。

FDP_ACF.1.4/SYSCAL TSF 应基于【用户态进程调用的系统调用接口名称和参数与系统调用规则不一致】明确拒绝主体访问客体。

应用要求:ST 作者应给出访问系统调用接口的用户态进程列表和系统调用接口列表,同时给出系统调用的管控规则。

8.1.4.11 FDP_ACF.1/Permission 基于安全属性的访问控制

8.1.4.11.1 从属于:无其他组件。

依赖关系:FDP_ACC.1/Permission 子集访问控制。

8.1.4.11.2 FDP_ACF.1.1/Permission TSF 应基于【

a) 主体及其安全属性:

应用软件:应用软件的 UID;

b) 客体及其安全属性:

系统服务(包括【赋值:TOE 提供的系统服务列表】):系统服务对应的权限或接口

】对客体执行【系统服务访问控制策略】。

8.1.4.11.3 FDP_ACF.1.2/Permission TSF 应执行以下规则,以决定在受控主体与受控客体间的一个操作是否被允许:【选择:

a) 用户或 TOE 明确授予的应用软件系统服务权限,应用软件拥有访问系统服务所需的权限一致,应用软件可访问相应的服务;

b) 应用软件不必获取用户或 TOE 授予访问系统服务的权限,应用软件通过 TOE 提供的接口访问系统服务前,需要用户选择并确认供应用软件访问的系统服务后,应用软件可访问用户选择系统服务】。

8.1.4.11.4 FDP_ACF.1.3/Permission TSF 应基于以下附加规则:【应用软件被 TOE 默认授予访问应用软件开发接口的权限】,明确授权主体访问客体。

FDP_ACF.1.4/Permission TSF 应基于【选择:

a) 应用软件被用户拒绝授予访问系统服务的权限;

b) 应用软件访问系统服务前没有得到用户的选择确认。

】明确拒绝主体访问客体。

应用要求:ST 作者应给出 TOE 提供的供应用软件访问的系统服务,如位置、相机、传声器、通讯录、媒体和文件、日历、剪贴板、短信、电话或通话记录等。

8.1.4.12 FDP_ACF.1/UserData 基于安全属性的访问控制

8.1.4.12.1 从属于:无其他组件。

依赖关系:FDP_ACC.1/UserData 子集访问控制。

8.1.4.12.2 FDP_ACF.1.1/UserData TSF 应基于【

a) 主体及其安全属性:TSF;

b) 客体及其安全属性:【选择:TOE 内部存储,【赋值:其他存储的用户数据】】用户数据资产的级别(低、中或高)

】对客体执行【用户数据解密策略】。

8.1.4.12.3 FDP_ACF.1.2/UserData TSF 应执行以下规则,以决定在受控主体与受控客体间的一个操作是否被允许:【

- a) 当 TOE 成功启动后,允许 TSF 解密低级别用户数据资产;
- b) 当 TOE 成功启动后,且启动后用户第一次身份鉴别成功后,允许 TSF 解密中级别用户数据资产;
- c) 当 TOE 成功启动后,用户身份鉴别成功且 TOE 屏幕未锁定时,允许 TSF 解密高级别用户数据资产】。

8.1.4.12.4 FDP_ACF.1.3/UserData TSF 应基于以下附加规则:【无】,明确授权主体访问客体。

8.1.4.12.5 FDP_ACF.1.4/UserData TSF 应基于【无】,明确拒绝主体访问客体。

应用要求:ST 作者应给出用户数据资产的范围,以及该范围内用户数据资产分级和存储位置。

8.1.4.13 FDP_ACF.1/SEE 基于安全属性的访问控制

从属于:无其他组件。

依赖关系:FDP_ACC.1/SEE 子集访问控制。

FDP_ACF.1.1/SEE TSF 应基于【

- a) 主体及其安全属性:
普通运行环境中的应用软件:应用软件 UID;
- b) 客体及其安全属性:
隔离执行环境中的应用软件:访问控制列表】对客体执行【隔离执行环境访问控制策略】。

FDP_ACF.1.2/SEE TSF 应执行以下规则,以决定在受控主体与受控客体间的一个操作是否被允许:【隔离执行环境中的应用软件将请求访问的普通运行环境中的应用软件的标识信息与访问控制列表中的信息进行比对,比对一致允许访问】。

FDP_ACF.1.3/SEE TSF 应基于以下附加规则【无】,明确授权主体访问客体。

FDP_ACF.1.4/SEE TSF 应基于【普通运行环境中的应用软件的标识信息与访问控制列表中的信息不一致】,明确拒绝主体访问客体。

8.1.4.14 FDP_ACF.1/DTC 基于安全属性的访问控制

8.1.4.14.1 从属于:无其他组件。

依赖关系:FDP_ACC.1/DTC 子集访问控制。

8.1.4.14.2 FDP_ACF.1.1/DTC TSF 应基于【

- a) 主体:TSF;
- b) 客体:【赋值:待传输的用户数据列表】;
- c) 安全属性:TOE 的安全等级、对端设备的安全能力或对端设备类型等设备安全信息、或待传输用户数据的风险等级。

】对客体执行【设备间数据传输管控策略】。

8.1.4.14.3 FDP_ACF.1.2/DTC TSF 应执行以下规则,以决定在受控主体与受控客体间的一个操作是否被允许:【选择:

- a) 告知用户,经过用户确认后传输;
- b) TOE 与对端设备之间建立可信信道后,基于传输用户数据的风险等级,对端设备的类型或安全能力等可保障待传输用户数据安全时,允许用户数据在设备间进行传输】。

8.1.4.14.4 FDP_ACF.1.3/DTC TSF 应基于附加规则:【无】,明确授权主体访问客体。

8.1.4.14.5 FDP_ACF.1.4/DTC TSF 应基于【选择:

- a) 告知用户,用户选择拒绝传输;
- b) 基于待传输用户数据的风险等级,对端设备的类型、对端设备的安全能力等无法保障数据安全】,明确拒绝主体访问客体。

应用要求:ST 作者应在 ST 文档中给出设备间数据传输管控方案,对于申请 EAL2+~EAL4+ 级别的 TOE,应在设备间数据传输前告知用户,用户确认后再进行传输;对于申请 EAL5+ 级别的 TOE,应在确认数据的风险等级基础上,结合对端设备类型、安全能力等因素,保障用户数据传输的安全性,若对端设备的类型或安全能力等因素可保障待传输数据安全,允许向对端设备传输并存储,若数据传输存在风险,应告知用户,并在用户确认下传输。

8.1.4.15 FDP_RIP.2 完全残余信息保护

从属于:FDP_RIP.1 子集残余信息保护。

依赖关系:无依赖关系。

FDP_RIP.2.1 TSF 应使得一个资源的任何先前信息内容,在所有客体【释放资源后】先前信息内容不可用。

注:客体指存储用户数据的 TOE 存储空间。

应用要求:ST 作者应在 ST 文档中说明残余信息保护的方法,移动终端通常采用恢复出厂方式对其存储的数据进行擦除,用户的敏感数据不能通过软硬件手段恢复,能保护用户设备转售、废弃后的数据安全。

8.1.4.16 FDP_SDC.1 存储数据的机密性

从属于:无其他组件。

依赖关系:无依赖关系。

FDP_SDC.1.1 TSF 应保护【选择:所有用户数据,以下用户数据【赋值:用户数据列表】】存储在【持久存储器】中的机密性。

应用说明:ST 作者应给出加密存储的用户数据列表,同时应与密钥层次 FCS_CKH_EXT.1/Low 和 FCS_CKH_EXT.1/MediumHigh,以及用户数据访问控制 FDP_ACC.1/UserData 和 FDP_ACF.1/UserData 关联和对应起来。对于申请 EAL2+ 或 EAL3+ 级别的 TOE,FCS_CKH_EXT.1/Low 和 FCS_CKH_EXT.1/MediumHigh 中的用户数据的加密密钥可选择任一隔离执行环境的实现方式进行加密存储,以保护用于用户数据列表资产保护密钥的安全。

对于申请 EAL4+ 或 EAL5+ 级别的 TOE,FCS_CKH_EXT.1/Low 和 FCS_CKH_EXT.1/MediumHigh 中用户数据的加密密钥应选择“使用【基于 SOC 集成安全处理单元实现的隔离执行环境】对【赋值:密钥列表】进行加密存储”或“使用【基于独立安全处理单元实现的隔离执行环境】对【赋值:密钥列表】进行加密存储”,以保护用于用户数据资产保护密钥的安全。

8.1.5 FIA 类:标识和鉴别

8.1.5.1 FIA_AFL.1 鉴别失败处理

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

FIA_AFL.1.1 TSF 应检测与【选择:口令、PIN、图案、指纹、2D 人脸、3D 人脸、其他】相关的【赋值:指定的错误次数(1 到 50 之间的整数)】次未成功鉴别尝试何时发生。

FIA_AFL.1.2 当【选择:达到、超过】所指定的未成功鉴别尝试次数时,TSF 应采取的【选择:延时登录、锁定终端、重启设备、删除用户数据、【赋值:降低攻击风险(如暴力攻击)的其他措施列表】】。

8.1.5.2 FIA_SOS.1 秘密的验证

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_SOS.1.1 TSF 应提供一种机制以验证秘密符合【选择:

- a) 口令或 PIN:口令或 PIN 长度不少于 4 位,并符合【赋值:字符和数字组合的规则】;
- b) 图案:至少包含 4 个点,每个点只能使用一次】。

8.1.5.3 FIA_SOS.2 TSF 生成秘密

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_SOS.2.1 TSF 应提供一种机制以产生符合【

- a) 生物信息鉴别的一次尝试 FAR 不应超过:【选择:
 - 1) 3D 人脸:1:100 000;
 - 2) 2D 人脸:1:50 000;
 - 3) 指纹:1:50 000】和
- b) 生物信息鉴别的一次尝试 FRR 不应超过:【选择:
 - 1) 3D 人脸:1:15;
 - 2) 2D 人脸:1:33;
 - 3) 指纹:1:33】

】的生物特征模板。

FIA_SOS.2.2 TSF 应能为【生物信息鉴别】使用 TSF 产生的生物特征模板。

应用要求:如果选择了生物信息鉴别方式,则应选择该组件。

8.1.5.4 FIA_UAU.1 鉴别的时机

从属于:无其他组件。

依赖关系:FIA_UID.1 标识的时机。

FIA_UAU.1.1 在用户被鉴别前,TSF 应允许执行代表用户的【赋值:解锁 TOE 之前允许 TSF 代表用户执行的操作列表】。

FIA_UAU.1.2 在允许执行代表该用户的任何其他由 TSF 促成的动作前,TSF 应要求每个用户都已被成功鉴别。

8.1.5.5 FIA_UAU.5/USER 多重鉴别机制

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_UAU.5.1/USER TSF 应提供【口令、PIN 和【选择:图案、指纹、2D 人脸、3D 人脸、无其他鉴别机制】】以支持用户鉴别。

FIA_UAU.5.2/USER TSF 应根据【赋值:描述多重鉴别机制如何提供鉴别的规则】鉴别任何用户所声称的身份。

应用要求:ST 作者应给出提供的多重鉴别机制的规则,如口令可在任何时候使用,指纹或人脸只能在设置了锁屏口令且注册了指纹或人脸后才能使用,指纹或人脸只能在未达到生物信息失败次数限制时使用,指纹或人脸只能用在非开机启动首次解锁屏幕场景等。

8.1.5.6 FIA_UAU.5/DEVICE 多重鉴别机制

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_UAU.5.1/DEVICE TSF 应提供【选择：在二个设备上登录相同的用户账号、PIN、二维码、NFC 标签、【赋值：鉴别对端设备身份的其他机制】】以支持对对端设备鉴别。

FIA_UAU.5.2/DEVICE TSF 应根据【赋值：描述多重鉴别机制如何提供对端设备鉴别的规则】鉴别任何对端设备所声称的身份。

应用要求：ST 作者应在 ST 文档中描述使用用户账号、PIN、二维码、或 NFC 标签等方式进行设备身份鉴别的机制，可使用的鉴别机制如下：

- a) TOE 和受信任的对端设备使用相同的用户账户连接到受信任的服务器，然后利用同账号进行身份鉴别；
- b) TOE 扫描受信任的对端设备生成的二维码，建立共享秘密，然后利用共享秘密进行身份鉴别；
- c) 受信任的对端设备扫描 TOE 生成的二维码，建立共享秘密，然后利用共享秘密进行身份鉴别；
- d) TOE 读取嵌入在受信任的对端设备中的 NFC 标签，建立共享秘密，然后利用共享秘密进行身份鉴别；
- e) 受信任的对端设备读取嵌入 TOE 中的 NFC 标签，建立共享秘密，然后利用共享秘密进行身份鉴别；
- f) 用户在 TOE 中输入由受信任的对端设备生成或存储在受信任的对端设备中的 PIN，然后利用 PIN 进行身份鉴别；
- g) 用户将 TOE 生成或存储在 TOE 中的 PIN 输入到受信任的对端设备中，然后利用 PIN 进行身份鉴别。

8.1.5.7 FIA_UAU.5/APP 多重鉴别机制

从属于：无其他组件。

依赖关系：无依赖关系。

FIA_UAU.5.1/APP TSF 应提供【数字签名】以支持应用软件鉴别。

FIA_UAU.5.2/APP TSF 应根据【通过对应用软件安装包的数字签名进行校验】鉴别任何应用软件所声称的身份。

8.1.5.8 FIA_UAU.6 重鉴别

从属于：无其他组件。

依赖关系：无依赖关系。

FIA_UAU.6.1 TSF 应在【选择：用户尝试修改用户鉴别因子、【赋值：ST 作者提供的需要重鉴别的条件列表】】条件下重新鉴别用户。

8.1.5.9 FIA_UAU.7 受保护的鉴别反馈

从属于：无其他组件。

依赖关系：FIA_UAU.1 鉴别的时机。

FIA_UAU.7.1 鉴别进行时，TSF 应仅向用户提供【赋值：反馈列表】。

8.1.5.10 FIA_UID.1 标识的时机

从属于：无其他组件

依赖关系：无依赖关系。

FIA_UID.1.1 在用户被识别之前,TSF 应执行代表用户的【赋值:TSF 促成的动作列表】。

FIA_UID.1.2 在允许执行代表该用户的任何其他 TSF 促成的动作之前,TSF 应要求每个用户都已被成功识别。

8.1.5.11 FIA_API.1 身份鉴别证明

从属于:无其他组件。

依赖关系:无依赖关系。

FIA_API.1.1 TSF 应提供【选择:基于数字签名的鉴别机制、【赋值:其他鉴别机制】】,通过向外部实体提供包含以下属性【选择:使用 TOE 设备证书签发的证书链、【赋值:其他属性列表】】的信息来证明【TOE】的身份。

应用说明:TOE 可使用数字签名技术,使用设备证书签发用于证明 TOE 身份的数字证书来证明自己的身份。

8.1.6 FMT 类:安全管理

8.1.6.1 FMT_MSA.1/Permission 安全属性的管理

从属于:无其他组件。

依赖关系:[FDP_ACC.1/Permission 子集访问控制];

FMT_SMF.1 管理功能。

FMT_MSA.1.1/Permission TSF 应执行【系统服务访问控制策略】,以仅限于【移动终端用户】能对安全属性【TOE 提供的系统服务权限】进行【查询、修改、【赋值:其他操作】】。

应用要求:移动终端用户可对 TOE 为应用软件提供的系统服务权限进行查询和修改。其他访问控制包括强制访问控制、自主访问控制、系统调用管控、用户数据解密、隔离执行环境访问控制和设备间数据传输管控等访问控制策略所对应的安全属性,移动终端用户无法进行管理。

8.1.6.2 FMT_MSA.3/Permission 静态属性初始化

从属于:无其他组件。

依赖关系:FMT_MSA.1 安全属性的管理。

FMT_MSA.3.1/Permission TSF 应执行【系统服务访问控制策略】,以便为用于执行 SFP 的安全属性提供【受限的】默认值。

FMT_MSA.3.2/Permission TSF 允许【移动终端用户】在创建客体或信息时指定替换性的初始值以代替原来的默认值。

应用要求:应用软件访问系统服务的权限都是由用户或 TOE 授予的,否则不应有其他权限,所以这里选择“受限的”。

8.1.6.3 FMT_SMF.1 管理功能

从属于:无其他组件。

依赖关系:无依赖关系。

FMT_SMF.1.1 TSF 应能执行如下安全管理功能:【选择:

- a) 设置和修改锁屏口令、PIN;
- b) 注册和修改【指纹或人脸】;
- c) 查询、修改已安装应用软件权限;
- d) 恢复出厂设置;

- e) 安装、卸载和更新应用软件；
- f) 查询 TOE 软件版本和更新 TOE 软件；
- g) 【赋值:其他安全管理功能】。

8.1.7 FPR类:隐私

8.1.7.1 FPR_PSE.1/APPDEV 假名

从属于:无其他组件。

依赖关系:无依赖关系。

FPR_PSE.1.1/APPDEV TSF 应使得【应用软件】不能确定与【终端设备】绑定的设备标识符。

FPR_PSE.1.2/APPDEV TSF 应能提供设备硬件标识的【至少一个】别名给【应用软件】。

FPR_PSE.1.3/APPDEV TSF 应【提供一个设备硬件的别名】并验证它是否符合【随机生成且用户可重置】。

应用要求:ST 作者应在 ST 中描述禁止应用软件读取的硬件设备标识,以及给应用软件提供的可变软件设备标识。

8.1.7.2 FPR_PSE.1/AD 假名

从属于:无其他组件。

依赖关系:无依赖关系。

FPR_PSE.1.1/AD TSF 应使得【广告平台】不能确定与【终端设备】绑定的设备标识符。

FPR_PSE.1.2/AD TSF 应能提供设备硬件标识的【至少一个】别名给【广告平台】。

FPR_PSE.1.3/AD TSF 应【提供一个设备硬件的别名】并验证它是否符合【随机生成且用户可重置】。

应用要求:ST 作者应在 ST 中描述禁止广告平台读取的硬件设备标识,以及给广告厂商提供随机生成且用户可重置软件设备标识能力。

8.1.8 FPT类:TSF保护

8.1.8.1 FPT_AEX_EXT.1 地址空间布局随机化

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_AEX_EXT.1.1 TSF 应为应用软件提供地址空间布局随机化机制。

FPT_AEX_EXT.1.2 TSF 应为内核提供地址空间布局随机化机制。

8.1.8.2 FPT_AEX_EXT.2 内存页权限控制

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_AEX_EXT.2.1 TSF 应提供以下物理内存保护机制:【选择:数据不可执行、特权模式不可执行、特权模式不可访问、可写内存不可执行、内存只可执行、【赋值:其他内存保护机制】】。

8.1.8.3 FPT_AEX_EXT.3 缓冲区溢出保护

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_AEX_EXT.3.1 TSF 应提供以下缓冲区溢出保护机制:【选择:基于栈的缓冲区溢出保护、基于堆的缓冲区溢出保护】。

8.1.8.4 FPT_AEX_EXT.4 内核完整性保护

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_AEX_EXT.4.1 TSF 应提供以下内核完整性保护机制:【选择:内核代码段只读保护、内核数据段不可执行、系统控制寄存器写保护、强制访问控制策略防篡改、【赋值:其他内核完整性保护机制】】。

应用说明:内核代码段只读权限保护,内核数据段不可执行权限保护,防止内核代码段和数据段被篡改,攻击者具备内核权限依然无法修改;系统寄存器写保护,包括系统控制寄存器、状态寄存器、页表基址寄存器等,防止寄存器被篡改;内核常量数据只读权限保护,防止内核常量数据被篡改,攻击者具备内核权限依然无法修改。通过这些内核完整性保护机制降低漏洞利用后导致的提权等风险。

8.1.8.5 FPT_AEX_EXT.5 控制流完整性保护

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_AEX_EXT.5.1 TSF 应提供以下控制流完整性保护机制:【选择:前向控制流完整性、后向控制流完整性、指针鉴别或【赋值:其他控制流完整性保护机制】】。

应用要求:防御 JOP/ROP 类控制流劫持的攻击行为。如软件方式实现前向控制流完整性保护、软件方式实现后向控制流完整性保护、硬件方式实现的前后向控制流完整性。ST 作者应在 ST 文档中描述控制流完整性保护机制。

8.1.8.6 FPT_FLS.1 失效即保持安全状态

从属于:无其他组件。

依赖关系:无其他组件。

FPT_FLS.1.1 TSF 在下列失效:【FPT_TUD_EXT.1/OS 中系统软件更新失败】发生时应保持一种安全状态。

8.1.8.7 FPT_JTA_EXT.1 JTAG 接口访问控制

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_JTA_EXT.1 TSF 应支持【选择:通过硬件断开物理连接、通过签名密钥进行接入鉴别】对 JTAG 接口进行访问控制。

应用要求:ST 作者应在 ST 文档中描述 TOE 是通过硬件断开与 JTAG 接口的物理连接或使用签名密钥限制对 JTAG 接口的访问。

8.1.8.8 FPT_PHP.3 物理攻击抵抗

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_PHP.3.1 TSF 应通过自动响应以抵抗对【TOE 的隔离执行环境】的【

a) 读取或篡改设备根密钥;

- b) 读取或篡改【赋值:FCS_CKH_EXT.1 密钥层次中密钥或数据列表】;
- c) 篡改 FPT_TST_EXT.1 中用于启动链镜像签名校验的【赋值:公钥、公钥的散列值、证书或其他数据】;
- d) 篡改 FPT_TUD_EXT.1 中用于更新包签名校验的【赋值:公钥、公钥的散列值、证书或其他数据】;
- e) 非授权读取或篡改基于 SOC 集成安全处理单元实现的隔离执行环境中的资产;
- f) 非授权读取或篡改基于独立安全处理单元实现的隔离执行环境中的资产;
- g) 读取或篡改【赋值:其他数据或密钥的列表】],这样才能符合安全功能要求。

应用要求:ST 作者应在 ST 文档中描述 TOE 针对根密钥、用户数据密钥层次中密钥保护、启动验证过程用到的公钥、安全更新用到的公钥和硬件密码引擎的物理攻击抵抗能力。

8.1.8.9 FPT_RCV.2 自动恢复

从属于:FPT_RCV.1 手工恢复。

依赖关系:AGD_OPE.1 用户操作指南。

FPT_RCV.2.1 当不能从【FPT_TST_EXT.1 中检测到的错误】自动恢复时,TSF 应进入一种维护模式,该模式提供返回到一个安全状态的能力。

FPT_RCV.2.2 对【FPT_TST_EXT.1 中检测到的错误】,TSF 应通过自动化过程使 TOE 返回到一个安全状态。

应用要求:ST 作者应在 ST 文档中描述 TOE 在启动验证阶段检测到错误如何恢复到安全状态。

8.1.8.10 FPT_SEE_EXT.1 隔离执行环境

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_SEE_EXT.1.1 TSF 应支持与操作系统运行的普通运行环境隔离的隔离执行环境:【选择:

- a) 基于 SOC 隔离模式实现的隔离执行环境,符合:
 - 1) 具备安全内存,通过处理器模式进行访问控制,普通运行区域的操作系统及应用软件无法直接访问安全内存空间;
 - 2) 具备支撑安全业务部署的输入/输出资源,包括但不限于时钟、硬件密码引擎、硬件真随机数发生器;
 - 3) 用户数据加密密钥及其保护密钥的生成、派生、存储在安全运行区域执行。
- b) 基于 SOC 集成安全处理单元实现的隔离执行环境,符合:
 - 1) 具备隔离的安全内存,如独立安全处理单元专用的 SRAM 或 DRAM,隔离区外部无法直接访问隔离区专用的内存区域;
 - 2) 具备独立的安全存储空间;
 - 3) 具备应支撑安全业务部署的输入/输出资源,包括但不限于时钟、硬件密码引擎或硬件真随机数发生器;独立的启动根;
 - 4) 具备独立的硬件密码引擎和真随机数发生器,支持对称、非对称、杂凑等算法;
 - 5) 具备独立安全时钟和功耗控制单元;
 - 6) 具备固化到独立安全处理单元中硬件唯一根密钥,不可篡改;
 - 7) 具备对抗物理攻击的能力,物理攻击包括侧信道、故障注入等主流硬件攻击方式。
- c) 基于独立安全处理单元实现的隔离执行环境,符合:
 - 1) 具备隔离的安全内存;

- 2) 具备独立的安全存储空间；
- 3) 具备支撑安全业务部署的输入/输出资源,包括但不限于时钟、硬件密码引擎、硬件真随机数发生器;独立的启动根；
- 4) 具备独立的硬件密码引擎和真随机数发生器,使用对称、非对称、杂凑等算法；
- 5) 具备独立安全时钟和功耗控制单元；
- 6) 具备固化到独立安全处理单元中硬件唯一根密钥,不可篡改；
- 7) 具备对抗物理攻击的能力,物理攻击包括侧信道、故障注入等主流硬件攻击方式。】

应用要求:ST 作者应在 ST 文档中描述 TOE 提供的隔离执行环境方案,对于申请 EAL2+ 或 EAL3+ 级别的 TOE,可选择任一隔离环境实现方式,为 TOE 中 TSF 数据存储和用户数据保护密钥存储提供安全隔离的执行环境。

对于申请 EAL4+ 或 EAL5+ 级别的 TOE,应选择“【基于 SOC 集成安全处理单元实现的隔离执行环境】或“符合【基于独立安全处理单元实现的隔离执行环境】”,为 TOE 中 TSF 数据存储和用户数据保护密钥存储提供安全隔离的执行环境。

8.1.8.11 FPT_STG_EXT.1 TSF 数据存储

8.1.8.11.1 从属于:无其他组件。

依赖关系:FCS.COP.1/SIGN 密码运算,或 FCS.COP.1/ENCRYPT 密码运算,或 FCS.COP.1/HASH 密码运算,或 FCS.COP.1/KEYHMAC 密码运算。

8.1.8.11.2 FPT_STG_EXT.1.1 TSF 应为【选择:口令、PIN、指纹鉴别模板和/或指纹鉴别模板加密密钥、人脸鉴别模板和/或人脸鉴别模板加密密钥、文件加密类密钥、【赋值:其他 TSF 数据列表】】的存储提供【选择:

- a) 基于 SOC 隔离模式实现的隔离执行环境；
- b) 基于 SOC 集成安全处理单元实现的隔离执行环境；
- c) 基于独立安全处理单元实现的隔离执行环境】。

8.1.8.11.3 FPT_STG_EXT.1.2 TSF 应使用下述方法对【选择:口令、PIN、指纹鉴别模板和/或指纹鉴别模板加密密钥、人脸鉴别模板和/或人脸鉴别模板加密密钥、文件加密类密钥、【赋值:其他 TSF 数据列表】】进行加密:【赋值:使用 FCS_COP.1/ENCRYPT 中对称密码算法对密钥进行加密】。

8.1.8.11.4 FPT_STG_EXT.1.3 TSF 应使用下述方法对【选择:口令、PIN、指纹鉴别模板和/或指纹鉴别模板加密密钥、人脸鉴别模板和/或人脸鉴别模板加密密钥、文件加密类密钥、【赋值:其他 TSF 数据列表】】的完整性进行保护:【选择:

- a) 使用 FCS_COP.1/ENCRYPT 中具备完整性保护能力的对称密码算法的工作模式对密钥进行加密；
- b) 使用 FCS_COP.1/HASH 中的杂凑算法对密钥加密后的密文的杂凑值进行校验；
- c) 使用 FCS_COP.1/KEYHMAC 中的 MAC 算法对密钥加密后的密文的 MAC 值进行校验；
- d) 【赋值:其他完整性校验方法】。

应用要求:ST 作者应在 ST 文档中描述口令、PIN、指纹鉴别模板和/或指纹鉴别模板加密密钥、人脸鉴别模板和/或人脸鉴别模板加密密钥等 TSF 关键数据保护的隔离执行环境,以及机密性和完整性保护机制。对于申请 EAL2+ 或 EAL3+ 级别的 TOE,可选择任一隔离环境实现方式,对 TSF 关键数据进行保护。

对于申请 EAL4+ 或 EAL5+ 级别的 TOE,FPT_STG_EXT.1.1 应选择“【基于 SOC 集成安全处理单元实现的隔离执行环境】或“【基于独立安全处理单元实现的隔离执行环境】”对 TSF 关键数据进行保护。

8.1.8.12 FPT_STM.1 可靠的时间戳

从属于:无其他组件。

依赖关系:无依赖关系。

FPT_STM.1.1 TSF 应能提供可靠的时间戳。

8.1.8.13 FPT_TST_EXT.1 启动完整性验证

从属于:无其他组件。

依赖关系:FCS.COP.1/SIGN 密码运算;

FCS.COP.1/HASH 密码运算。

FPT_TST_EXT.1.1 TSF 应从固化在不可篡改硬件中的启动可信根开始,使用 FCS_COP.1/SIGN 或 FCS.COP.1/HASH 中规定的密码算法逐级对启动链中的【启动加载程序、操作系统内核、隔离执行环境镜像或【赋值:其他镜像】】进行签名校验,同时【选择:

- a) 用于签名校验的【选择:公钥应存储在不可篡改的硬件中、公钥的散列值存储在不可篡改的硬件或公钥存储在受硬件保护的存储区域】;
- b) 对启动链上每个被加载镜像进行度量并记录完整性验证信息,并将度量信息提供给可信的外部实体;
- c) 使用与 a)不同的公钥在【选择:基于 SOC 集成安全处理单元实现的隔离执行环境、基于独立安全处理单元实现的隔离执行环境】中对启动链再次进行签名校验,且用于签名校验的【选择:公钥存储在不可篡改的硬件中、公钥的散列值存储在不可篡改的硬件、公钥存储在受硬件保护的存储区域】】。

应用要求:ST 作者应在 ST 文档中描述 TOE 启动过程中整个启动链的校验机制,以及用于签名校验的公钥的保护机制。对于申请 EAL5+级别的 TOE,应符合 c)的要求。

8.1.8.14 FPT_TST_EXT.2 运行完整性验证

从属于:无其他组件。

依赖关系:FCS.COP.1/SIGN 密码运算;

FCS.COP.1/HASH 密码运算。

FPT_TST_EXT.2.1 TSF 应在正常工作期间周期性地运行自检程序以证明【赋值:TSF 的组成部分或 TSF 数据】能正确运行。

FPT_TST_EXT.2.2 TSF 应将自检程序运行在【选择:基于处理器隔离模式实现的隔离执行环境、基于 SOC 隔离模式实现的隔离执行环境】检测到运行错误时应记录审计信息。

应用要求:ST 作者应在 ST 文档中描述 TOE 在正常工作期间对 TSF 组成部分或数据校验机制,以及校验程序的保护机制。对于申请 EAL2+或 EAL3+级别的 TOE,可选择任一隔离执行环境实现方式,为 TOE 中自检程序提供运行环境。对于申请 EAL4+或 EAL5+级别的 TOE,应选择“【基于 SOC 集成安全处理单元实现的隔离执行环境】或“符合【基于独立安全处理单元实现的隔离执行环境】”,为 TOE 中自检程序提供运行环境。

8.1.8.15 FPT_TUD_EXT.1/OS 系统软件更新

从属于:无其他组件。

依赖关系:FCS.COP.1/SIGN 密码运算;

FCS.COP.1/HASH 密码运算。

FPT_TUD_EXT.1.1/OS TSF 应在安装【TOE 系统软件】更新包之前使用数字签名机制对【TOE 系统软件】更新包的签名进行验证。

FPT_TUD_EXT.1.2/OS TSF 应验证用于校验【TOE 系统软件】更新包数字签名的公钥【为 TOE 中预置的不可篡改证书中的公钥】。

8.1.8.16 FPT_TUD_EXT.1/APP 应用软件验证

从属于:无其他组件。

依赖关系:FCS.COP.1/SIGN 密码运算;

FCS.COP.1/HASH 密码运算。

FPT_TUD_EXT.1.1/APP TSF 应在安装【应用软件】更新包之前使用数字签名机制对【应用软件】更新包的签名进行验证。

FPT_TUD_EXT.1.2/APP TSF 应验证用于校验【应用软件】更新包数字签名的公钥【选择:为与首次安装时存储在 TOE 中证书的公钥一致的公钥,为 TOE 中预置的不可篡改证书中的公钥】。

8.1.9 FTA 类:TOE 访问

8.1.9.1 FTA_SSL.1 TSF 原发会话锁定

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

FTA_SSL.1.1 TSF 应在达到【赋值:用户不活动的时间间隔】后,通过以下方法锁定一个交互式会话:

- a) 清除或覆写显示设备的显示内容,使当前的内容不可读;
- b) 除了会话解锁活动之外,终止用户数据存取/显示设备的任何活动,但【选择:允许短信数据写入,允许电话呼入并显示来电信息界面且在通话结束后应恢复锁定,允许使用相机功能,【赋值:其他允许的操作】】。

FTA_SSL.1.2 TSF 应在解锁会话之前发生以下事件:【成功地完成对终端用户的鉴别】。

8.1.9.2 FTA_SSL.2 用户原发会话锁定

从属于:无其他组件。

依赖关系:FIA_UAU.1 鉴别的时机。

FTA_SSL.2.1 TSF 应允许通过以下方法实现对他自己拥有的交互会话进行用户原发锁定:

- a) 清除或覆写显示设备的显示内容,使当前的内容不可读;
- b) 除了会话解锁活动之外,终止用户数据存取/显示设备的任何活动,但【选择:允许短信数据写入,允许电话呼入并显示来电信息界面且在通话结束后应恢复锁定,允许使用相机功能,【赋值:其他允许的操作】】。

FTA_SSL.2.2 TSF 应在解锁会话之前发生以下事件:【成功地完成对终端用户的鉴别】。

8.1.10 FTP 类:可信路径/信道

8.1.10.1 FTP_ITC.1/TLS TSF 间可信信道

从属于:无其他组件。

依赖关系:无依赖关系。

FTP_ITC.1.1/TLS TSF 应在它自己和另一个可信 IT 产品之间提供一条通信信道,该信道在逻辑上与其他通信信道截然不同,可标识其端点,且能保护信道中数据免遭修改或泄露。

FTP_ITC.1.2/TLS TSF 应允许【选择：TSF、【赋值：ST 作者指定的另一个可信 IT 产品】】经由可信信道发起通信。

FTP_ITC.1.3/TLS 对于【系统软件更新包下载、应用软件的下载、【赋值：其他需要可信信道的功能列表】】，TSF 应经由可信信道发起通信。

应用要求：当 TOE 与远程 IT 设备进行通信时，应使用可信信道，ST 作者应给出使用 TLS 建立可信信道的功能。

8.1.10.2 FTP_ITC.1/DEVICE TSF 间可信信道

从属于：无其他组件。

依赖关系：无依赖关系。

FTP_ITC.1.1/DEVICE TSF 应在它自己和另一个其他移动终端之间提供一条通信信道，该信道在逻辑上与其他通信信道截然不同，可标识其端点，且能保护信道中数据免遭修改或泄露。

FTP_ITC.1.2/DEVICE TSF 应【选择：TSF、其他移动终端设备】经由可信信道发起通信。

FTP_ITC.1.3/DEVICE 对于【TOE 与其他移动终端进行设备间数据传输、【赋值：其他需要使用设备间可信信道的功能列表】】，TSF 应经由可信信道发起通信。

8.2 安全保障要求

8.2.1 概述

移动终端的安全保障要求由 GB/T 18336.3—2024 的安全保障要求组件组成，移动终端 EAL2+、EAL3+、EAL4+ 和 EAL5+ 保障级的安全保障要求组件见表 2。EAL2+ 是在 EAL2 的基础上增加 ALC_FLR.1；EAL3+ 是在 EAL3 的基础上增加 ALC_FLR.1；EAL4+ 是在 EAL4 的基础上增加 ALC_FLR.3；EAL5+ 是在 EAL5 的基础上增加 ALC_FLR.3。

表 2 安全保障要求组件

保障类	保障组件	备注			
		EAL2+	EAL3+	EAL4+	EAL5+
ADV 类	ADV_ARC.1	✓	✓	✓	✓
	ADV_FSP.2	✓			
	ADV_FSP.3		✓		
	ADV_FSP.4			✓	
	ADV_FSP.5				✓
	ADV_IMP.1			✓	✓
	ADV_INT.2				✓
	ADV_TDS.1	✓			
	ADV_TDS.2		✓		
	ADV_TDS.3			✓	
	ADV_TDS.4				✓
AGD 类	AGD_OPE.1	✓	✓	✓	✓
	AGD_PRE.1	✓	✓	✓	✓

表 2 安全保障要求组件（续）

保障类	保障组件	备注			
		EAL2+	EAL3+	EAL4+	EAL5+
ALC类	ALC_CMC.2	√			
	ALC_CMC.3		√		
	ALC_CMC.4			√	√
	ALC_CMS.2	√			
	ALC_CMS.3		√		
	ALC_CMS.4			√	
	ALC_CMS.5				√
	ALC_DEL.1	√	√	√	√
	ALC_DVS.1		√	√	√
	ALC_FLR.1	√	√		
	ALC_FLR.3			√	√
	ALC_LCD.1		√	√	√
	ALC_TAT.1			√	
	ALC_TAT.2				√
ASE类	ASE_CCL.1	√	√	√	√
	ASE_ECD.1	√	√	√	√
	ASE_INT.1	√	√	√	√
	ASE_OBJ.2	√	√	√	√
	ASE_REQ.2	√	√	√	√
	ASE_SPD.1	√	√	√	√
	ASE_TSS.1	√	√	√	√
ATE类	ATE_COV.1	√			
	ATE_COV.2		√	√	√
	ATE_DPT.1		√		
	ATE_DPT.2			√	
	ATE_DPT.3				√
	ATE_FUN.1	√	√	√	√
	ATE_IND.2	√	√	√	√
AVA类	AVA_VAN.2	√	√		
	AVA_VAN.3			√	
	AVA_VAN.4				√
注：“√”表示要求。“空白”表示不涉及。					

8.2.2 ADV类

表 2 所列出的 ADV 类保障组件应符合 GB/T 18336.3—2024 中的 10.2~10.5 和 10.7。

8.2.3 AGD类

表 2 所列出的 AGD 类保障组件应符合 GB/T 18336.3—2024 中的 11.2 和 11.3。

8.2.4 ALC类

表 2 所列出的 ALC 类保障组件应符合 GB/T 18336.3—2024 中的 12.2~12.7 和 12.9。

8.2.5 ASE类

表 2 所列出的 ASE 类保障组件应符合 GB/T 18336.3—2024 中的 9.2~9.8。

8.2.6 ATE类

表 2 所列出的 ATE 类保障组件应符合 GB/T 18336.3—2024 中的 13.2~13.5。

8.2.7 AVA类

表 2 所列出的 AVA 类保障组件应符合 GB/T 18336.3—2024 中的 14.3。

9 测试评估方法

9.1 安全功能要求的测试方法

9.1.1 FAU类:安全审计测试方法

9.1.1.1 FAU_GEN.1 审计数据产生测试方法

FAU_GEN.1 审计数据产生测试方法如下:

- a) 关闭安全审计功能,然后分别执行如下操作:系统开关机,账号登录和退出登录,网络连接、断开,文件读、写和删除,应用安装、运行和卸载,数字证书的生成、使用和删除,权限的申请、授权和拒绝,ST 赋值的“其他专门可审计事件”对应的操作;检查是否不生成审计日志;
- b) 开启安全审计功能,然后分别执行如下操作:系统开关机,账号登录和退出登录,网络连接、断开,文件读、写和删除,应用安装、运行和卸载,多次操作事件触发审计日志超限,数字证书的生成、使用和删除,权限的申请、授权、拒绝,ST 赋值的“其他专门可审计事件”对应的操作;检查是否正确生成审计事件对应的审计日志;
- c) 检查步骤 b)中生成的审计日志是否记录了事件的日期和时间、事件类型、主体身份和事件的结果、ST 赋值的“其他审计相关信息”。

9.1.1.2 FAU_STG.1 受保护的审计存储测试方法

FAU_STG.1 受保护的审计存储测试方法如下:

- a) 模拟攻击者使用非法进程删除审计记录,检查非法进程是否删除审计记录失败;
- b) 模拟用户使用合法进程删除审计记录,检查合法进程是否成功删除审计记录;
- c) 模拟攻击者使用未授权的进程修改(如写入)审计记录,检查未授权的进程是否修改审计记录失败;

- d) 模拟用户使用被授权的进程修改(如写入)审计记录,检查授权的进程是否成功修改审计记录。

9.1.1.3 FAU_STG.4 防止审计数据丢失测试方法

FAU_STG.4 防止审计数据丢失测试方法如下:

- a) 模拟用户多次操作,触发审计日志满的情形,然后执行系统重启的操作,检查是否记录最近一次系统启动事件;
- b) 模拟用户多次操作,触发审计日志满的情形,然后分别执行特权和非特权用户的被审计操作,检查是否记录特权用户操作事件,是否未记录非特权用户操作事件;
- c) 模拟用户多次操作,触发审计日志满的情形,记录下最早的审计记录,然后执行系统重启的操作,检查是否记录最早的审计记录是否被覆盖和最近系统启动时间;
- d) 检查审计日志满、存储失效时,审计日志是否按 ST 赋值的“审计存储失效时所采取的其他动作”进行运行。

注:根据ST文档的选择执行测试步骤。如果选择“忽略可审计事件”,执行步骤a)、d);如果选择“阻止可审计事件,除非具有特权的授权用户产生的审计事件”,执行步骤b)、d);如果选择“覆盖所存储的最早的审计记录”,执行步骤c)、d)。

9.1.2 FCS类:密码支持测试方法

9.1.2.1 FCS_CKH_EXT.1/Low 密钥层次测试方法

基于 ST 的赋值“描述根据 FCS_CKM.1/Symmetric, FCS_CKM.1/Asymmetric 或 FCS_CKM.5 来生成或派生出密钥层次中的所有密钥”、赋值“密钥列表”,输出密钥层级表,包含各级密钥名称、涉及的密码算法和密钥间的关系(如:密钥 1 通过派生得到密钥 2,密钥 3 由密钥生成算法生成,密钥 2 通过加密算法保护密钥 3),其中密码算法为密钥生成算法、密钥派生算法或加密算法。

FCS_CKH_EXT.1/Low 密钥层次测试方法如下:

- a) 基于等价类遍历 ST 赋值的“低级别用户数据资产列表”,触发加密流程,通过日志打印或代码片段识别出密钥名称、密码算法、密钥间的关系,检查密钥保护层级是否与密钥层级表一致;
- b) 遍历 ST 赋值的“密钥列表”,通过日志打印或代码片段识别出密钥派生和/或生成算法,检查密钥生成算法是否与密钥层级表一致;
- c) 遍历 ST 赋值的“密钥列表”(持久化存储部分),触发密钥的存储,通过日志打印或代码片段识别出密钥加密算法关键字,检查加密存储的算法关键字是否与密钥层级表一致;
- d) 遍历 ST 赋值的“密钥列表”(非持久化存储部分),触发密钥的生成或派生,通过日志打印或代码片段识别出密钥派生和/或生成算法关键字,检查密钥生成或派生的算法关键字是否与密钥层级表一致;
- e) 遍历 ST 赋值的“密钥列表”(持久化存储部分),触发密钥的存储,通过日志打印或代码片段识别出隔离执行环境的关键字,检查加密存储用的环境是否为基于处理器隔离模式实现的隔离执行环境;
- f) 遍历 ST 赋值的“密钥列表”(持久化存储部分),触发密钥的存储,通过日志打印或代码片段识别出隔离执行环境的关键字,检查加密存储用的环境是否为基于处理器集成安全处理单元实现的隔离执行环境;
- g) 遍历 ST 赋值的“密钥列表”(持久化存储部分),触发密钥的存储,通过日志打印或代码片段识别出隔离执行环境的关键字,检查加密存储用的环境是否为基于独立安全处理单元实现的

隔离执行环境。

注：测试步骤为 a)~d)；其余测试步骤根据 ST 文档的选择决定是否执行；如果选择“基于处理器隔离模式实现的隔离执行环境”，执行步骤 e)；如果选择“基于处理器集成安全处理单元实现的隔离执行环境”，执行步骤 f)，如果选择“基于独立安全处理单元实现的隔离执行环境”，执行步骤 g)。

9.1.2.2 FCS_CKH_EXT.1/MediumHigh 密钥层次测试方法

基于 ST 的赋值“描述根据 FCS_CKM.1/Symmetric, FCS_CKM.1/Asymmetric 或 FCS_CKM.5 来生成或派生出密钥层次中的所有密钥”、赋值“密钥列表”，输出密钥层级表，包含各级密钥名称、涉及的密码算法和密钥间的关系（如：密钥 1 通过派生得到密钥 2，密钥 3 由密钥生成算法生成，密钥 2 通过加密算法保护密钥 3），其中密码算法为密钥生成算法、密钥派生算法或加密算法。

FCS_CKH_EXT.1/MediumHigh 密钥层次测试方法如下：

- 基于等价类遍历 ST 赋值的“中等级别和高级别用户数据资产列表”，触发加密流程，通过日志打印或代码片段识别出密钥名称、密钥派生和/或生成算法、密码算法、密钥间的关系，检查密钥保护层级是否与密钥层级表一致；
- 遍历 ST 赋值的“密钥列表”，通过日志打印或代码片段识别出密钥派生和/或生成算法，检查密钥生成算法是否与密钥层级表一致；
- 遍历 ST 赋值的“密钥列表”（持久化存储部分），触发密钥的存储，通过日志打印或代码片段识别出密钥加密算法关键字，检查加密存储的算法关键字是否与密钥层级表一致；
- 遍历 ST 赋值的“密钥列表”（非持久化存储部分），触发密钥的生成或派生，通过日志打印或代码片段识别出密钥派生和/或生成算法关键字，检查密钥生成或派生算法关键字是否与密钥层级表一致；
- 遍历 ST 赋值的“密钥列表”（持久化存储部分），触发密钥的存储，通过日志打印或代码片段识别出隔离执行环境的关键字，检查加密存储用的环境是否为基于处理器隔离模式实现的隔离执行环境；
- 遍历 ST 赋值的“密钥列表”（持久化存储部分），触发密钥的存储，通过日志打印或代码片段识别出隔离执行环境的关键字，检查加密存储用的环境是否为基于处理器集成安全处理单元实现的隔离执行环境；
- 遍历 ST 赋值的“密钥列表”（持久化存储部分），触发密钥的存储，通过日志打印或代码片段识别出隔离执行环境的关键字，检查加密存储用的环境是否为基于独立安全处理单元实现的隔离执行环境。

注：应执行的测试步骤是 a)~d)，其余测试步骤需要根据 ST 文档的选择决定是否执行，如果选择“基于处理器隔离模式实现的隔离执行环境”执行步骤 e)，如果选择“基于处理器集成安全处理单元实现的隔离执行环境”执行步骤 f)，如果选择“基于独立安全处理单元实现的隔离执行环境”执行步骤 g)。

9.1.2.3 FCS_CKM.1/Symmetric 密钥生成测试方法

遍历 ST 中全部对称密钥，基于 ST 的赋值“国家、行业或组织要求的密码管理相关标准”、赋值“密钥长度，应大于或等于 128 位对称密钥”、选择“使用 FCS_RNG.1 中的随机数生成器，使用 FCS_CKM.5 中指定的密钥派生函数”输出对称密钥生成算法表，包含各对称密钥对应的密钥名称、密码算法、密码标准、密钥长度和密钥生成的应用场景。

FCS_CKM.1/Symmetric 密钥生成测试方法如下：

- 遍历对称密钥生成算法表中的对称密钥，通过代码片段识别出密码算法来源或运算逻辑，或通过密钥向量运算的方法，检查对称密钥生成的算法的运算逻辑是否符合对称密钥生成算法表中的密码标准（来源合法或运算正确）；

- b) 遍历对称密钥生成算法表中的对称密钥,触发相应应用场景下的密钥生成流程,通过日志打印或代码片段识别出密钥派生和/或生成算法关键字,检查对称密钥生成的算法关键字是否与对称密钥生成算法表中的密码算法一致;
- c) 遍历对称密钥生成算法表中的对称密钥,通过日志打印或代码片段识别出密钥长度,检查对称密钥的长度是否为对称密钥生成算法表中的密钥长度,且密钥长度大于或等于 128 位。

注: 密钥向量运算的测试方法是给定密钥算法所需的密钥材料[如 DRBG 中的熵输入(entropyInput)、随机数(nonce)等],调用对应的密码算法进行运算,运算结果符合既定的密码算法结果。

9.1.2.4 FCS_CKM.1/Asymmetric 密钥生成测试方法

遍历 ST 中全部非对称密钥,基于 ST 的赋值“国家、行业或组织要求的密码管理相关标准”、赋值“密钥生成算法”、赋值“安全的密钥长度”,输出非对称密钥生成算法表,包含各非对称密钥对应的密钥名称、密码算法、密码标准、密钥长度和密钥生成的应用场景。

FCS_CKM.1/Asymmetric 密钥生成测试方法如下:

- a) 遍历非对称密钥生成算法表中的非对称密钥,通过代码片段识别出密码算法来源或运算逻辑,或通过密钥向量运算的方法,检查非对称密钥生成的算法的运算逻辑是否符合非对称密钥生成算法表中的密码标准(来源合法或运算正确);
- b) 遍历非对称密钥生成算法表中的非对称密钥,触发相应应用场景下的密钥生成流程,通过日志打印或代码片段识别出密钥生成算法关键字,检查非对称密钥生成的算法关键字是否与非对称密钥生成算法表中的密码算法一致;
- c) 遍历非对称密钥生成算法表中的非对称密钥,通过日志打印或代码片段识别出密钥长度,检查非对称密钥的长度是否为非对称密钥生成算法表中的安全的密钥长度。

9.1.2.5 FCS_CKM.2 密钥分发测试方法

遍历 ST 中全部密钥分发的场景,基于 ST 的赋值“标准列表”、赋值“密钥分发方法”输出密钥分发算法表,包含各密钥对应的密钥名称、密钥分发方法、密码标准和密钥分发的应用场景。

FCS_CKM.2 密钥分发测试方法如下:

遍历密钥分发算法表中的密钥分发的应用场景,通过代码片段识别出密码算法来源或运算逻辑,或通过密钥向量运算的方法,检查密钥分发的算法的运算逻辑是否符合密钥分发算法表中的标准(来源合法或运算正确)。

9.1.2.6 FCS_CKM.5 密钥派生测试方法

遍历 ST 中全部密钥派生的场景,基于 ST 的赋值“标准列表”、赋值“密钥派生算法”、赋值“密钥长度列表,密钥长度应大于或等于 128 位”、赋值“输入参数”、赋值“密钥类型”输出密钥派生算法表,包含各密钥对应的密钥名称、密钥派生算法、密码标准、密钥长度、输入参数、密钥类型。

FCS_CKM.5 密钥派生测试方法如下:

遍历密钥派生算法表中的密钥派生的场景,通过代码片段识别出密码算法来源或运算逻辑,或通过密钥向量运算的方法,检查密钥派生的算法的运算逻辑是否符合密钥派生算法表中的标准(来源合法或运算正确)。

9.1.2.7 FCS_CKM.6 密钥销毁的时间和事件测试方法

遍历 ST 中全部密钥销毁的场景,基于 ST 中的选择“不再需要”、赋值“密钥或密钥材料销毁的其他情况”、赋值“密钥(包括密钥材料)列表”、赋值“密钥销毁方法”输出密钥销毁表,包含各密钥/密钥材料对应的密钥/密钥材料名称、密钥销毁的时机(如:TLS 会话结束)和密钥销毁的方法(如:数据覆写

或指令清除)。

FCS_CKM.6 密钥销毁的时间和事件测试方法如下:

遍历密钥销毁表中的密钥销毁的场景,通过代码片段识别出密钥销毁的时机、密钥销毁的方法,或导出密钥销毁前后的内存做对比,检查密钥销毁的方法是否与密钥销毁表中的方法一致。

注:提取密钥销毁前后的内存做对比,具体的操作是先将待销毁的密钥明文打印到日志中,提取内存确定密钥在内存中位置;然后触发密钥销毁,再次提取内存检查原位置处的密钥已被擦除。

9.1.2.8 FCS_CKM_EXT.1 根密钥保护测试方法

FCS_CKM_EXT.1 根密钥保护测试方法如下:

- 审查厂商提供的根密钥受硬件保护的设计文档,检查根密钥是否受硬件保护,保护方案是否符合业界优秀实践;
- 使用非法程序访问根密钥进行密钥运算,检查非法程序是否访问根密钥失败;
- 使用合法的硬件密码引擎访问根密钥进行密钥运算,检查合法硬件密码引擎是否成功访问根密钥。

9.1.2.9 FCS_COP.1/SIGN 密码运算测试方法

遍历 ST 中全部签名生成和验证的场景,基于 ST 的赋值“符合国际标准或国家标准中规定的公开密码标准”、赋值“密码算法”、赋值“安全的密钥长度”,输出签名生成和验证表,包含各场景对应的场景名称、密码算法、密码标准和密钥长度。

FCS_COP.1/SIGN 密码运算测试方法如下:

- 遍历签名生成和验证表中的签名生成和验证的场景,通过代码片段识别出密码算法来源或运算逻辑,或通过密钥向量运算的方法,检查签名生成和验证的算法的运算逻辑是否符合签名生成和验证表中的密码标准(来源合法或运算正确);
- 遍历签名生成和验证表中的签名生成和验证的场景,触发签名生成和验证的流程,通过日志打印或代码片段识别出签名生成和验证的算法关键字,检查签名生成和验证的算法关键字是否与签名生成和验证表中的密码算法一致;
- 遍历签名生成和验证表中的签名生成和验证的场景,通过日志打印或代码片段识别出密钥长度,检查签名生成和验证算法的密钥长度是否为签名生成和验证表中的安全的密钥长度。

9.1.2.10 FCS_COP.1/ENCRYPT 密码运算测试方法

遍历 ST 中全部对称密钥加解密的场景,基于 ST 的赋值“符合国际标准或国家标准中规定的公开密码标准”、赋值“密码算法”、赋值“安全的密钥长度”,输出对称密钥加解密表,包含各场景对应的场景名称、密码算法、密码标准和密钥长度。

FCS_COP.1/ENCRYPT 密码运算测试方法如下:

- 遍历对称密钥加解密表中的对称密钥加解密的场景,通过代码片段识别出密码算法来源或运算逻辑,或通过密钥向量运算的方法,检查对称密钥加解密的算法的运算逻辑是否符合对称密钥加解密表中的密码标准(来源合法或运算正确);
- 遍历对称密钥加解密表中的对称密钥加解密的场景,触发对称密钥加解密的流程,通过日志打印或代码片段识别出对称密钥加解密的算法关键字,检查对称密钥加解密的算法关键字是否与对称密钥加解密表中的密码算法一致;
- 遍历对称密钥加解密表中的对称密钥加解密的场景,通过日志打印或代码片段识别出密钥长度,检查对称密钥加解密的密钥长度是否为对称密钥加解密表中的安全的密钥长度。

9.1.2.11 FCS_COP.1/HASH 密码运算测试方法

遍历 ST 中全部散列计算的场景,基于 ST 的赋值“符合国际标准或国家标准中规定的公开密码标准”、赋值“密码算法”、赋值“消息摘要长度”输出散列计算算法表,包含各场景对应的场景名称、密码算法、密码标准和消息摘要长度。

FCS_COP.1/HASH 密码运算测试方法如下:

- a) 遍历散列计算算法表中的散列计算的场景,通过代码片段识别出密码算法来源或运算逻辑,或通过密钥向量运算的方法,检查散列计算的算法的运算逻辑是否符合散列计算算法表中的密码标准(算法来源合法或运算正确);
- b) 遍历散列计算算法表中的散列计算的场景,触发散列计算的流程,通过日志打印或代码片段识别出散列计算的算法关键字,检查散列计算的算法关键字是否与散列计算算法表中的密码算法一致;
- c) 遍历散列计算算法表中的散列计算的场景,通过日志打印或代码片段识别出消息摘要长度,检查散列计算的消息摘要长度是否为散列计算算法表中的消息摘要长度。

9.1.2.12 FCS_COP.1/KEYHMAC 密码运算测试方法

遍历 ST 中基于密钥的散列消息鉴别的场景,基于 ST 的赋值“符合国际标准或国家标准中规定的公开密码标准”、赋值“密码算法”、赋值“密钥长度”输出密钥散列消息鉴别算法表,包含各场景对应的场景名称、密码算法、密码标准和密钥长度。

FCS_COP.1/KEYHMAC 密码运算测试方法如下:

- a) 遍历密钥散列消息鉴别算法表中的散列消息鉴别的场景,通过代码片段识别出密码算法来源或运算逻辑,或通过密钥向量运算的方法,检查散列消息鉴别的算法的运算逻辑是否符合密钥散列消息鉴别算法表中的密码标准(算法来源合法或运算正确);
- b) 遍历密钥散列消息鉴别算法表中的散列消息鉴别的场景,触发散列消息鉴别的流程,通过日志打印或代码片段识别出散列消息鉴别的算法关键字,检查散列消息鉴别的算法关键字是否与密钥散列消息鉴别算法表中的密码算法一致;
- c) 遍历密钥散列消息鉴别算法表中的散列消息鉴别的场景,通过日志打印或代码片段识别出密钥长度,检查散列消息鉴别的密钥长度是否为密钥散列消息鉴别算法表中的密钥长度。

9.1.2.13 FCS_RNG.1 随机数生成测试方法

FCS_RNG.1 随机数生成测试方法如下:

- a) 采集 TOE 随机数生成器数字化处理后的数据集,数据集不少于 1 百万位;
- b) 使用随机数检测工具对采集的随机数序列进行随机性测试,检查随机性是否符合 GB/T 32915—2016 规定的随机性要求。

9.1.3 FDP 类:用户数据保护测试方法

9.1.3.1 FDP_ACC.1/MAC 子集访问控制测试方法

基于 ST 中的选择“文件、网络对象、套接字、系统参数(如产品型号、处理器型号、版本和功能状态等)、系统服务”、赋值“系统其他对象”、赋值“操作许可列表”输出强制访问控制列表(按客体类型和操作许可划分等价类),包含客体、操作许可(如:读、写或执行)、对应的合法主体进程(选择 1 个典型的进程即可)和非法主体进程(选择 1 个典型的进程即可)。

FDP_ACC.1/MAC 子集访问控制测试方法如下:

- a) 遍历强制访问控制列表中的客体,利用合法进程访问标签对应的客体,执行合法的操作,检查合法进程是否成功访问;
- b) 遍历强制访问控制列表中的客体,利用非法进程访问标签对应的客体,执行非法的操作,检查非法进程是否访问失败。

9.1.3.2 FDP_ACC.1/DAC 子集访问控制测试方法

基于 ST 中的选择“文件、网络对象、套接字、系统参数(如产品型号、处理器型号、版本和功能状态等)、系统服务”、赋值“其他对象列表”输出自主访问控制列表(按客体类型划分等价类),包含客体和对应的拥有者。

FDP_ACC.1/DAC 子集访问控制测试方法如下:

- a) 遍历自主访问控制列表中的客体,检查某个未被拥有者授权的主体是否读取客体失败;
- b) 遍历自主访问控制列表中的客体,检查某个已被拥有者授权的主体是否成功读取客体;
- c) 遍历自主访问控制列表中的客体,检查某个未被拥有者授权的主体是否写入客体失败;
- d) 遍历自主访问控制列表中的客体,检查某个已被拥有者授权的主体是否成功写入客体;
- e) 遍历自主访问控制列表中的客体,检查某个未被拥有者授权的主体是否执行客体失败;
- f) 遍历自主访问控制列表中的客体,检查某个已被拥有者授权的主体是否成功执行客体。

9.1.3.3 FDP_ACC.1/SYSCALL 子集访问控制测试方法

基于 ST 中的赋值“用户态进程列表”、赋值“系统调用接口列表”输出系统调用访问控制列表,包含系统调用和对应的可访问的用户态进程、不可访问的用户态进程。

FDP_ACC.1/SYSCALL 子集访问控制测试方法如下:

- a) 基于等价类遍历系统调用访问控制列表,利用合法进程访问系统调用,检查是否调用成功;
- b) 基于等价类遍历系统调用访问控制列表,利用非法进程访问系统调用,检查是否调用成功。

9.1.3.4 FDP_ACC.1/Permission 子集访问控制测试方法

基于 ST 中赋值“TOE 提供的系统服务列表”,选择读、写或赋值“其他操作列表”,输出系统服务访问控制列表(按系统服务划分等价类),包含系统服务和对应的操作。

FDP_ACC.1/Permission 子集访问控制测试方法如下:

- a) 遍历系统服务访问控制列表,在终端用户未授权遍历系统服务访问控制列表中的对应操作,检查是否操作成功;
- b) 遍历系统服务访问控制列表,在终端用户已授权遍历系统服务访问控制列表中的对应操作,检查是否操作失败。

9.1.3.5 FDP_ACC.1/UserData 子集访问控制测试方法

基于 ST 中选择“TOE 内部存储”、赋值“其他存储的用户数据”,输出用户数据解密列表(按数据类型划分等价类),包含用户数据类型(如:低级别用户数据、中级别用户数据或高级别用户数据)和对应的解密操作(如:TOE 成功启动、TOE 成功启动且第一次身份鉴别成功或用户身份鉴别成功且 TOE 屏幕解锁)。

FDP_ACC.1/UserData 子集访问控制测试方法如下:

- a) 创建低级别用户数据,在设备成功启动前(如设备刚上电但系统未完成加载)读取数据,检查是否读取数据的明文失败;
- b) 在设备成功启动后读取低级别用户数据,检查是否读取数据的明文成功;

- c) 创建中级别用户数据,设备重启未完成首次身份鉴别时读取数据,检查是否读取数据的明文失败;
- d) 设备完成首次身份鉴别后读取中级别用户数据,检查是否读取数据的明文成功;
- e) 创建高级别用户数据,在锁屏时读取数据,检查是否读取数据的明文失败;
- f) 在解锁时读取高级别用户数据,检查是否读取数据的明文成功。

9.1.3.6 FDP_ACC.1/SEE 子集访问控制测试方法

FDP_ACC.1/SEE 子集访问控制测试方法如下:

- a) 模拟普通运行环境中的应用软件,合法读取隔离执行环境中的服务,检查是否读取成功;
- b) 模拟普通运行环境中的应用软件,非法读取隔离执行环境中的服务,检查是否读取失败;
- c) 模拟普通运行环境中的应用软件,合法写入隔离执行环境中的服务,检查是否写入成功;
- d) 模拟普通运行环境中的应用软件,非法写入隔离执行环境中的服务,检查是否写入失败;
- e) 模拟普通运行环境中的应用软件,合法执行隔离执行环境中的服务,检查是否执行成功;
- f) 模拟普通运行环境中的应用软件,非法执行隔离执行环境中的服务,检查是否执行失败。

9.1.3.7 FDP_ACC.1/DTC 子集访问控制测试方法

对于申请 EAL2+~EAL4+级别的 TOE,FDP_ACC.1/DTC 子集访问控制测试方法如下:

- a) 设备传输数据给对端设备,检查设备是否提醒用户进行确认;
- b) 用户拒绝数据传输,检查数据传输是否失败;
- c) 用户同意数据传输,检查数据传输是否成功。

以下给出结合待传输的数据风险等级、本地设备安全等级、对端设备的安全等级判断是否允许传输数据的方案的测试步骤,其他方案参考以下测试方法执行。

基于 ST 中赋值“待传输的用户数据列表”和对应的设计,输出数据风险等级传输表,包含用户数据类型(如:低级别用户数据、中级别用户数据或高级别用户数据)和数据风险等级(如:一级、二级或三级)及对应允许传输的本地设备安全等级(如:大于或等于一级、大于或等于二级或大于或等于三级)和对端设备安全等级(如:大于或等于一级、大于或等于二级或大于或等于三级)。

对于申请 EAL5+的级别 TOE,FDP_ACC.1/DTC 子集访问控制测试方法如下:

- a) 遍历数据风险等级传输表中的用户数据类型,本地设备安全等级低于允许传输的等级,将数据传输给对端设备,检查是否提示风险,用户拒绝数据传输后,检查数据传输是否失败;
- b) 遍历数据风险等级传输表中的用户数据类型,本地设备安全等级等于或高于允许传输的等级,传输数据给对端设备,检查是否提示风险,用户拒绝数据传输后,检查数据传输是否失败;
- c) 遍历数据风险等级传输表中的用户数据类型,对端设备安全等级低于允许传输的等级,将数据传输给对端设备,检查是否提示风险,用户同意传输后,检查数据传输是否成功;
- d) 遍历数据风险等级传输表中的用户数据类型,对端设备安全等级等于或高于允许传输的等级,将数据传输给对端设备,检查是否提示风险,用户同意传输后,检查数据传输是否成功。

9.1.3.8 FDP_ACF.1/MAC 基于安全属性的访问控制测试方法

测试方法同 9.1.3.1“FDP_ACC.1/MAC 子集访问控制测试方法”。

9.1.3.9 FDP_ACF.1/DAC 基于安全属性的访问控制测试方法

测试方法同 9.1.3.2“FDP_ACC.1/DAC 子集访问控制测试方法”。

9.1.3.10 FDP_ACF.1/SYSCALL 基于安全属性的访问控制测试方法

测试方法同 9.1.3.3“FDP_ACC.1/SYSCALL 子集访问控制测试方法”。

9.1.3.11 FDP_ACF.1/Permission 基于安全属性的访问控制测试方法

测试方法同 9.1.3.4“FDP_ACC.1/Permission 子集访问控制测试方法”。

9.1.3.12 FDP_ACF.1/UserData 基于安全属性的访问控制测试方法

测试方法同 9.1.3.5“FDP_ACC.1/UserData 子集访问控制测试方法”。

9.1.3.13 FDP_ACF.1/SEE 基于安全属性的访问控制测试方法

测试方法同 9.1.3.6“FDP_ACC.1/SEE 子集访问控制测试方法”。

9.1.3.14 FDP_ACF.1/DTC 基于安全属性的访问控制测试方法

测试方法同 9.1.3.7“FDP_ACC.1/DTC 子集访问控制测试方法”。

9.1.3.15 FDP_RIP.2 完全残余信息保护测试方法

基于 ST 设计,输出数据擦除规格表,包含用户数据类型(如:低级别用户数据、中级别用户数据或高级别用户数据)、数据擦除的操作(如:恢复出厂)和数据擦除的结果(如:使用 0x00、0xFF 或随机字节字符,或无意义文件进行依次覆写)。

FDP_RIP.2 完全残余信息保护测试方法如下:

- a) 遍历数据擦除规格表中的用户数据类型,读取被测试数据的 ROM 单元或区域,检查是否存在数据二进制数值;
- b) 执行恢复出厂的操作,然后再次读取被测试数据的 ROM 单元或区域,检查数据二进制数值是否已被擦除(如:ROM 单元或区域是否为写入的字符或无意义文件)。

9.1.3.16 FDP_SDC.1 存储数据的机密性测试方法

测试方法同 9.1.3.5“FDP_ACC.1/UserData 子集访问控制测试方法”。

9.1.4 FIA 类:标识和鉴别测试方法

9.1.4.1 FIA_AFL.1 鉴别失败处理测试方法

基于 ST 中赋值“指定的错误次数(1 到 50 之间的整数)”、选择“口令、PIN、图案、指纹、2D 人脸、3D 人脸或其他”、选择“延时登录、锁定终端、重启设备、删除用户数据”、赋值“降低攻击风险(如暴力攻击)的其他措施列表”,输出鉴别失败处理表,包含鉴别机制(如:口令、PIN、图案、指纹、2D 人脸、3D 人脸或其他)和对应的错误次数阈值及缓解措施(如:延时登录、锁定终端、重启设备、删除用户数据或降低攻击风险的其他措施列表)。

FIA_AFL.1 鉴别失败处理测试方法如下:

- a) 遍历鉴别失败处理表中的鉴别机制,登录连续失败不超过错误次数阈值,检查是否不触发对应的缓解措施;
- b) 遍历鉴别失败处理表中的鉴别机制,登录连续失败超过错误次数阈值,检查是否触发了对应的缓解措施;
- c) 符合鉴别失败对应的缓解措施后,重新输入正确的身份鉴别因子,检查是否登录成功。

9.1.4.2 FIA_SOS.1 秘密的验证测试方法

基于 ST 中的设计,输出秘密强度验证表,包含鉴别机制(如:口令或 PIN)和对应的秘密强度验证

规则(如:口令或 PIN 长度不少于 4 位)。

FIA_SOS.1 秘密的验证测试方法如下:

- a) 遍历秘密强度验证表中的鉴别机制,录入不符合秘密强度的鉴别因子,检查是否录入失败;
- b) 遍历秘密强度验证表中的鉴别机制,录入符合秘密强度的鉴别因子,检查是否录入成功。

9.1.4.3 FIA_SOS.2 TSF 生成秘密测试方法

FIA_SOS.2 TSF 生成秘密测试方法如下:

遍历 ST 中选择的生物信息鉴别机制,按表 3 中各鉴别机制对应的生物样本库测试要求进行比对测试,检查 FAR 和 FRR 是否符合 ST 中对应鉴别机制的指标要求。

表 3 生物信息鉴别测试要求

鉴别机制	生物样本库测试要求(n 代表人数、 m 代表单人采集模板数量、 t 代表比对测试次数)
3D 人脸	$n \times m \times t \geq 1\,000\,000$, 其中 $n \geq 250$ 且 $m \geq 40$
2D 人脸	$n \times m \times t \geq 500\,000$, 其中 $n \geq 75$ 且 $m \geq 160$
指纹	$n \times m \times t \geq 500\,000$, 其中 $n \geq 25$ 且 $m \geq 80$

9.1.4.4 FIA_UAU.1 鉴别的时机测试方法

FIA_UAU.1 鉴别的时机测试方法如下:

- a) 在用户身份鉴别前,遍历执行 ST 赋值的“解锁 TOE 之前允许 TSF 代表用户执行的操作列表”中的操作,检查操作是否执行成功;
- b) 在用户身份鉴别前,通过命令行或快捷键尝试执行 1 个鉴别前不应执行的操作(基于 ST 设计选取),检查操作是否执行失败。

9.1.4.5 FIA_UAU.5/USER 多重鉴别机制测试方法

基于 ST 中的选择“图案、指纹、2D 人脸、3D 人脸或其他鉴别机制”、赋值“描述多重鉴别机制如何提供鉴别的规则”,输出用户多重鉴别机制表,包含用户鉴别机制(口令和 PIN 是必选)及对应的可使用的时机(如:任何时候或非开机启动首次解锁且未达到生物信息失败次数限制时)和无法使用的时机(如:无、开机启动首次解锁或达到生物信息失败次数限制)。

FIA_UAU.5/USER 多重鉴别机制测试方法如下:

- a) 遍历用户多重鉴别机制表中的用户鉴别机制,基于等价类遍历可使用的时机,使用正确的鉴别因子鉴别,检查是否鉴别成功;
- b) 遍历用户多重鉴别机制表中的用户鉴别机制,基于等价类遍历无法使用的时机,尝试使用正确的鉴别因子鉴别,检查是否无鉴别入口,或鉴别失败。

9.1.4.6 FIA_UAU.5/DEVICE 多重鉴别机制测试方法

基于 ST 中的选择“在两个设备上登录相同的用户账号、PIN、二维码、NFC 标签”、赋值“验证对端设备身份的其他机制”、赋值“描述多重鉴别机制如何提供对端设备鉴别的规则”,输出设备多重鉴别机制表,包含设备鉴别机制(如:用户账号、PIN、二维码或 NFC 标签)及对应可使用的时机和无法使用的时机。

FIA_UAU.5/DEVICE 多重鉴别机制测试方法如下:

- a) 遍历设备多重鉴别机制表中的设备鉴别机制,基于等价类遍历可使用的时机,使用正确的鉴

别因子鉴别,检查是否鉴别成功;

- b) 遍历设备多重鉴别机制表中的设备鉴别机制,基于等价类遍历无法使用的时机,尝试使用正确的鉴别因子鉴别,检查是否无鉴别入口,或鉴别失败。

9.1.4.7 FIA_UAU.5/APP 多重鉴别机制测试方法

FIA_UAU.5/APP 多重鉴别机制测试方法如下:

- a) 安装正确数字签名的应用软件,检查是否安装成功;
- b) 安装错误或无数字签名的应用软件,检查是否安装失败。

9.1.4.8 FIA_UAU.6 重鉴别测试方法

基于 ST 中的选择“用户尝试修改用户鉴别因子、用户尝试解锁锁定设备”、赋值“ST 作者提供的需要重鉴别的条件列表”,输出用户重鉴别表,包含用户鉴别机制和对应的重鉴别的时机(如:用户尝试修改用户认证鉴别因子或用户尝试解锁锁定设备)。

FIA_UAU.6 重鉴别测试方法如下:

- a) 遍历用户重鉴别表中的用户鉴别机制,基于等价类遍历重鉴别的时机,检查鉴别入口是否与用户重鉴别表保持一致,无非法入口;
- b) 遍历用户重鉴别表中的用户鉴别机制,基于等价类遍历重鉴别的时机,使用正确的可用于重鉴别的鉴别因子鉴别,检查是否鉴别成功;
- c) 遍历用户重鉴别表中的用户鉴别机制,基于等价类遍历重鉴别的时机,使用错误的可用于重鉴别的鉴别因子鉴别,检查是否鉴别失败。

9.1.4.9 FIA_UAU.7 受保护的鉴别反馈测试方法

基于 ST 中赋值“反馈列表”,输出用户鉴别反馈表,包含用户鉴别机制和对应的鉴别反馈(如:口令或 PIN 解锁时仅反馈占位符或图案解锁时不反馈解锁图案路径)。

FIA_UAU.7 受保护的鉴别反馈测试方法如下:

遍历用户鉴别反馈表中的用户鉴别机制,输入部分鉴别材料,检查用户鉴别机制的鉴别反馈是否与用户鉴别反馈表保持一致。

9.1.4.10 FIA_UID.1 标识的时机测试方法

测试方法同 9.1.4.4“FIA_UAU.1 鉴别的时机测试方法”。

9.1.4.11 FIA_API.1 身份鉴别证明测试方法

基于 ST 中的选择“基于数字签名的鉴别机制”或赋值“其他鉴别机制”、选择“使用 TOE 设备证书签发的证书链”或赋值“其他属性列表”,输出设备鉴别表,包含设备鉴别机制(如:数字签名或其他鉴别机制)和对应的设备身份证明信息(如:使用 TOE 设备证书签发的证书链或其他属性列表)。

FIA_API.1 身份鉴别证明测试方法如下:

遍历设备鉴别表中的设备鉴别机制,触发向外部实体证明设备身份的场景,通过日志或回显打印识别出设备身份证明信息,检查设备身份证明信息是否与设备鉴别表保持一致,且符合业界优秀实践(如:设备身份证明信息为使用 TOE 设备证书签发的证书链时,证书链的一级 CA 代表设备厂商)。

9.1.5 FMT 类:安全管理测试方法

9.1.5.1 FMT_MSA.1/Permission 安全属性的管理测试方法

基于 ST 中的赋值“TOE 提供的系统服务权限”“其他操作”,输出系统服务权限列表,包含系统服

务权限和对应的终端用户可执行的操作(如:查询、修订、其他,其中查询和修订是必选)。

FMT_MSA.1/Permission 安全属性的管理测试方法如下:

遍历系统服务权限列表中的系统服务权限,基于某个应用软件,遍历终端用户可执行的操作(如查询和修订),检查是否操作成功。

9.1.5.2 FMT_MSA.3/Permission 静态属性初始化测试方法

基于 ST 中的设计,选择一个典型的应用软件,输出其默认权限列表(如:读写通讯录或读写图片视频)。

FMT_MSA.3/Permission 静态属性初始化测试方法如下:

- a) 安装选定的典型应用软件,通过系统 UI、命令行或日志打印识别出其默认申请的权限列表,检查所选定的应用软件申请到的权限列表是否与基于 ST 设计输出的默认权限列表一致;
- b) 终端用户主动增加、删除选定的应用软件申请的初始权限,通过系统 UI、命令行或日志打印识别出其默认申请的权限列表,检查所选定的应用软件申请到的权限列表是否与终端用户设置的列表一致。

9.1.5.3 FMT_SMF.1 管理功能测试方法

FMT_SMF.1 管理功能测试方法如下:

- a) 设置锁屏口令,用设置的口令解锁屏幕,检查是否解锁成功;
- b) 修改锁屏口令,用修改后的口令解锁屏幕,检查是否解锁成功;
- c) 设置锁屏 PIN,用设置的 PIN 解锁屏幕,检查是否解锁成功;
- d) 修改锁屏 PIN,用修改后的 PIN 解锁屏幕,检查是否解锁成功;
- e) 注册锁屏指纹,用注册的指纹解锁屏幕,检查是否解锁成功;
- f) 修改锁屏指纹,用修改后的指纹解锁屏幕,检查是否解锁成功;
- g) 注册锁屏人脸,用注册的人脸解锁屏幕,检查是否解锁成功;
- h) 修改锁屏人脸,用修改后的人脸解锁屏幕,检查是否解锁成功;
- i) 安装某个应用软件,通过系统 UI 或命令行查询其权限,检查是否成功查询到应用软件的权限;
- j) 终端用户通过系统 UI 或命令行修改(如:增加或删除)这个应用软件的权限,然后再次查询其权限,检查是否成功修改应用软件的权限;
- k) 创建全级别用户数据(如低等级、中等级或高等级),执行恢复出厂操作,检查是否恢复出厂设置成功且正确擦除用户数据;
- l) 终端用户通过应用安装平台(如系统自带的应用市场),下载、安装、卸载和更新某个应用软件,检查下载、安装、卸载、更新操作是否操作成功;
- m) 终端用户通过系统设置查询 TOE 软件版本,检查是否查询到正确的 TOE 版本号;
- n) 终端用户通过系统设置更新 TOE 软件版本,检查是否更新成功且 TOE 版本号正确;
- o) 遍历 ST 赋值的“其他安全管理功能”,触发安全管理功能,检查安全管理功能是否正常生效(如检测出病毒、备份正确恢复等)。

9.1.6 FPR 类:隐私测试方法

9.1.6.1 FPR_PSE.1/APPDEV 假名测试方法

基于 ST 设计,输出第三方应用假名表,包含身份类型(如:设备身份或用户身份)、真实身份 ID(如:设备的 IMEI 或 SN 等,或用户的姓名)和假名 ID(如:设备假名标识或用户假名标识)。

FPR_PSE.1/APPDEV 假名测试方法如下：

- a) 模拟第三方应用直接访问设备标识(如 IMEI 或 SN),检查是否访问失败；
- b) 模拟第三方应用获取设备硬件标识,检查是否获取设备假名标识且无法推理出真实设备标识；
- c) 模拟第三方应用获取用户标识,检查是否获取用户假名标识且无法推理出真实用户标识；
- d) 终端用户主动重置标识,模拟第三方应用再次获取用户标识,检查是否获取用户假名标识,用户假名标识是否不同于步骤 c)中的用户假名标识,且无法推理出真实用户标识。

9.1.6.2 FPR_PSE.1/AD 假名测试方法

基于 ST 设计,输出广告假名表,包含身份类型(如:设备身份或用户身份)、真实身份 ID(如:设备的 IMEI 或 SN 等,或用户的姓名)和假名 ID(如:设备假名标识或用户假名标识)。

FPR_PSE.1/AD 假名测试方法如下：

- a) 模拟广告平台直接访问设备标识(如 IMEI 或 SN),检查是否访问失败；
- b) 模拟广告平台获取设备硬件标识,检查是否获取设备假名标识,且无法推理出真实设备标识；
- c) 模拟广告平台获取用户标识,检查是否获取用户假名标识,且无法推理出真实用户标识；
- d) 终端用户主动重置标识,模拟广告平台再次获取用户标识,检查是否获取用户假名标识,用户假名标识是否不同于步骤 c)中的用户假名标识,且无法推理出真实用户标识。

9.1.7 FPT 类:TSF 保护测试方法

9.1.7.1 FPT_AEX_EXT.1 地址空间布局随机化测试方法

FPT_AEX_EXT.1 地址空间布局随机化测试方法如下：

- a) 启动设备,使用工具、命令行或日志打印出进程(选一个典型进程即可)和内核的地址空间布局 1 和 2；
- b) 重启设备,使用工具、命令行或日志打印出进程和内核的地址空间布局 3 和 4；
- c) 再次重启设备,使用工具、命令行或日志打印出进程和内核的地址空间布局 5 和 6；
- d) 对比进程地址空间布局 1、3 和 5,检查进程地址空间布局 1、3 和 5 是否不一致且无明显的规律；
- e) 对比内核地址空间布局 2、4 和 6,检查内核地址空间布局 2、4 和 6 是否不一致且无明显的规律。

9.1.7.2 FPT_AEX_EXT.2 内存页权限控制测试方法

基于 ST 中的选择“数据不可执行、特权模式不可执行、特权模式不可访问、可写内存不可执行、内存只可执行”、赋值“其他内存保护机制”,输出内存页权限控制机制列表,每种机制对应需要执行的测试步骤见表 4,其中步骤 a)~步骤 i)见内存页权限控制测试方法描述。

表 4 内存页权限控制机制及对应测试步骤

内存页权限控制机制	对应测试步骤
数据不可执行	a)
特权模式不可执行	b)
特权模式不可访问	c)

表 4 内存页权限控制机制及对应测试步骤（续）

内存页权限控制机制	对应测试步骤
可写内存不可执行	d)和 e)
内存只可执行	f)和 g)
其他内存保护机制	h)和 i)

FPT_AEX_EXT.2 内存页权限控制测试方法如下：

- a) 使用用户态测试程序执行被标记了数据不可执行的内存数据,检查是否执行失败；
- b) 使用内核态测试程序执行被标记了特权模式不可执行的内存数据,检查是否执行失败；
- c) 使用内核态测试程序读写被标记了特权模式不可访问的内存数据,检查是否读取和写入失败；
- d) 使用用户态测试程序执行被标记了可写内存不可执行的内存数据,检查是否执行失败；
- e) 使用用户态测试程序写入被标记了可写内存不可执行的内存数据,检查是否写入成功；
- f) 使用用户态测试程序读写被标记了内存只可执行的内存数据,检查是否读取和写入失败；
- g) 使用用户态测试程序执行被标记了内存只可执行的内存数据,检查是否执行成功；
- h) 遍历其他内存保护机制,构造违反保护机制的场景,检查是否操作失败；
- i) 遍历其他内存保护机制,构造符合保护机制的场景,检查是否操作成功。

9.1.7.3 FPT_AEX_EXT.3 缓冲区溢出保护测试方法

基于 ST 中的选择“基于栈的缓冲区溢出保护、基于堆的缓冲区溢出保护”,输出缓冲区溢出保护机制列表,每种机制对应需要执行的测试步骤见表 5,其中步骤 a)、步骤 b)见缓冲区溢出保护测试方法描述。

表 5 缓冲区溢出保护机制及对应测试步骤

缓冲区溢出保护机制	对应测试步骤
栈溢出保护	a)
堆溢出保护	b)

FPT_AEX_EXT.3 缓冲区溢出保护测试方法如下：

- a) 使用测试程序触发栈溢出场景,通过系统行为或日志打印识别出拦截效果(如重启、正常结束或强制终止进程等),检查 TOE 是否成功拦截栈溢出；
- b) 使用测试程序触发堆溢出场景,通过系统行为或日志打印识别出拦截效果(如重启、正常结束或强制终止进程等),检查 TOE 是否成功拦截堆溢出。

9.1.7.4 FPT_AEX_EXT.4 内核完整性保护测试方法

基于 ST 中的选择“内核代码段只读保护、内核数据段不可执行、系统控制寄存器写保护、强制访问控制策略防篡改”、赋值“其他内核完整性保护机制”,输出内核完整性保护机制列表,每种机制对应需要执行的测试步骤见表 6,其中步骤 a)~步骤 h)见内核完整性保护测试方法描述。

表 6 内核完整性保护机制及对应测试步骤

内核完整性保护机制	对应测试步骤
内核代码段只读保护	a)和 b)
内核数据段不可执行	c)和 d)
系统控制寄存器写保护	e)
强制访问控制策略防篡改	f)
其他内核完整性保护机制	g)和 h)

FPT_AEX_EXT.4 内核完整性保护测试方法如下：

- a) 使用内核态测试程序写入和执行内核代码段中的数据,检查写入和执行是否执行失败；
- b) 使用内核态测试程序读取内核代码段中的数据,检查是否读取成功；
- c) 使用内核态测试程序执行内核数据段中的数据,检查是否执行失败；
- d) 使用内核态测试程序读取和写入内核数据段中的数据,检查是否读取和写入成功；
- e) 遍历 TOE 保护的寄存器,使用内核态测试程序写入寄存器,检查是否写入失败；
- f) 使用内核态测试程序篡改强制访问控制策略文件,检查是否篡改失败；
- g) 遍历其他内核完整性保护机制,构造违反保护机制的场景,检查是否操作失败；
- h) 遍历其他内核完整性保护机制,构造符合保护机制的场景,检查是否操作成功。

9.1.7.5 FPT_AEX_EXT.5 控制流完整性保护测试方法

基于 ST 中的选择“前向控制流完整性、后向控制流完整性、指针鉴别”、赋值“其他控制流完整性保护机制”,输出控制流完整性保护机制列表,每种机制对应需要执行的测试步骤见表 7,其中步骤 a)~步骤 d)见控制流完整性保护测试方法描述。

表 7 控制流完整性保护机制及对应测试步骤

控制流完整性保护机制	对应测试步骤
前向控制流完整性	a)
后向控制流完整性	b)
指针鉴别	c)
其他控制流完整性保护机制	d)

FPT_AEX_EXT.5 控制流完整性保护测试方法如下：

- a) 通过日志打印或命令行识别出 TOE 开启的编译选项,检查是否开启前向控制流完整性保护(如使用编译器控制流完整性或控制流保护技术)；
- b) 通过日志打印或命令行识别出 TOE 开启的编译选项,检查是否开启后向控制流完整性保护(如使用镜像调用栈或返回流保护技术)；
- c) 通过日志打印或命令行识别出 TOE 开启的编译选项,检查是否开启指针鉴别保护(如 ARM 指针认证码或英特尔控制流增强技术)；
- d) 遍历其他控制流完整性保护机制,通过日志打印或命令行识别出 TOE 开启的编译选项,检查是否开启其他控制流完整性保护。

9.1.7.6 FPT_FLS.1 失效即保持安全状态测试方法

FPT_FLS.1 失效即保持安全状态测试方法如下：

- a) TOE 系统更新过程中通过强制重启或掉电,检查系统版本号是否能回滚到升级前的状态；
- b) 在当前情形下,抽检三个 TSF 保护能力(如地址空间布局随机化),检查抽检的三个 TSF 保护能力是否正常；
- c) 在当前情形下,重新触发 TOE 系统更新,检查 TOE 系统软件是否能更新成功。

9.1.7.7 FPT_JTA_EXT.1 JTAG 接口访问控制测试方法

基于 ST 中的选择“通过硬件断开物理连接、通过签名密钥进行接入鉴别”,输出 JTAG 接口访问控制方法列表,每种方法对应需要执行的测试步骤见表 8,其中步骤 a)~步骤 c)见 JTAG 接口访问控制测试方法描述。

表 8 JTAG 接口访问控制方法及对应测试步骤

JTAG 接口访问控制方法	对应测试步骤
通过硬件断开物理连接	a)
通过签名密钥进行接入鉴别	b)和 c)

FPT_JTA_EXT.1 JTAG 接口访问控制测试方法如下。

- a) 拆机或由厂商提供证据,检查 TOE 硬件上的 JTAG 接口是否被物理消除且无外接点；
- b) 通过测试工具使用正确的数字证书或密钥访问 JTAG 接口,检查是否鉴别成功；
- c) 通过测试工具使用错误的数字证书或密钥(如过期或型号不对应)访问 JTAG 接口,检查是否鉴别失败。

9.1.7.8 FPT_PHP.3 物理攻击抵抗测试方法

基于 ST 描述和业界优秀实践,输出物理攻击方法表,包含物理攻击方法和对应的 TOE 抵抗力的证据(如:某功能设计描述)。

FPT_PHP.3 物理攻击抵抗测试方法如下：

厂商提供 TOE 的隔离执行环境的设计证据(如方案、型号、证书或源码),检查 TOE 是否抵御电磁泄露或激光注入等典型物理攻击。

9.1.7.9 FPT_RCV.2 自动恢复测试方法

FPT_RCV.2 自动恢复测试方法如下：

- a) 在 TOE 启动阶段刷入被篡改的镜像,检查系统是否进入维护模式；
- b) 在维护模式下,重新刷入正确的镜像,检查系统是否重新恢复到正常模式。

9.1.7.10 FPT_SEE_EXT.1 隔离执行环境测试方法

基于 ST 描述和业界优秀实践,输出隔离执行环境表,包含隔离执行环境实现方法和对应的安全性证据(如某功能设计描述),每种方法对应需要执行的测试步骤见表 9,其中步骤 a)~步骤 c)见隔离执行环境测试方法描述。

表 9 隔离执行环境方法及对应测试步骤

隔离执行环境实现方法	对应测试步骤
基于处理器隔离模式实现	a)
基于处理器集成安全处理单元实现	b)
基于独立安全处理单元实现	c)

FPT_SEE_EXT.1 隔离执行环境测试方法如下：

- a) 厂商提供 TOE 的隔离执行环境的设计证据(如方案、型号、证书或源码),检查是否符合处理器隔离模式的业界优秀实践；
- b) 厂商提供 TOE 的隔离执行环境的设计证据(如方案、型号、证书或源码),检查是否符合处理器集成安全处理单元的业界优秀实践；
- c) 厂商提供 TOE 的隔离执行环境的设计证据(如方案、型号、证书或源码),检查是否符合独立安全处理单元的业界优秀实践。

9.1.7.11 FPT_STG_EXT.1 TSF 数据存储测试方法

基于 ST 对 FPT_STG_EXT.1.1 的设计描述,输出数据安全存储表,包含数据类型(如:口令、PIN、指纹鉴别模板和/或指纹鉴别模板加密密钥、人脸鉴别模板和/或人脸鉴别模板加密密钥或其他 TSF 数据)和对应的隔离执行环境(如:处理器隔离模式、处理器集成安全处理单元或独立安全处理单元),不同数据类型需要执行的测试步骤见表 10,其中步骤 a)~步骤 e)见 TSF 数据存储测试方法描述。

表 10 不同数据类型及对应测试步骤

数据类型	对应测试步骤
口令	a)
PIN	b)
指纹鉴别模板和/或指纹鉴别模板加密密钥	c)
人脸鉴别模板和/或人脸鉴别模板加密密钥	d)
其他 TSF 数据	e)

FPT_STG_EXT.1 TSF 数据存储测试方法如下：

- a) 执行口令的注册和鉴别操作,通过日志打印或代码片段识别出口令数据关键字、隔离环境关键字,检查口令数据的存储是否发生在隔离环境中,且隔离环境与数据安全存储表中一致；
- b) 执行 PIN 的注册和鉴别操作,通过日志打印或代码片段识别出 PIN 数据关键字、隔离环境关键字,检查 PIN 数据的存储是否发生在隔离环境中,且隔离环境与数据安全存储表中一致；
- c) 执行指纹的注册和鉴别操作,通过日志打印或代码片段识别出指纹数据关键字、隔离环境关键字,检查指纹数据的存储是否发生在隔离环境中,且隔离环境与数据安全存储表中一致；
- d) 执行人脸的注册和鉴别操作,通过日志打印或代码片段识别出人脸数据关键字、隔离环境关键字,检查人脸数据的存储是否发生在隔离环境中,且隔离环境与数据安全存储表中一致；
- e) 遍历触发其他 TSF 数据的业务场景,通过日志打印或代码片段识别出数据关键字、隔离环境关键字,检查 TSF 数据的存储是否发生在隔离环境中,且隔离环境与数据安全存储表中

一致。

注：FPT_STG_EXT.1.2的测试方法同9.1.2.10“FCS_COP.1/ENCRYPT 密码运算测试方法”；FPT_STG_EXT.1.3的测试方法同9.1.2.10“FCS_COP.1/ENCRYPT 密码运算测试方法”、9.1.2.11“FCS_COP.1/HASH 密码运算测试方法”、9.1.2.12“FCS_COP.1/KEYHMAC 密码运算测试方法”。

9.1.7.12 FPT_STM.1 可靠的时间戳测试方法

FPT_STM.1 可靠的时间戳测试方法如下：

基于操作指南设置 TOE 的时间，然后通过系统 UI 或命令行观察时间，检查设置的时间是否正确生效。

9.1.7.13 FPT_TST_EXT.1 启动完整性验证测试方法

基于 ST 描述梳理出启动规格表，包含启动入口[如：快速启动模式(Fastboot)、恢复模式(Recovery)或救援模式(Rescue)]和对应的镜像列表。

FPT_TST_EXT.1 启动完整性验证测试方法如下：

- a) 遍历启动规格表中的启动入口，刷入合法镜像，检查 TOE 是否能正确启动，进入对应的系统模式；
- b) 遍历启动规格表中的启动入口，基于等价类刷入被篡改的非法镜像，检查 TOE 是否拦截非法启动成功，且启动失败。

9.1.7.14 FPT_TST_EXT.2 运行完整性验证测试方法

基于 ST 中的赋值“TSF 的组成部分或 TSF 数据”、选择“基于处理器隔离模式实现的隔离执行环境、基于处理器集成安全处理单元实现的隔离执行环境、基于独立安全处理单元实现的隔离执行环境”，输出运行完整性验证表，包含 TSF 数据和对应的隔离执行环境(如：处理器隔离模式、处理器集成安全处理单元或独立安全处理单元)。

FPT_TST_EXT.2 运行完整性验证测试方法如下：

- a) TOE 正常启动触发安全自检，通过审计日志识别出隔离环境关键字和自检结果信息，检查是否自检成功，且自检环境与运行完整性验证表一致；
- b) 基于等价类篡改运行完整性验证表中的 TSF 数据，再次触发 TOE 安全自检，通过审计日志识别出隔离环境关键字和自检结果信息，检查是否自检失败，且自检环境与运行完整性验证表一致。

9.1.7.15 FPT_TUD_EXT.1/OS 系统软件更新测试方法

FPT_TUD_EXT.1/OS 系统软件更新测试方法如下：

- a) 下载正确签名的系统软件升级包并安装，通过日志打印或代码片段识别出校验更新包公钥的关键字，检查是否升级成功，且校验的公钥是否为 TOE 中预置的不可篡改证书中的公钥；
- b) 下载错误或无数字签名的系统软件升级包并安装，检查是否升级失败。

9.1.7.16 FPT_TUD_EXT.1/APP 应用软件验证测试方法

FPT_TUD_EXT.1/APP 应用软件验证测试方法如下：

- a) 下载正确签名的应用软件升级包并安装，通过日志打印或代码片段识别出校验更新包公钥的关键字，检查是否升级成功且校验公钥为 ST 中选择的“与首次安装时存储在 TOE 中证书的公钥一致的公钥”或“为 TOE 中预置的不可篡改证书中的公钥”；
- b) 下载错误或无数字签名的应用软件升级包并安装，检查是否升级失败。

9.1.8 FTA类:TOE访问测试方法

9.1.8.1 FTA_SSL.1 TSF 原发会话锁定测试方法

FTA_SSL.1 TSF 原发会话锁定测试方法如下:

- a) 基于等价类遍历 ST 赋值的“用户不活动的时间间隔”,设置设备锁定时间为该时间间隔,使用户不操作设备的时间间隔超过设置的锁定时间,检查设备是否正常锁定;
- b) 设备锁定状态时,触发短信写入,检查设备是否正常收到短信;
- c) 设备锁定状态时,触发电话呼入和通话,检查设备是否显示来电信息界面且在通话结束后应恢复锁定;
- d) 设备锁定状态时,触发相机拍照,检查设备是否正常拍照;
- e) 设备锁定状态时,遍历触发 ST 赋值的“其他允许的操作”,检查设备是否操作成功;
- f) 设备锁定状态时,完成终端用户的鉴别,查看设备是否解锁成功。

9.1.8.2 FTA_SSL.2 用户原发会话锁定测试方法

FTA_SSL.2 用户原发会话锁定测试方法如下:

- a) 用户通过快捷键锁定设备,检查设备是否正常锁定;
- b) 设备锁定状态时,触发短信写入,检查设备是否正常收到短信;
- c) 设备锁定状态时,触发电话呼入和通话,检查设备是否显示来电信息界面且在通话结束后应恢复锁定;
- d) 设备锁定状态时,触发相机拍照,检查设备是否正常拍照;
- e) 设备锁定状态时,遍历触发 ST 赋值的“其他允许的操作”,检查设备是否操作成功;
- f) 设备锁定状态时,完成终端用户的鉴别,查看设备是否解锁成功。

9.1.9 FTP类:可信路径/信道测试方法

9.1.9.1 FTP_ITC.1/TLS TSF 间可信信道测试方法

基于 ST 中的赋值“ST 作者指定的另一个可信 IT 产品”、赋值“其他需要可信信道的功能列表”,输出可信 IT 产品可信信道表,包含场景(如:系统软件更新包下载)和对应的可信信道(如可信信道使用的 TLS 版本)。

FTP_ITC.1/TLS TSF 间可信信道测试方法如下:

遍历远程可信 IT 可信信道表中的场景,通过工具抓包[如网络数据包捕获命令(tcpdump)]并解析[如网络封包分析工具(wireshark)]识别出 TLS 协议的版本号,检查 TLS 协议是否与可信 IT 产品可信信道表一致,且可信信道安全协议版本符合业界安全性要求(如 TLS 协议版本大于或等于 1.2)。

9.1.9.2 FTP_ITC.1/DEVICE TSF 间可信信道测试方法

如果可信信道是开源协议执行步骤 a),如果是自研协议执行步骤 b)。基于 ST 中的赋值“其他需要使用设备间可信信道的功能列表”,输出移动终端间可信信道表,包含场景(如:TOE 与其他移动终端进行设备间数据传输)和对应的可信信道(如:设备间信道使用的开源协议或自研协议)。

FTP_ITC.1/DEVICE TSF 间可信信道测试方法如下:

- a) 遍历移动终端间可信信道表中的场景,通过抓包解析识别出开源协议的版本号,检查使用开源协议的可信信道是否与移动终端间可信信道表一致,且可信信道安全协议版本符合业界优秀实践(如 TLS 协议版本大于或等于 1.2);

- b) 遍历移动终端间可信信道表中的场景,通过日志打印或代码片段识别出保护信道机密性/完整性的密码算法、密钥长度,检查使用自研协议的可信信道密码算法的密钥安全强度是否大于 112 位。

9.2 安全保障要求的评估方法

9.2.1 ADV 类评估方法

安全保障类 ADV 类的评估方法见 GB/T 30270—2024 中第 13 章,具体见表 11。

表 11 ADV 类

保障类	保障组件	评估方法对应 GB/T 30270—2024 章条号
ADV 类	ADV_ARC.1	13.3.1
	ADV_FSP.2	13.4.2
	ADV_FSP.3	13.4.3
	ADV_FSP.4	13.4.4
	ADV_FSP.5	13.4.5
	ADV_IMP.1	13.5.1
	ADV_INT.2	13.6.2
	ADV_TDS.1	13.8.1
	ADV_TDS.2	13.8.2
	ADV_TDS.3	13.8.3
	ADV_TDS.4	13.8.4

9.2.2 AGD 类评估方法

安全保障类 AGD 类的评估方法见 GB/T 30270—2024 中第 14 章,具体见表 12。

表 12 AGD 类

保障类	保障组件	评估方法对应 GB/T 30270—2024 章条号
AGD 类	AGD_OPE.1	14.3.1
	AGD_PRE.1	14.4.1

9.2.3 ALC 类评估方法

安全保障类 ALC 类的评估方法见 GB/T 30270—2024 中第 15 章,具体见表 13。

表 13 ALC 类

保障类	保障组件	评估方法对应 GB/T 30270—2024 章条号
ALC 类	ALC_CMC.2	15.2.2
	ALC_CMC.3	15.2.3
	ALC_CMC.4	15.2.4

表 13 ALC 类（续）

保障类	保障组件	评估方法对应 GB/T 30270—2024 章条号
ALC 类	ALC_CMS.2	15.3.2
	ALC_CMS.3	15.3.3
	ALC_CMS.4	15.3.4
	ALC_CMS.5	15.3.5
	ALC_DEL.1	15.4.1
	ALC_DVS.1	15.5.1
	ALC_FLR.1	15.6.1
	ALC_FLR.3	15.6.3
	ALC_LCD.1	15.7.1
	ALC_TAT.1	15.9.1
	ALC_TAT.2	15.9.2

9.2.4 ASE 类评估方法

安全保障类 ASE 类的评估方法见 GB/T 30270—2024 中第 12 章,具体见表 14。

表 14 ASE 类

保障类	保障组件	评估方法对应 GB/T 30270—2024 章条号
ASE 类	ASE_CCL.1	12.4.1
	ASE_ECD.1	12.7.1
	ASE_INT.1 ST	12.3.1
	ASE_OBJ.2	12.6.2
	ASE_REQ.2	12.8.2
	ASE_SPD.1	12.5.1
	ASE_TSS.1	12.9.1

9.2.5 ATE 类评估方法

安全保障类 ATE 类的评估方法见 GB/T 30270—2024 中第 16 章,具体见表 15。

表 15 ATE 类

保障类	保障组件	评估方法对应 GB/T 30270—2024 章条号
ATE 类	ATE_COV.1	16.3.1
	ATE_COV.2	16.3.2
	ATE_DPT.1	16.4.1

表 15 ATE 类（续）

保障类	保障组件	评估方法对应 GB/T 30270—2024 章条号
ATE 类	ATE_DPT.2	16.4.2
	ATE_DPT.3	16.4.3
	ATE_FUN.1	16.5.1
	ATE_IND.2	16.6.2

9.2.6 AVA 类评估方法

安全保障类 AVA 类的基本评估方法见 GB/T 30270—2024 中第 17 章,具体见表 16。

表 16 AVA 类

保障类	保障组件	评估方法对应 GB/T 30270—2024 章条号
AVA 类	AVA_VAN.2	17.2.2
	AVA_VAN.3	17.2.3
	AVA_VAN.4	17.2.4

在 GB/T 30270—2024 相关章节脆弱性评估方法的基础上,本文件对移动终端对脆弱性评估进行细化,具体见 9.3。

9.3 脆弱性评估测试细则

9.3.1 信息收集

在脆弱性评估中,信息收集是一个至关重要的阶段,可帮助测试人员深入了解目标系统的基本情况、潜在漏洞和缺陷,为后续的脆弱性分析和穿透性攻击奠定基础。以下是一些常用的信息收集方式。

- a) TOE 产商提供产品信息:利用厂商提供的用户手册、设计文档、接口文档等资料,以及通过端口扫描工具、Web 应用软件扫描工具或漏洞扫描器等技术手段,对目标系统进行扫描,以获取 TOE 开放的端口、服务、预装的应用软件、操作系统版本、内核版本和处理器型号等关键信息。
- b) 公开渠道收集的漏洞或脆弱性相关信息:基于 TOE 厂商资料中获取的信息,如操作系统版本、内核版本、处理器型号等,通过搜索引擎、安全会议或漏洞库等公开渠道,搜集与 TOE 相关的漏洞、攻击路径等脆弱性信息。

在进行信息收集时,脆弱性评估人员应根据目标系统的特点和测试的具体目标选择最合适的信息收集方式。

9.3.2 脆弱性分析

9.3.2.1 目的

脆弱性评定活动的目的是确定 TOE 在预期使用环境下的缺陷或漏洞的存在及其可利用性。这种确定是基于评估者分析结果,并由评估者的测试结果予以证明。

9.3.2.2 脆弱性分析方法

在最低等级的脆弱性分析中,评估者仅通过执行公开可用信息的调查来识别 TOE 上是否存在已知弱点;在更高级别的分析中,评估者需对 TOE 的评估证据执行结构化的分析。

脆弱性分析对象 TOE 从操作系统(包括应用层、框架层和内核层)、硬件平台(包括固件层和硬件层)以单独分析的形式被执行,其中操作系统包括应用层、框架层和内核层,若操作系统提供了隔离执行环境,则隔离执行环境也应进行脆弱性分析;硬件平台包括固件层和硬件层,见图 11。

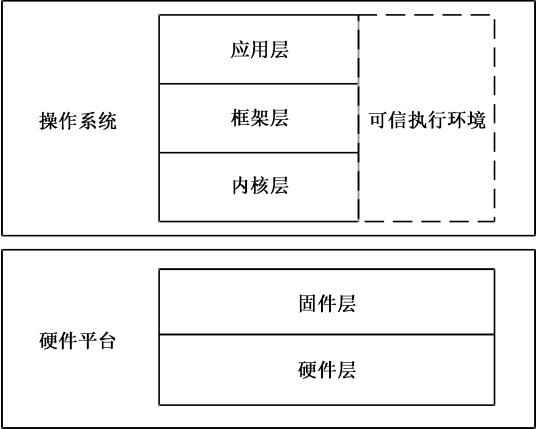


图 11 脆弱性分析方法

在执行脆弱性分析后,还应评定潜在脆弱性影响、通过穿透性测试确定脆弱性的可利用性。上述过程是迭代的,即对潜在脆弱性的穿透测试过程中可能又识别出新的潜在脆弱性问题。

9.3.2.3 操作系统脆弱性分析

9.3.2.3.1 应用层脆弱性分析

应用层涉及的脆弱点见表 17。

表 17 应用层脆弱点

系统对应层级	脆弱点	描述
应用层	AVA_VAN.APP.1	访问控制缺陷
	AVA_VAN.APP.2	端口或服务暴露缺陷
	AVA_VAN.APP.3	敏感数据暴露缺陷
	AVA_VAN.APP.4	内存操作缺陷
	AVA_VAN.APP.5	资源竞争缺陷
	AVA_VAN.APP.6	签名绕过缺陷
	AVA_VAN.APP.7	功能校验绕过缺陷
	AVA_VAN.APP.8	输入校验缺陷
	AVA_VAN.APP.9	目录遍历缺陷
	AVA_VAN.APP.10	文件或数据解析缺陷
	AVA_VAN.APP.11	默认配置缺陷
	AVA_VAN.APP.12	密钥管理缺陷
	AVA_VAN.APP.13	加密算法缺陷

基于应用层脆弱点,应用层脆弱性分析如下:

- a) 访问控制缺陷 AVA_VAN.APP.1:某个应用程序的访问控制存在缺陷(如未进行访问权限控制或访问权限保护级别过低等),使得未授权的用户或实体能利用该缺陷获得超出其正常权限的访问权限,导致应用文件被非法篡改或删除、应用敏感功能被非法访问或用户数据被未经授权的访问等;
- b) 端口或服务暴露缺陷 AVA_VAN.APP.2:某个应用程序暴露了应用的非必要端口或服务,利用该缺陷可非法访问应用资源,导致应用数据被非法访问或应用敏感功能被未授权使用等;
- c) 敏感数据暴露缺陷 AVA_VAN.APP.3:某个应用程序未对应用敏感数据(如密钥或用户数据等)进行加密或访问控制保护,利用该缺陷可非法获得应用敏感数据;
- d) 内存操作缺陷 AVA_VAN.APP.4:某个应用程序代码中存在内存操作缺陷(如释放后重用、缓冲区溢出、读写越界或整数溢出等),利用该缺陷可对应用程序的任意地址空间进行访问,导致数据非法访问或应用程序非法控制,以及应用敏感功能的未授权访问等;
- e) 资源竞争缺陷 AVA_VAN.APP.5:某个应用程序存在资源竞争缺陷[如检查时间到使用时间竞争(Time-of-Check to Time-of-Use)],利用该缺陷可对应用部分资源进行修改或访问,导致应用程序出现拒绝服务、应用文件被非法访问或应用被执行恶意代码等;
- f) 签名绕过缺陷 AVA_VAN.APP.6:某个应用程序签名校验过程存在绕过缺陷,利用该缺陷可非法访问应用程序开发接口、非法修改应用文件或非法加载恶意文件,导致用户数据被非法篡改或应用被非法控制等;
- g) 功能校验绕过缺陷 AVA_VAN.APP.7:对某个应用程序功能进行访问时存在功能校验绕过缺陷(如绕过屏幕锁等),利用该缺陷可非法访问应用受保护的功能或数据,导致用户数据被非法篡改或应用被非法控制等;
- h) 输入校验缺陷 AVA_VAN.APP.8:某个应用程序处理接口存在输入校验缺陷(如对用户输入的数据未严格验证输入内容或验证逻辑不够完善),可利用该缺陷对应用程序进行拒绝服务攻击、SQL 注入攻击、XSS 攻击或命令注入攻击等,导致应用程序崩溃或用户数据被非法访问;
- i) 目录遍历缺陷 AVA_VAN.APP.9:当某个应用程序对文件进行处理时(如创建文件、解压文件或删除文件等)未对文件路径进行正确校验(如未校验文件名中或文件路径中所包含的“../”字符串等),可能导致应用程序受到目录遍历攻击,利用该缺陷可访问应用中未经授权的文件和目录,导致应用程序被拒绝服务攻击或应用文件被非法创建、访问或修改等;
- j) 文件或数据解析缺陷 AVA_VAN.APP.10:某个应用程序在解析文件或数据流时存在缺陷(如媒体流解析错误或配置文件字段处理错误等),利用该缺陷可触发内存操作缺陷(AVA_VAN.APP.4)或应用程序异常,导致应用程序崩溃或应用被非法攻占;
- k) 默认配置缺陷 AVA_VAN.APP.11:某个应用程序的默认配置存在缺陷(如默认开启调试开关、使用默认密码或使用不安全的传输协议等),利用该缺陷可非法调试应用、非法访问用户数据或非法访问应用功能,导致数据泄露、应用程序拒绝服务或应用程序被非法控制等;
- l) 密钥管理缺陷 AVA_VAN.APP.12:某个应用程序存在密钥管理缺陷(如硬编码密钥、明文保存密钥或密钥生存周期管理不足等),可利用该缺陷提取应用关键密钥信息,导致敏感信息泄露、用户数据被非法访问等;
- m) 加密算法缺陷 AVA_VAN.APP.13:某个应用程序采用的加密算法存在缺陷(如弱加密算法或私有算法等),利用该缺陷可破解应用加解密过程,导致用户数据被非法访问等。

9.3.2.3.2 框架层脆弱性分析

框架层脆弱点见表 18。

表 18 框架层脆弱点

系统对应层级	脆弱点	描述
框架层	AVA_VAN.FRA.1	访问控制缺陷
	AVA_VAN.FRA.2	端口或服务暴露
	AVA_VAN.FRA.3	运行时代码缺少完整性校验
	AVA_VAN.FRA.4	输入校验缺陷
	AVA_VAN.FRA.5	资源竞争缺陷
	AVA_VAN.FRA.6	目录遍历缺陷
	AVA_VAN.FRA.7	文件或数据解析缺陷
	AVA_VAN.FRA.8	密钥管理缺陷
	AVA_VAN.FRA.9	加密算法缺陷

基于框架层脆弱点,框架层脆弱性分析如下:

- a) 访问控制缺陷 AVA_VAN.FRA.1:框架层服务接口存在访问控制缺陷(如接口未进行访问权限控制或接口访问权限保护级别过低等),利用该缺陷可获得超出其应有级别的访问权限,导致文件被非法篡改或删除、用户数据被非法访问等;
- b) 端口或服务暴露缺陷 AVA_VAN.FRA.2:框架层暴露了非必要的端口或服务,利用该缺陷可非法访问系统资源或服务,导致用户数据被非法访问或敏感功能被非法调用;
- c) 运行时代码缺少完整性校验 AVA_VAN.FRA.3:框架层在运行时未对应用软件代码进行完整性校验,利用该缺陷可修改或覆盖运行时代码,并执行被非法篡改后的代码,进而攻占应用软件,导致应用软件被非法控制、应用数据泄露或应用软件拒绝服务等;
- d) 输入校验缺陷 AVA_VAN.FRA.4:框架层服务接口存在输入参数校验缺陷(如未正确判断输入参数类型或未对数组长度进行正确校验等),使输入参数超出程序处理的预期,利用该缺陷可对框架层服务接口实施拒绝服务攻击、SQL 注入攻击或命令注入攻击等,导致框架层服务崩溃或用户数据被非法访问;
- e) 资源竞争缺陷 AVA_VAN.FRA.5:在框架层服务接口支持多进程或多线程同时访问的情况下,当两个或更多线程同时尝试访问和修改同一资源时,可能产生竞争条件,利用该缺陷可非法操作数据(如写入文件操作的瞬间对文件进行非法数据注入),导致文件或数据被非法篡改等;
- f) 目录遍历缺陷 AVA_VAN.FRA.6:当框架层服务对文件进行处理时(如创建文件、解压文件或删除文件等)未对文件路径进行正确校验(如未校验文件名中或文件路径中所包含的“../”字符串等),可能导致框架层服务受到目录遍历攻击,利用该缺陷可访问框架层服务中未经授权的文件和目录,导致框架层服务中断、或文件被非法创建、访问或修改等;
- g) 文件或数据解析缺陷 AVA_VAN.FRA.7:框架层服务进程对文件或数据流解析时存在缺陷(如媒体流解析错误或配置文件字段处理错误等),利用该缺陷可触发内存操作缺陷或程序异常,导致框架层服务崩溃或框架层服务被非法控制;
- h) 密钥管理缺陷 AVA_VAN.FRA.8:框架层服务存在密钥管理缺陷(如硬编码密钥、明文保存密钥或密钥生存周期管理不足等),可利用该缺陷提取框架层服务关键密钥信息,导致敏感信息泄露、用户数据被非法访问等;
- i) 加密算法缺陷 AVA_VAN.FRA.9:框架层服务采用的加密算法存在缺陷(如弱加密算法或私有算法等),利用该缺陷可破解框架层服务的加解密过程,导致用户数据被非法访问等。

9.3.2.3.3 内核层脆弱性分析

框架层脆弱点见表 19。

表 19 内核层脆弱点

系统对应层级	脆弱点	描述
内核层	AVA_VAN.KER.1	访问控制缺陷
	AVA_VAN.KER.2	输入校验缺陷
	AVA_VAN.KER.3	内存操作缺陷
	AVA_VAN.KER.4	资源竞争缺陷
	AVA_VAN.KER.5	目录遍历缺陷
	AVA_VAN.KER.6	默认配置缺陷
	AVA_VAN.KER.7	密钥管理缺陷
	AVA_VAN.KER.8	加密算法缺陷

基于内核层脆弱点,内核层脆弱性分析如下:

- a) 访问控制缺陷 AVA_VAN.KER.1:内核访问权限控制存在缺陷(如驱动节点权限设置不当或权限管控策略不严等),利用该缺陷可获得超出其应有级别的访问权限,非法调用驱动程序接口等,导致系统拒绝服务、用户数据或系统数据被非法访问和修改等;
- b) 输入校验缺陷 AVA_VAN.KER.2:内核接口存在输入校验缺陷(如未正确判断输入参数类型、未对数组长度进行正确校验等),利用该缺陷可控制输入的参数,进行非法地址映射或传入非法数据,造成内存错误,再利用内存错误进行系统的非法提权,并进一步执行系统敏感操作(如关闭安全防护开关或打开录音功能等),非法访问用户数据或系统数据;
- c) 内存操作缺陷 AVA_VAN.KER.3:内核代码存在内存操作缺陷(如释放后重用、缓冲区溢出、读写越界或整数溢出等),利用该缺陷可对任意地址空间进行访问,导致非法访问数据或非法执行恶意代码或非法访问系统敏感功能等;
- d) 资源竞争缺陷 AVA_VAN.KER.4:在内核资源支持多进程同时访问的情况下,当两个或更多进程通过同时尝试访问和修改同一资源时,可能产生竞争条件,利用该缺陷可对数据进行非法操作(如写入文件操作的瞬间对文件进行非法数据注入),导致文件或数据被非法篡改等;
- e) 目录遍历缺陷 AVA_VAN.KER.5:当内核层对文件进行处理时(如创建文件、解压文件或删除文件等)未对文件路径进行正确校验(如未校验文件名中或文件路径中所包含的“../”字符串等),可能导致内核受到目录遍历攻击,利用该缺陷可访问系统未经授权的文件和目录,导致内核崩溃、或文件被非法创建或访问或修改等;
- f) 默认配置缺陷 AVA_VAN.KER.6:内核默认配置存在缺陷(如默认设置不安全的文件访问权限、默认未开启安全防御措施或配置不安全系统设置等),利用该缺陷可篡改网络报文、非法访问内核功能、非法访问内核文件等;
- g) 密钥管理缺陷 AVA_VAN.KER.7:内核代码存在密钥管理缺陷(如硬编码密钥、明文保存密钥或密钥生存周期管理不足等),可利用该缺陷提取内核关键密钥信息,导致敏感信息泄露、用户数据被非法访问等;
- h) 加密算法缺陷 AVA_VAN.KER.8:内核代码中采用的加密算法存在缺陷(如弱加密算法或私有算法等),利用该缺陷可破解内核中的加解密过程,导致用户数据或系统数据被非法访问。

9.3.2.3.4 可信执行环境脆弱性分析

可执行环境脆弱点见表 20。

表 20 可信执行环境脆弱点

系统对应层级	脆弱点	描述
可信执行环境	AVA_VAN.SEOS.1	内存操作缺陷
	AVA_VAN.SEOS.2	隔离机制缺陷
	AVA_VAN.SEOS.3	访问控制缺陷
	AVA_VAN.SEOS.4	可信执行程序签名绕过缺陷
	AVA_VAN.SEOS.5	程序日志泄露机密数据
	AVA_VAN.SEOS.6	鉴别与授权机制缺陷

基于可信执行环境脆弱点,可信执行环境脆弱性分析如下:

- a) 内存操作缺陷 AVA_VAN.SEOS.1:可信应用或可信执行环境中的代码存在内存操作缺陷(如释放后重用、缓冲区溢出、读写越界或整数溢出等),利用该缺陷可对任意应用地址空间进行访问,导致非法访问数据或非法控制应用或非法访问应用敏感功能等;
- b) 隔离机制缺陷 AVA_VAN.SEOS.2: REE 与可信执行环境之间的硬件隔离缺陷(如共享内存区域未适当地隔离),REE 中的恶意软件利用该缺陷可能访问或修改可信执行环境中的数据,导致数据泄露;
- c) 访问控制缺陷 AVA_VAN.SEOS.3:在可信执行环境中,可信应用软件绕过对受保护资源(如指纹采集器、安全摄像头、数据解密引擎或安全屏幕)的访问控制,可任意访问可信执行环境管理的系统资源,获得任一可信应用软件的控制权,导致敏感资源泄露;
- d) 可信执行程序(Trust Application)签名绕过缺陷 AVA_VAN.SEOS.4:可信执行环境缺乏合理的可信执行程序验证机制,或绕过签名验证机制(如在不受签名验证的情况下,向应用软件注入恶意代码),利用这个缺陷,恶意程序在系统中执行,导致数据泄露、系统功能被篡改或停止服务;
- e) 程序日志泄露机密数据 AVA_VAN.SEOS.5:由于设置配置错误或访问控制策略不足等缺陷,将密钥等机密数据输出到日志,导致敏感信息的泄露;
- f) 鉴别与授权机制缺陷 AVA_VAN.SEOS.6:可信执行环境缺乏严格的身份鉴别机制可能使敏感数据被 REE 访问,导致数据未经用户授权泄露或篡改。

9.3.2.4 硬件平台脆弱性分析

9.3.2.4.1 固件层脆弱性分析

固件层脆弱点见表 21。

表 21 固件层脆弱点

系统对应层级	脆弱点	描述
固件层	AVA_VAN.FIR.1	签名绕过缺陷
	AVA_VAN.FIR.2	密钥管理缺陷
	AVA_VAN.FIR.3	内存操作缺陷

基于固件层脆弱点,固件层脆弱性分析如下:

- a) 签名绕过缺陷 AVA_VAN.FIR.1:固件更新和加载机制存在缺陷,使恶意软件通过伪造的更新进入设备,攻击者可能利用未经验证的更新包,篡改设备的功能或植入后门程序,导致系统崩溃、系统被非法控制等;
- b) 密钥管理缺陷 AVA_VAN.FIR.2:固件存在密钥管理缺陷(如硬编码密钥、明文保存密钥或密钥生存周期管理不足等),可利用该缺陷提取关键密钥信息,导致敏感信息泄露或用户数据被非法访问等;
- c) 内存操作缺陷 AVA_VAN.FIR.3:软件中存在内存操作缺陷(如释放后重用、缓冲区溢出、读写越界或整数溢出等),利用该缺陷可对任意应用地址空间进行访问,导致非法访问数据或非法控制应用或非法访问应用敏感功能等。

9.3.2.4.2 硬件层脆弱性分析

硬件层脆弱点见表 22。

表 22 硬件层脆弱点

系统对应层级	脆弱点	描述
硬件层	AVA_VAN.HAR.1	侧信道分析缺陷
	AVA_VAN.HAR.2	物理注入缺陷
	AVA_VAN.HAR.3	内存硬件缺陷
	AVA_VAN.HAR.4	硬件调试接口暴露缺陷

基于硬件层脆弱点,硬件层脆弱性分析如下:

- a) 侧信道分析缺陷 AVA_VAN.HAR.1:侧信道分析是通过分析密码系统的物理实现(如电磁波、功耗或时间延迟等)来获取敏感信息,利用该缺陷可推测出密钥或密码等机密数据,导致密钥或用户敏感数据泄露;
- b) 物理注入缺陷 AVA_VAN.HAR.2:当硬件器件未做好充分的保护(如关键器件未进行封装防护或关键信号存在表层走线等)时,存在物理注入缺陷(如可接收光信号注入或可接收超声波注入等),利用该缺陷可对物理器件进行信号注入,导致在用户无感知的情况向设备发送非法指令;
- c) 内存硬件缺陷 AVA_VAN.HAR.3:当内存硬件器件未进行有针对性的防护时,利用该缺陷(如内存相邻行数据可被翻转等)可修改内存数据,导致敏感数据被篡改或泄露等;
- d) 硬件调试接口暴露缺陷 AVA_VAN.HAR.4:当设备的调试接口(如 JTAG 接口或 UART 接口等)未能进行充分保护而暴露时,可利用该缺陷非法访问硬件调试接口,下发配置,导致可绕过安全启动并修改底层软件(包括修改操作系统和固件,导致系统功能被破坏或植入恶意代码)或访问内存和寄存器等敏感数据。

9.3.3 穿透性测试方法

9.3.3.1 操作系统穿透性测试方法

9.3.3.1.1 应用层穿透性测试方法

应用层穿透性测试方法如下。

- a) 访问控制缺陷 AVA_VAN.APP.1:

- 1) AVA_ATT.APP.1:通过脚本查看所有应用文件(含配置文件、日志文件或其他敏感数据文件)的访问权限,如果应用文件的权限设置不当,尝试对应用文件进行读取或修改操作,验证未经授权用户是否能访问用户数据或修改应用配置等;
- 2) AVA_ATT.APP.2:通过脚本查看应用软件开发接口的权限访问控制,如果应用软件开发接口的权限访问控制不足,尝试通过接口对应用资源进行访问(如访问敏感功能、访问用户数据等)。
- b) 端口或服务暴露缺陷 AVA_VAN.APP.2:
AVA_ATT.APP.3:通过扫描工具[如网络安全扫描工具(Nmap)或漏洞扫描工具(Nessus)]等方式查看应用软件开放的所有端口和服务,如果存在暴露的应用端口或服务,则尝试通过暴露的端口或服务来访问应用的敏感功能或用户数据。
- c) 敏感数据暴露缺陷 AVA_VAN.APP.3:
AVA_ATT.APP.4:通过脚本分析应用软件的代码或配置,查看涉及的敏感数据(如密钥、用户数据或配置文件等)的存储位置,包括数据库、文件系统或内存中,如果敏感数据未加密保存或未进行访问控制保护,则尝试访问应用的敏感数据。
- d) 内存操作缺陷 AVA_VAN.APP.4:
AVA_ATT.APP.5:检查应用软件代码存在的内存操作缺陷(如释放后重用、缓冲区溢出、读写越界或整数溢出等),尝试构造非法内容,触发内存操作缺陷。如果可成功触发内存操作缺陷(如产生系统崩溃、读写越界或修改内存等),进一步尝试修改内存空间以控制代码执行流程,从而在应用中执行任意代码,并获得用户数据或提升系统权限。
- e) 资源竞争缺陷 AVA_VAN.APP.5:
AVA_ATT.APP.6:检查应用软件文件更新过程中,“检查文件签名”和“加载文件”之间的时间间隔时长。如果存在的时间间隔的时长可允许完成文件替换,则尝试在检查文件签名后的瞬间将更新文件进行替换(需尝试不少于10次),以绕过校验机制,加载恶意更新文件。
- f) 签名绕过缺陷 AVA_VAN.APP.6:
AVA_ATT.APP.7:检查应用软件文件更新(含插件更新)过程中签名校验实现方式,如果使用无效的签名校验或只对部分更新文件进行签名校验,则尝试替换更新文件,以绕过签名校验机制,加载恶意更新文件。
- g) 功能校验绕过缺陷 AVA_VAN.APP.7:
AVA_ATT.APP.8:检查应用软件在功能校验过程中(如屏幕锁)的防暴力破解方案的实现过程,如果未采用有效的防暴力破解机制,则尝试不同的输入组合绕过应用软件功能校验,获得未经授权的应用功能访问权限。
- h) 输入校验缺陷 AVA_VAN.APP.8:
AVA_ATT.APP.9:通过脚本查看开放的应用软件中所有的开发接口。如果应用软件存在开放的接口,尝试通过这些接口触发内存操作缺陷或命令注入,以获得对内存空间的修改权限并控制代码执行流程,或植入恶意命令,导致访问未经授权访问用户数据或调用应用的敏感功能。
- i) 目录遍历缺陷 AVA_VAN.APP.9:
AVA_ATT.APP.10:如果应用软件未正确校验文件、目录的路径,尝试触发目录遍历缺陷(如控制路径中增加“../”字段或通过编码方式隐藏“../”字段、修改软连接路径等)绕过访问控制,导致可访问或修改应用软件中的敏感文件。
- j) 文件或数据解析缺陷 AVA_VAN.APP.10:
1) AVA_ATT.APP.11:如果应用软件在解析文件或数据流时没有正确处理边界条件或输

入条件,尝试构造非预期的数据类型、超过预期长度的数据或包含非法字符或编码的数据,触发应用软件崩溃;

- 2) AVA_ATT.APP.12:如果应用软件在解析输入数据并直接或间接将这些数据用于系统命令执行时,没有适当的清理或转义,尝试修改内存空间控制代码执行的流程,或植入恶意命令,导致访问未经授权访问用户数据或调用应用的敏感功能。

k) 默认配置缺陷 AVA_VAN.APP.11:

AVA_ATT.APP.13:通过脚本检测应用使用的传输协议类型。如果发现应用默认使用不安全的传输协议,或尽管使用了安全的传输协议但在传输过程中未进行合理的证书校验,尝试在传输协议通道中截获数据包,窃取或篡改其中的内容,并进一步尝试还原用户数据或改变应用软件的处理逻辑。

l) 密钥管理缺陷 AVA_VAN.APP.12:

AVA_ATT.APP.14:如果应用软件存在密钥管理缺陷(如代码硬编码密码或文件明文保存密钥等),尝试利用密码还原加密前的应用数据或用户文件等。

m) 加密算法缺陷 AVA_VAN.APP.13:

AVA_ATT.APP.15:检查应用软件采用的加密算法,如果使用弱加密算法或私有算法等,尝试利用算法的已知弱点,还原加密内容,从而获取应用数据或用户数据等。

9.3.3.1.2 框架层穿透性测试方法

框架层穿透性测试方法如下。

a) 访问控制缺陷 AVA_VAN.FRA.1:

AVA_ATT.FRA.1:通过自动化脚本检测框架层服务和接口的访问权限,如果发现接口访问控制存在缺陷,尝试访问框架服务的敏感功能和用户数据等。

b) 端口或服务暴露 AVA_VAN.FRA.2:

AVA_ATT.FRA.2:使用扫描工具(如 Nmap、Nessus)等方式查看框架层开放的端口和服务,尝试通过暴露的端口或服务,访问未经授权的敏感功能或用户数据等。

c) 运行时代码缺少签名校验 AVA_VAN.FRA.3:

AVA_ATT.FRA.3:检查框架层是否对应用软件运行时代码进行签名校验(如采用逆向工具分析应用软件代码),尝试修改或替换运行时代码,并通过替换的恶意代码获取用户数据或调用应用敏感功能等。

d) 输入校验缺陷 AVA_VAN.FRA.4:

AVA_ATT.FRA.4:如果框架层服务接口可接收外部参数(如支持其他程序或用户传入数据),尝试向接口传入非法内容,使框架服务崩溃或产生其他未预期的行为等。

e) 资源竞争缺陷 AVA_VAN.FRA.5:

AVA_ATT.FRA.5:如果框架层服务接口可接收外部参数(如支持其他程序或用户传入数据),尝试通过多线程或异步任务同时触发相同的接口调用,触发异常行为(如服务崩溃或数据不一致等);如果成功触发异常行为,再尝试构造攻击代码,利用条件竞争漏洞执行系统级操作,获取更高权限,访问和提取用户数据或系统数据。

f) 目录遍历缺陷 AVA_VAN.FRA.6:

AVA_ATT.FRA.6:如果框架层服务与文件/目录操作相关的代码中对文件的操作和使用过程中未检查路径,尝试触发目录遍历缺陷(如在路径中增加“../”字段或修改软连接路径等),并进一步尝试读写框架层高权限等级的文件。

g) 文件或数据解析缺陷 AVA_VAN.FRA.7:

AVA_ATT.FRA.7:如果框架层服务中与文件或数据解析的代码存在缺陷,尝试触发文件或数据流的解析错误,向服务发送特质的文件或数据流,导致框架层服务崩溃;如果成功则尝试控制代码执行流程或执行命令注入植入恶意命令,进一步访问用户数据或调用框架层服务的敏感功能。

h) 密钥管理缺陷 AVA_VAN.FRA.8:

AVA_ATT.FRA.8:如果框架层服务存在密钥管理缺陷(如代码硬编码密码或文件明文保存密钥等),尝试利用密码缺陷还原加密前的数据或文件,从而获取服务数据或用户数据等。

i) 加密算法缺陷 AVA_VAN.FRA.9:

AVA_ATT.FRA.9:查看框架层服务采用的加密算法,如果使用弱加密算法或私有算法等,尝试利用破解弱加密算法和私有算法加密过程,并还原被加密的内容,从而获取服务数据或用户数据等。

9.3.3.1.3 内核层穿透性测试方法

内核层穿透性测试方法如下。

a) 访问控制缺陷 AVA_VAN.KER.1:

- 1) AVA_ATT.KER.1:通过脚本查看所有系统文件的访问权限,如果文件的访问控制存在缺陷,尝试对文件进行读取或修改,获取用户数据和修改系统配置等;
- 2) AVA_ATT.KER.2:通过脚本查看系统驱动程序接口的访问权限,尝试利用访问控制缺陷对驱动程序接口进行访问(如调用系统命令等),进一步尝试利用驱动程序接口执行系统高权限操作、访问系统文件等。

b) 输入校验缺陷 AVA_VAN.KER.2:

AVA_ATT.KER.3:如果驱动程序接口可接收外部参数(例如支持其他程序传入数据),尝试向接口传入非法内容,使系统内核产生崩溃等。

c) 内存操作缺陷 AVA_VAN.KER.3:

AVA_ATT.KER.4:检查内核代码存在的内存操作缺陷(如缓冲区溢出或读写越界等),尝试构造非法内容,触发内核操作缺陷。如果可成功触发内存操作缺陷(如产生系统崩溃或读写越界、修改内存等),进一步尝试修改内存空间以控制代码执行流程,从而在内核中执行任意代码,窃取用户数据或提升系统权限。

d) 资源竞争缺陷 AVA_VAN.KER.4:

AVA_ATT.KER.5:如果驱动程序接口可接收外部参数(如支持其他程序传入数据),尝试通过多线程或异步任务同时触发接口调用,触发异常行为(如系统崩溃、数据不一致等)。如果成功触发异常行为,进一步构造攻击代码,并在内核中执行,观察是否能成功利用条件竞争漏洞执行系统级操作,获取更高权限。如果获得了更高权限,尝试访问和提取用户数据或系统数据。

e) 目录遍历缺陷 AVA_VAN.KER.5:

AVA_ATT.KER.6:如果内核中与文件/目录操作相关的代码中对文件的操作和使用过程中未检查路径,尝试触发目录遍历缺陷(如控制路径中增加“../”字段、修改软连接路径等),并进一步尝试读写系统高权限等级的文件。

f) 默认配置缺陷 AVA_VAN.KER.6:

AVA_ATT.KER.7:通过脚本查看内核安全保护机制开启情况,如果系统未开启内核安全保护机制,尝试结合内存操作缺陷(AVA_VAN.KER.3)进行攻击测试(如尝试构造非法输入等)。如果可成功触发内存操作缺陷(如产生系统崩溃、读写越界或修改内存等),则可尝试修

改内存空间以控制代码执行流程,从而在内核中执行任意代码,并进一步尝试通过以上措施窃取用户数据或提升系统权限。

g) 密钥管理缺陷 AVA_VAN.KER.7:

AVA_ATT.KER.8:如果内核实现中存在密钥管理缺陷(如代码硬编码密码或文件明文保存密钥等),尝试利用密码还原加密前的数据或文件,从而获取系统数据或用户数据等。

h) 加密算法缺陷 AVA_VAN.KER.8:

AVA_ATT.KER.9:如果内核中使用的加密算法是弱加密算法或私有算法等,尝试利用算法弱点破解加密过程,还原被加密的内容,从而获取系统数据或用户数据等。

9.3.3.1.4 可信执行环境穿透性测试方法

可信执行环境穿透性测试方法如下。

a) 内存操作缺陷 AVA_VAN.SEOS.1:

- 1) AVA_ATT.SEOS.1 尝试向安全操作系统暴露的接口传入人工构造的异常数据,并观察系统状态和日志记录,以确认是否存在数据验证不足的情况;
- 2) AVA_ATT.SEOS.2 生成大量随机输入数据,尝试对可能的输入接口进行压力测试,监控系统内存使用情况,观察是否出现崩溃、内存泄露的持续增加,并记录测试中的所有异常结果,检查是否存在缓冲区溢出等漏洞可攻击可信执行环境获取可信执行环境控制权。

b) 隔离机制缺陷 AVA_VAN.SEOS.2:

AVA_ATT.SEOS.3 在访问可信执行环境的过程中,尝试修改 REE 可访问的物理内存,并观察可信执行环境的行为是否出现异常,该异常可用于获取可信执行环境的控制权,并从 REE 可访问的物理内存中提取残留在内存中的密钥。

c) 访问控制缺陷 AVA_VAN.SEOS.3:

- 1) AVA_ATT.SEOS.4 使用某一个安全应用的凭证尝试访问其他安全应用的数据,验证安全应用是否无法访问其他安全应用持久化的数据;
- 2) AVA_ATT.SEOS.5 通过非特权安全应用的凭证,尝试访问可信执行环境的高权限接口,验证授权管理机制的有效性。

d) 可信执行程序加载验证过程缺陷 AVA_VAN.SEOS.4:

- 1) AVA_ATT.SEOS.6 寻找存在已知漏洞的旧版本可信执行程序,尝试将这一存在漏洞的旧版本可信应用软件加载至系统中,重新利用旧版本的漏洞攻击可信执行环境;
- 2) AVA_ATT.SEOS.7 分析可信执行程序的加载和验证路径,尝试绕过合法性验证机制的潜在漏洞,绕过系统应用校验机制,在可信执行环境中植入后门。

e) 程序日志泄露机密数据 AVA_VAN.SOS.5:

AVA_ATT.SEOS.8 触发可信执行环境的不同事件和行为,监控并检查安全系统日志配置。寻找存在敏感数据(如密钥或私钥)被泄露的情况,尝试触发可信执行环境的不同事件和行为,监控并检查安全系统日志配置,在日志文件中寻找敏感数据(如密钥、私钥或用户凭证等)是否被泄露,并检查应用软件的配置设置,确认日志文件的权限设置是否适当,以防止未授权用户访问。如果发现日志文件中包含敏感信息,尝试利用这些信息进一步穿透系统,例如通过获取数据库连接字符串来访问数据库,或利用暴露的凭证来提升权限。

f) 鉴别与授权机制缺陷 AVA_VAN.SEOS.6:

AVA_ATT.SEOS.9 验证身份鉴别机制是否存在,尝试在无鉴别凭据的情况下,添加账号,修改用户生物凭据,发起支付,检查是否存在可不出示凭据即实现高安全等级需求的操作。

9.3.3.2 硬件平台穿透性测试方法

9.3.3.2.1 测试对象范围

该方法仅对 CPU、存储器的固件层和硬件层进行穿透性测试。

9.3.3.2.2 固件层穿透性测试方法

固件层穿透性测试方法如下。

- a) 签名绕过缺陷 AVA_VAN.FIR.1:
 - 1) AVA_ATT.FIR.1 分析启动过程处理器固件的格式,判断加载固件是否有签名保护,尝试修改固件内容,注入后门后再加载固件,在加载固件后触发后门,以获取处理器控制权;
 - 2) AVA_ATT.FIR.2 分析处理器固件的加载过程和签名验证过程,寻找导致签名绕过的验证不完备缺陷,尝试修改固件内容,注入后门后再加载固件,在加载固件后触发后门,以获取处理器控制权。
- b) 密钥管理缺陷 AVA_VAN.FIR.2:

AVA_ATT.FIR.3 扫描固件二进制文件,分析处理器固件中是否存在明文密钥或私钥,尝试提取出这些密钥。
- c) 内存操作缺陷 AVA_VAN.FIR.3:
 - 1) AVA_ATT.FIR.4 识别处理器固件对外暴露的接口,分析接口参数的格式和边界条件,尝试向固件传入人工构造的异常数据,以确认是否存在输入数据验证不足的问题,导致处理器故障不可用;
 - 2) AVA_ATT.FIR.5 使用模糊测试工具自动化构造数据,对处理器固件进行模糊测试,观察系统状态和日志记录,以确认是否存在输入数据验证不足;并进一步构造数据尝试攻击处理器固件,以获取处理器控制权。

9.3.3.2.3 硬件层穿透性测试方法

硬件层穿透性测试方法如下。

- a) 侧信道分析缺陷 AVA_VAN.HAR.1:

AVA_ATT.HAR.1:通过分析密码算法的电磁波和功耗等信息,尝试获取算法运行的密钥。
- b) 物理注入缺陷 AVA_VAN.HAR.2:

AVA_ATT.HAR.2:通过物理手段注入电磁/电压毛刺,对密码算法的运行进行故障干扰,使密码运算过程中产生错误,然后对电磁/电压干扰产生的错误密文信息进行分析,尝试获取算法运行的密钥。
- c) 内存硬件缺陷 AVA_VAN.HAR.3:

AVA_ATT.HAR.3:对动态随机存取内存(DRAM)进行频繁访问,重复不断地对特定内存行写入 0-1-0-1,如果相邻内存行存在位翻转,则说明受到内存硬件缺陷(如利用行锤攻击执行的缺陷)影响,尝试对关键字段(如密钥)进行修改。
- d) 硬件调试接口暴露缺陷 AVA_VAN.HAR.3:

AVA_ATT.HAR.4:观察系统硬件调试接口(如 JTAG 接口或 UART 接口等),尝试对系统硬件调试接口进行访问,突破对硬件调试接口的鉴别功能,如果可成功访问硬件调试接口,进一步尝试通过调试模式指令关闭安全启动,如通过调试模式指令刷入关闭安全启动的非法固件包并关闭安全启动,通过调试模式访问内存和寄存器等敏感数据。

9.3.4 脆弱性评估分级要求

脆弱性评估分级要求见表 23。

表 23 脆弱性评估分级要求

类别	脆弱点	穿透性测试方法	EAL2+ /EAL3+ (AVA_VAN.2)	EAL4+ (AVA_VAN.3)	EAL5+ (AVA_VAN.4)
应用层	访问控制缺陷 AVA_VAN.APP.1	AVA_ATT.APP.1	✓	✓	✓
		AVA_ATT.APP.2	✓	✓	✓
	端口或服务暴露缺陷 AVA_VAN.APP.2	AVA_ATT.APP.3	✓	✓	✓
	敏感数据暴露缺陷 AVA_VAN.APP.3	AVA_ATT.APP.4	✓	✓	✓
	内存操作缺陷 AVA_VAN.APP.4	AVA_ATT.APP.5	✓	✓	✓
	资源竞争缺陷 AVA_VAN.APP.5	AVA_ATT.APP.6			✓
	签名绕过缺陷 AVA_VAN.APP.6	AVA_ATT.APP.7		✓	✓
	功能校验绕过缺陷 AVA_VAN.APP.7	AVA_ATT.APP.8	✓	✓	✓
	输入校验缺陷 AVA_VAN.APP.8	AVA_ATT.APP.9		✓	✓
	目录遍历缺陷 AVA_VAN.APP.9	AVA_ATT.APP.10		✓	✓
	文件或数据解析缺陷 AVA_VAN.APP.10	AVA_ATT.APP.11		✓	✓
		AVA_ATT.APP.12		✓	✓
	默认配置缺陷 AVA_VAN.APP.11	AVA_ATT.APP.13	✓	✓	✓
	密钥管理缺陷 AVA_VAN.APP.12	AVA_ATT.APP.14	✓	✓	✓
	加密算法缺陷 AVA_VAN.APP.13	AVA_ATT.APP.15	✓	✓	✓
框架层	访问控制缺陷 AVA_VAN.FRA.1	AVA_ATT.FRA.1	✓	✓	✓
	端口或服务暴露 AVA_VAN.FRA.2	AVA_ATT.FRA.2	✓	✓	✓
	运行时代码缺少完整性校验 AVA_VAN.FRA.3	AVA_ATT.FRA.3			✓
	输入校验缺陷 AVA_VAN.FRA.4	AVA_ATT.FRA.4		✓	✓

表 23 脆弱性评估分级要求（续）

类别	脆弱点	穿透性测试方法	EAL2+ /EAL3+ (AVA_VAN.2)	EAL4+ (AVA_VAN.3)	EAL5+ (AVA_VAN.4)
框架层	资源竞争缺陷 AVA_VAN.FRA.5	AVA_ATT.FRA.5		✓	✓
	目录遍历缺陷 AVA_VAN.FRA.6	AVA_ATT.FRA.6		✓	✓
	文件或数据解析缺陷 AVA_VAN.FRA.7	AVA_ATT.FRA.7		✓	✓
	密钥管理缺陷 AVA_VAN.FRA.8	AVA_ATT.FRA.8	✓	✓	✓
	加密算法缺陷 AVA_VAN.FRA.9	AVA_ATT.FRA.9	✓	✓	✓
内核层	访问控制缺陷 AVA_VAN.KER.1	AVA_ATT.KER.1	✓	✓	✓
		AVA_ATT.KER.2		✓	✓
	输入校验缺陷 AVA_VAN.KER.2	AVA_ATT.KER.3		✓	✓
	内存操作缺陷 AVA_VAN.KER.3	AVA_ATT.KER.4		✓	✓
	资源竞争缺陷 AVA_VAN.KER.4	AVA_ATT.KER.5		✓	✓
	目录遍历缺陷 AVA_VAN.KER.5	AVA_ATT.KER.6		✓	✓
	默认配置缺陷 AVA_VAN.KER.6	AVA_ATT.KER.7		✓	✓
	密钥管理缺陷 AVA_VAN.KER.7	AVA_ATT.KER.8	✓	✓	✓
	加密算法缺陷 AVA_VAN.KER.8	AVA_ATT.KER.9	✓	✓	✓
可信执行环境	内存操作缺陷 AVA_VAN.SEOS.1	AVA_ATT.SEOS.1		✓	✓
		AVA_ATT.SEOS.2		✓	✓
	隔离机制缺陷 AVA_VAN.SEOS.2	AVA_ATT.SEOS.3		✓	✓
	访问控制缺陷 AVA_VAN.SEOS.3	AVA_ATT.SEOS.4	✓	✓	✓
		AVA_ATT.SEOS.5	✓	✓	✓
	可信执行程序加载验证过程 缺陷AVA_VAN.SEOS.4	AVA_ATT.SEOS.6		✓	✓
		AVA_ATT.SEOS.7			✓
	程序日志泄露机密数据 AVA_VAN.SEOS.5	AVA_ATT.SEOS.8	✓	✓	✓

表 23 脆弱性评估分级要求（续）

类别	脆弱点	穿透性测试方法	EAL2+ /EAL3+ (AVA_VAN.2)	EAL4+ (AVA_VAN.3)	EAL5+ (AVA_VAN.4)
可信执行环境	鉴别与授权机制缺陷 AVA_VAN.SEOS.6	AVA_ATT.SEOS.9	✓	✓	✓
固件层	签名绕过缺陷 AVA_VAN.FIR.1	AVA_ATT.FIR.1			✓
		AVA_ATT.FIR.2			✓
	密钥管理缺陷 AVA_VAN.FIR.2	AVA_ATT.FIR.3	✓	✓	✓
	内存操作缺陷 AVA_VAN.FIR.3	AVA_ATT.FIR.4		✓	✓
		AVA_ATT.FIR.5		✓	✓
硬件层	侧信道分析缺陷 AVA_VAN.HAR.1	AVA_ATT.HAR.1		✓	✓
	物理注入缺陷 AVA_VAN.HAR.2	AVA_ATT.HAR.2			✓
	内存硬件缺陷 AVA_VAN.HAR.3	AVA_ATT.HAR.3			✓
	硬件调试接口暴露缺陷 AVA_VAN.HAR.4	AVA_ATT.HAR.4	✓	✓	✓
注：“✓”表示要求。“空白”表示不要求。					

10 基本原理

10.1 安全目的基本原理

移动终端安全目的能应对所有可能的威胁、假设和组织安全策略,即每一种威胁、假设和组织安全策略都至少有一个安全目的与其对应,因此是完备的。每一个安全目的都有相应的威胁、假设和组织安全策略与之对应,这证明每个安全目的都是必要的;每一个威胁、假设和组织安全策略都有相应的一个或多个安全目的与之对应,因此说明了安全目的是充分的。

移动终端的安全目的能应对所有可能的安全威胁、假设和组织安全策略,其对应关系见表 24。

表 24 安全目的与安全威胁、假设和组织安全策略的对应关系

安全目的	安全威胁、假设和组织安全策略												
	T.UNAUTHACCESS	T.ACCESSMALICIOUS	T.EAVESDROP	T.PHYSICAL	T.RESIDUALDATA	T.INTDESTROY	T.MALICIOUSAPP	T.DEVSPPOOF	T.SSIONSPPOOF	P.CRYPTOMANAG	A.PHYSICAL	A.PERSONNEL	A.REMOTE
O.AUDIT		✓											
O.AUTH	✓			✓					✓				
O.ACTROL	✓			✓		✓	✓						
O.ENCRYPT	✓		✓	✓		✓			✓	✓			
O.INFOERASE					✓					✓			
O.SECCOM			✓						✓	✓			
O.SESSIONMANAG									✓				
O.INTEGRITY				✓		✓							
O.DEVAUTH								✓					
O.PRIVACY							✓						
OE.PHYSICAL											✓		
OE.PERSONNEL												✓	
OE.REMOTE													✓
注：“✓”表示要求。“空白”表示不要求。													

下面的 a)~m)给出了安全目的与安全威胁、假设和组织安全策略的对应关系说明。

- a) T.UNAUTHACCESS:非授权用户或进程访问移动终端的安全功能数据和用户数据,并对安全功能数据和用户数据进行恶意操作。O.AUTH 能保障未授权用户在访问移动终端时需经过用户身份鉴别,未通过鉴别的用户无法访问安全功能和数据,并保障移动终端在鉴别失败达到一定次数时限制用户的鉴别行为,限制攻击者反复猜测鉴别数据。O.ENCTYPT 保障对重要数据进行加密,防止未授权用户的访问,O.ACTROL 保障移动终端具备访问控制措施,用户对数据和资源的访问需严格依照访问控制策略。
- b) T.ACCESSMALICIOUS:授权用户因安全意识薄弱或误操作,对移动终端进行不正确地配置,或授权用户恶意利用权限进行非法操作,使移动终端安全受到威胁。O.AUDIT 能保证对用户操作行为的审计,可用于误操作或非法操作行为的追溯,并对审计数据进行保护并只限授权用户查看,同时保证审计迹已满的情况下,不影响审计功能和其他安全功能的执行。
- c) T.EAVESDROP:恶意用户或进程可能监听或修改移动终端与其他设备之间或移动终端与远程可信 IT 产品间传递的用户数据或 TSF 数据。O.SECCOM 能保证为移动终端与其他设备之间以及移动终端与外部可信 IT 实体间的通信提供可信通道,防止数据被监听和修改,同时 O.ENCTYPT 保证传输数据采用加密方式,防止被窃取。

- d) T.PHYSICAL:恶意用户通过访问 TOE 的物理接口来访问资产,或尝试通过猜测口令和/或仿冒生物信息技术,从而获得对用户数据资产的访问权限。O.AUTH 能保障未授权用户在访问移动终端时需经过用户身份鉴别;O.ACTROL 防止移动终端重要数据、进程及资源等在未授权情况下被访问、修改或删除;O.ENCTYPT 和 O.INTEGRITY 保护移动终端的机密性和完整性,防止攻击者通过物理方式破解移动终端。
- e) T.RESIDUALDATA:恶意用户或进程可能利用移动终端残留信息的处理缺陷,在执行过程中对未删除的残留信息进行利用,以获取敏感信息或滥用 TOE 的安全功能。O.INFOERASE 能保证重要的数据在使用完成后会被删除或被安全处理,不会留下可被攻击者利用的残留数据信息。
- f) T.INTDESTROY:恶意用户或进程通过安全攻击非法地浏览、修改或删除 TSF 数据或可执行代码,破坏移动终端的完整性。O.ACTROL 防止移动终端重要数据、进程及资源等在未授权情况下被访问、修改或删除。O.ENCTYPT 和 O.INTEGRITY 保证移动终端在启动、更新和运行过程中完整性,防止攻击者破解移动终端,非法地查看、修改或删除 TSF 数据或可执行代码。
- g) T.MALICIOUSAPP:恶意软件可能通过伪装成授权应用或进程访问用户数据和系统敏感资源。O.ACTROL 保障移动终端具备访问控制措施,用户对数据和资源的访问需严格依照访问控制策略;O.PRIVACY 提供身份脱敏功能,通过身份脱敏实现应用收集的用户数据不能与用户的真实身份绑定起来,保护用户隐私。
- h) T.DEVSPOOF:恶意设备欺骗 TOE 连接到该设备,使用伪装成受信任的对端设备访问用户数据,造成 TOE 功能被滥用或用户数据被泄露。O.DEVAUTH 实现鉴别尝试与 TOE 建立连接的设备,通过鉴别的设备才能建立连接。
- i) T.SSIONSPOOF:恶意用户伪装成可信赖的实体与 TOE 建立会话,获取 TOE 敏感或保密信息,或滥用 TOE 的安全功能。O.AUTH 能保障未授权用户在访问 TOE 时需经过用户身份鉴别,未通过鉴别的用户无法访问 TSF 数据和用户数据。O.COMMS 和 O.SESSIONMANAG 能对与 TOE 通信的其他 IT 实体的身份进行鉴别,并为 TOE 与其他可信 IT 实体间的通信提供可信通道,防止数据被窃取或功能被滥用,同时 O.ENCRYPT 保证传输数据采用加密方式,防止被窃取。
- j) P.CRYPTOMANAG:O.ENCRYPT 保证移动终端使用的密码算法应符合国家、行业或组织要求的密码管理相关标准,并移动终端应提供密码功能以维护移动智能操作系统的保密性和完整性;O.INFOERASE 通过保证移动终端资源被用户或进程释放后并配置给其他用户或进程时,TSF 数据和用户相关密钥数据不再持久存在。O.SECCOM 通过可信信道实现通信数据的保密性保护。
- k) A.PHYSICAL:假设移动终端运行所依赖的运行环境能符合移动终端安全运行的所需的物理保护。OE.PHYSICAL 保证移动终端运行所依赖的运行环境能符合移动终端安全运行的所需的物理保护。
- l) A.PERSONNEL:假设移动终端的合法用户能按管理员指南来管理移动终端的安全功能,对移动终端不存在恶意的破坏企图。OE.PERSONNEL 移动终端的合法用户能按操作指南来管理移动终端的安全功能,对移动终端不存在恶意的破坏企图。
- m) A.REMOTE:假设用于管理移动终端的远程 IT 设备、应用设备是安全的。OE.REMOTE 保证了移动终端的远程管理设备、应用商店等远程 IT 实体是安全的且其数据和用户信息是被保护的。

10.2 安全要求的基本原理

安全要求包括安全功能要求和安全保障要求,安全功能要求实现 TOE 的安全目的,安全要求基本原理表明如果实现了所有安全功能要求,则实现了 TOE 的所有安全目的,因此安全功能要求与安全目的的对应关系即安全要求与安全目的的对应关系。

安全功能要求与安全目的的对应关系见表 25。

表 25 安全功能要求与安全目的的对应关系

安全功能要求	安全目的									
	O.AUDIT	O.AUTH	O.ACTROL	O.ENCRYPT	O.INFOERASE	O.SECCOM	O.SESSIOMMANAG	O.INTEGRITY	O.DEVAUTH	O.PRIVACY
FAU_GEN.1	√									
FAU_STG.1	√									
FAU_STG.4	√									
FCS_CKH_EXT.1/Low				√						
FCS_CKH_EXT.1/MediumHigh				√						
FCS_CKM.1/Symmetric				√						
FCS_CKM.1/Asymmetric				√						
FCS_CKM.2				√						
FCS_CKM.3				√						
FCS_CKM.5				√						
FCS_CKM.6				√						
FCS_CKM_EXT.1				√						
FCS_COP.1/SIGN				√						
FCS_COP.1/ENCRYPT				√						
FCS_COP.1/HASH				√						
FCS_COP.1/KEYHMAC				√						
FCS_RNG.1				√						
FDP_ACC.1/MAC			√							
FDP_ACC.1/DAC			√							
FDP_ACC.1/SYSCALL			√							
FDP_ACC.1/Permission			√							
FDP_ACC.1/UserData			√							
FDP_ACC.1/SEE			√							
FDP_ACC.1/DTC			√							

表 25 安全功能要求与安全目的的对应关系（续）

安全功能要求	安全目的									
	O.AUDIT	O.AUTH	O.ACTROL	O.ENCRYPT	O.INFOERASE	O.SECCOM	O.SESSIOMANAG	O.INTEGRITY	O.DEVAUTH	O.PRIVACY
FDP_ACF.1/MAC			✓							
FDP_ACF.1/DAC			✓							
FDP_ACF.1/SYSCALL			✓							
FDP_ACF.1/Permission			✓							
FDP_ACF.1/UserData			✓							
FDP_ACF.1/SEE			✓							
FDP_ACF.1/DTC			✓							
FDP_RIP.2					✓					
FDP_SDC.1				✓						
FIA_AFL.1		✓								
FIA_SOS.1		✓								
FIA_SOS.2		✓								
FIA_UAU.1		✓								
FIA_UAU.5/USER		✓								
FIA_UAU.5/DEVICE		✓							✓	
FIA_UAU.5/APP		✓								
FIA_UAU.6		✓					✓			
FIA_UAU.7		✓								
FIA_UID.1		✓								
FIA_API.1		✓								
FMT_MSA.1/Permission			✓							
FMT_MSA.3/Permission			✓							
FMT_SMF.1		✓					✓	✓		
FPR_PSE.1/APPDEV										✓
FPR_PSE.1/AD										✓
FPT_AEX_EXT.1								✓		
FPT_AEX_EXT.2								✓		
FPT_AEX_EXT.3								✓		
FPT_AEX_EXT.4								✓		

表 25 安全功能要求与安全目的的对应关系（续）

安全功能要求	安全目的									
	O.AUDIT	O.AUTH	O.ACTROL	O.ENCRYPT	O.INFOERASE	O.SECCOM	O.SESSEIONMANAG	O.INTEGRITY	O.DEVAUTH	O.PRIVACY
FPT_AEX_EXT.5								✓		
FPT_FLS.1								✓		
FPT_JTA_EXT.1								✓		
FPT_PHP.3								✓		
FPT_RCV.2								✓		
FPT_SEE_EXT.1								✓		
FPT_STG_EXT.1								✓		
FPT_STM.1	✓									
FPT_TST_EXT.1								✓		
FPT_TST_EXT.2								✓		
FPT_TUD_EXT.1/OS								✓		
FPT_TUD_EXT.1/APP								✓		
FTA_SSL.1							✓			
FTA_SSL.2							✓			
FTP_ITC.1/TLS						✓				
FTP_ITC.1/DEVICE						✓			✓	
注：“✓”表示要求。“空白”表示不要求。										

- 以下 a)~j)给出了安全功能要求与安全目的之间的对应关系说明。
- a) O.AUDIT:该目的可通过安全功能要求 FAU_GEN.1 来实现审计日志生成以及身份关联的目的,FAU_STG.1、FAU_STG.4 可保障审计的存储安全,通过安全功能要求 FPT_STM.1 为审计提供可靠时间戳。
 - b) O.AUTH:该目的可通过安全功能要求 FIA_UAU.1 对访问用户进行鉴别处理,以区分授权用户和非授权用户,FIA_AFL.1 提供了鉴别失败的锁定机制,FIA_SOS.1 规定了用户鉴别数据(如:口令)的强度要求,通过安全功能要求 FIA_UAU.5、FIA_UAU.6 和 FIA_UAU.7 来实现用户鉴别的时机、用户多重鉴别方式,密码输入的显示以及会话恢复时的重鉴别。通过安全功能要求 FIA_API.1 实现向外部实体证明设备身份的机制。通过安全功能要求 FMT_SMF.1 实现对锁屏时间和鉴别数据的管理。
 - c) O.ACTROL:该目的可通过安全功能要求 FDP_ACC.1 和 FDP_ACF.1 来实现基于安全属性进行访问控制,防止非授权用户的恶意访问。通过安全功能要求 FMT_MSA.1 和 FMT_MSA.3 实现对安全属性的管理。

- d) O.ENCRYPT:该目的可通过安全功能要求 FCS_CKH_EXT.1、FCS_CKM.1、FCS_CKM.2、FCS_CKM.3、FCS_CKM.5、FCS_CKM.6 和 FCS_COP.1 实现数据加密过程中的密钥生成、协商、派生、销毁和密码运算进行要求,通过安全功能要求 FDP_SDC.1 实现数据的加密存储。
- e) O.RESIDUALINFO:该目的可通过安全功能要求 FDP_RIP.2 实现残余数据和属性的保护和控制,保证残余数据不会被非授权用户使用从而导致用户敏感信息的丢失。
- f) O.SECCOM:该目的可通过安全功能要求 FTP_ITC.1 提供 TSF 间可信信道,对传输的数据进行加密。
- g) O.SESSIONMANAG:该目的可通过安全功能要求 FTA_SSL.1 和 FTA_SSL.2 实现会话锁定管理,解锁时通过安全功能要求 FIA_UAU.6 实现会话恢复时的重鉴别功能。
- h) O.INTEGRITY:该目的可通过安全功能要求 FPT_AEX_EXT.1、FPT_AEX_EXT.2、FPT_AEX_EXT.3、FPT_AEX_EXT.4、FPT_AEX_EXT.5、FPT_FLS.1、FPT_JTA_EXT.1、FPT_PHP. 3、FPT_RCV. 2、FPT_SEE_EXT. 1、FPT_STG_EXT. 1、FPT_TST_EXT. 1、FPT_TST_EXT.2、FPT_TUD_EXT.1/OS 和 FPT_TUD_EXT.1/APP 实现 TOE 启动、更新和运行提供完整性保护机制,防止系统镜像、升级包、内核等 TOE 关键数据被非法篡改,以及 TOE 的安全功能被绕过;通过安全功能要求 FMT_SMF.1 实现系统安全更新的管理。
- i) O.DEVAUTH:该目的可通过安全功能要求 FIA_UAU.5/DEVICE、FTP_ITC.1/DEVICE 对端设备身份鉴别机制,在通信之前应对对端设备进行身份鉴别。
- j) O.PRIVACY:该目的可通过安全功能要求 FPR_PSE.1/APPDEV 和 FPR_PSE.1/AD 是实现为应用软件提供可重置设备标识符,防止应用开发者和广告主跟踪用户,实现应用开发者或广告厂商收集的用户数据不能与 TOE 的固定设备标识符绑定,保护用户隐私安全。

10.3 组件依赖关系

选取组件时,需符合所选组件之间的相互依赖关系,表 26 和表 27 分别列出了所选安全功能组件和安全保障组件的依赖关系说明。

表 26 安全功能组件依赖关系

序号	安全功能组件	依赖关系
1	FAU_GEN.1	FPT_STM.1
2	FAU_STG.2	FAU_GEN.1
3	FAU_STG.5	FAU_STG.2、FAU_GEN.1
4	FCS_CKH_EXT.1/Low	FCS_CKM.1/Symmetric,或 FCS_CKM.1/Asymmetric,FCS_CKM.5 FCS.COP.1/ENCRYPT
5	FCS_CKH_EXT.1/ MediumHigh	FCS_CKM.1/Symmetric,或 FCS_CKM.1/Asymmetric,FCS_CKM.5 FCS.COP.1/ENCRYPT
6	FCS_CKM.1/Symmetric	FCS_CKM.2,或 FCS_CKM.5,或 FCS_COP.1/HASH; FCS_RNG.1; FCS_CKM.6
7	FCS_CKM.1/Asymmetric	FCS_CKM.2,或 FCS_CKM.5,或 FCS_COP.1/HASH; FCS_RNG.1; FCS_CKM.6

表 26 安全功能组件依赖关系（续）

序号	安全功能组件	依赖关系
8	FCS_CKM.2	FCS_CKM.1/Symmetric,或 FCS_CKM.1/Asymmetric,或 FCS_CKM.5
9	FCS_CKM.5	FCS_CKM.2,或 FCS_COP.1/HASH;FCS_CKM.6
10	FCS_CKM.6	FCS_CKM.1/Symmetric,或 FCS_CKM.1/Asymmetric
11	FCS_CKM_EXT.1	无依赖关系
12	FCS_COP.1/SIGN	c FCS_CKM.1/Symmetric,或 FCS_CKM.1/Asymmetric; FCS_CKM.5
13	FCS_COP.1/ENCRYPT	FCS_CKM.1/Symmetric,或 FCS_CKM.1/Asymmetric; FCS_CKM.5
14	FCS_COP.1/HASH	无依赖关系,HASH算法不涉及密钥生成或销毁
15	FCS_COP.1/KEYHMAC	FCS_CKM.1/Symmetric,或 FCS_CKM.1/Asymmetric; FCS_CKM.5
16	FCS_RNG.1	无依赖关系
17	FDP_ACC.1/MAC	FDP_ACF.1/MAC
18	FDP_ACC.1/DAC	FDP_ACF.1/DAC
19	FDP_ACC.1/SYSCALL	FDP_ACF.1/SYSCALL
20	FDP_ACC.1/Permission	FDP_ACF.1/Permission
21	FDP_ACC.1/UserData	FDP_ACF.1/UserData
22	FDP_ACC.1/SEE	FDP_ACF.1/SEE
23	FDP_ACC.1/DTC	FDP_ACF.1/DTC
24	FDP_ACF.1/MAC	FDP_ACC.1/MAC
25	FDP_ACF.1/DAC	FDP_ACC.1/DAC
26	FDP_ACF.1/SYSCALL 制	FDP_ACC.1/SYSCALL
27	FDP_ACF.1/Permission	FDP_ACC.1/Permission
28	FDP_ACF.1/UserData	FDP_ACC.1/UserData
29	FDP_ACF.1/SEE	FDP_ACC.1/SEE
30	FDP_ACF.1/DTC	FDP_ACC.1/DTC
31	FDP_RIP..2	无依赖关系
32	FDP_SDC.1	无依赖关系
33	FIA_AFL.1	FIA_UAU.1
34	FIA_SOS.1	无依赖关系
35	FIA_SOS.2 TSF	无依赖关系
36	FIA_UAU.1	FIA_UID.1
37	FIA_UAU.5/USER	无依赖关系
38	FIA_UAU.5/DEVICE	无依赖关系

表 26 安全功能组件依赖关系（续）

序号	安全功能组件	依赖关系
39	FIA_UAU.5/APP	无依赖关系
40	FIA_UAU.6	无依赖关系
41	FIA_UAU.7	FIA_UAU.1
42	FIA_UID.1	无依赖关系
43	FIA_API.1	无依赖关系
44	FMT_MSA.1/Permission	FDP_ACC.1/Permission; FMT_SMF.1; 移动终端通常只有授权用户角色,无需选择组件 FMT_SMR.1
45	FMT_MSA.3/Permission	FMT_MSA.1/Permission;移动终端通常只有授权用户角色,无需选择 组件FMT_SMR.1
46	FMT_SMF.1	无依赖关系
47	FPR_PSE.1/APPDEV	无依赖关系
48	FPR_PSE.1/AD	无依赖关系
49	FPT_AEX_EXT.1	无依赖关系
50	FPT_AEX_EXT.2	无依赖关系
51	FPT_AEX_EXT.3	无依赖关系
52	FPT_AEX_EXT.4	无依赖关系
53	FPT_AEX_EXT.5	无依赖关系
54	FPT_FLS.1	无依赖关系
55	FPT_JTA_EXT.1 JTAG	无依赖关系
56	FPT_PHP.3	无依赖关系
57	FPT_RCV.2	AGD_OPE.1
58	FPT_SEE_EXT.1	无依赖关系
59	FPT_STG_EXT.1	FCS.COP.1/SIGN,或FCS.COP.1/ENCRYPT,或FCS.COP.1/HASH, 或FCS.COP.1/KEYHMAC
60	FPT_STM.1	无依赖关系
61	FPT_TST_EXT.1	FCS.COP.1/SIGN;FCS.COP.1/HASH
62	FPT_TST_EXT.2	FCS.COP.1/SIGN;FCS.COP.1/HASH
63	FPT_TUD_EXT.1/OS	FCS.COP.1/SIGN;FCS.COP.1/HASH
64	FPT_TUD_EXT.1/APP	FCS.COP.1/SIGN;FCS.COP.1/HASH
65	FTA_SSL.1 TSF	FIA_UAU.1
66	FTA_SSL.2	FIA_UAU.1
67	FTP_ITC.1/TLS	无依赖关系
68	FTP_ITC.1/DEVICE	无依赖关系

表 27 安全保障组件依赖关系

序号	安全保障组件	依赖关系
1	ADV_ARC.1	ADV_FSP.1;ADV_TDS.1
2	ADV_FSP.2	ADV_TDS.1
3	ADV_FSP.3	ADV_TDS.1
4	ADV_FSP.4	ADV_TDS.1
5	ADV_FSP.5	ADV_TDS.1;ADV_IMP.1
6	ADV_IMP.1	ADV_TDS.3;ALC_TAT.1
7	ADV_INT.2	ADV_IMP.1;ADV_TDS.3;ALC_TAT.1
8	ADV_TDS.1	ADV_FSP.2
9	ADV_TDS.2	ADV_FSP.3
10	ADV_TDS.3	ADV_FSP.4
11	ADV_TDS.4	ADV_FSP.5
12	AGD_OPE.1	ADV_FSP.1
13	AGD_PRE.1	无依赖关系
14	ALC_CMC.2	ALC_CMS.1
15	ALC_CMC.3	ALC_CMS.1;ALC_DVS.1;ALC_LCD.1
16	ALC_CMC.4	ALC_CMS.1;ALC_DVS.1;ALC_LCD.1
17	ALC_CMS.2	无依赖关系
18	ALC_CMS.3	无依赖关系
19	ALC_CMS.4	无依赖关系
20	ALC_CMS.5	无依赖关系
21	ALC_DEL.1	无依赖关系
22	ALC_DVS.1	无依赖关系
23	ALC_FLR.1	无依赖关系
24	ALC_FLR.3	无依赖关系
25	ALC_LCD.1	无依赖关系
26	ALC_TAT.1	ADV_IMP.1
27	ALC_TAT.2	ADV_IMP.1
28	ASE_CCL.1	ASE_INT.1;ASE_ECD.1;ASE_REQ.1
29	ASE_ECD.1	无依赖关系
30	ASE_INT.1	无依赖关系
31	ASE_OBJ.2	ASE_SPD.1
32	ASE_REQ.2	ASE_OBJ.2; ASE_ECD.1
33	ASE_SPD.1	无依赖关系
34	ASE_TSS.1	ASE_INT.1;ASE_REQ.1;ADV_FSP.1

表 27 安全保障组件依赖关系（续）

序号	安全保障组件	依赖关系
35	ATE_COV.1	ADV_FSP.2;ATE_FUN.1
36	ATE_COV.2	ADV_FSP.2;ATE_FUN.1
37	ATE_DPT.1	ADV_ARC.1;ADV_TDS.2;ATE_FUN.1
38	ATE_DPT.2	ADV_ARC.1;ADV_TDS.3;ATE_FUN.1
39	ATE_DPT.3	ADV_ARC.1;ADV_TDS.4;ATE_FUN.1
40	ATE_FUN.1	ATE_COV.1
41	ATE_IND.2	ADV_FSP.2;AGD_OPE.1;AGD_PRE.1;ATE_COV.1; ATE_FUN.1
42	AVA_VAN.2	ADV_ARC.1;ADV_FSP.2;ADV_TDS.1;AGD_OPE.1; AGD_PRE.1
43	AVA_VAN.3	ADV_ARC.1;ADV_FSP.4;ADV_TDS.3;ADV_IMP.1; AGD_OPE.1;AGD_PRE.1;ATE_DPT.1
44	AVA_VAN.4	ADV_ARC.1;ADV_FSP.4;ADV_TDS.3;ADV_IMP.1; AGD_OPE.1;AGD_PRE.1;ATE_DPT.1

附录 A

(资料性)

用户数据保护和密钥层次结构

A.1 用户数据保护

TOE 通常对其存储的用户数据资产进行分类保护,一般分为以下三类:

- a) 低级别数据资产:该类数据在 TOE 关机时处于加密状态,被基于设备唯一密钥派生出来的数据加密密钥保护,在用户开机后但还没有解锁屏幕前即可对数据进行解密,如自动锁屏时长或响铃模式;
- b) 中级别数据资产:该类数据被用户锁屏口令和设备唯一密钥共同保护,在 TOE 开机后且用户首次输入锁屏口令解锁 TOE 对数据进行解密,如图库、联系人、短信、日历或通话记录等;
- c) 高级别数据资产:该级别数据被用户锁屏口令和设备唯一密钥共同保护,在 TOE 开机且用户首次输入锁屏口令解锁 TOE 后对数据进行解密,重新锁定屏幕后,数据被重新加密,解锁之前不可访问和解密,如用户健康数据等。

A.2 密钥层次结构

密钥层次结构用于说明密钥的生成、派生关系。密钥有两种主要类型:数据加密密钥和密钥加密密钥,根密钥也可认为是密钥加密密钥。数据加密密钥用于保护数据,利用加密算法对数据进行加密存储。密钥加密密钥用于保护其他密钥(如数据加密密钥或其他密钥加密密钥),密钥层次结构见图 A.1。

每一类用户数据资产都由数据加密密钥加密,同时这些数据加密密钥被密钥加密密钥保护,每个数据加密密钥或密钥加密密钥可随机生成,或可从其他密钥(如根密钥)/信息(如用户口令)派生,也可组合随机方式和派生方式生成。密钥层次结构通常从根密钥和/或用户口令,并对数据加密密钥、密钥加密密钥进行派生或加密,具体见每类数据的密钥层次组件(FCS_CKH_EXT.1/Low 和 FCS_CKH_EXT.1/MediumHigh)描述。

设备唯一密钥是在设备生产过程中预置在设备硬件中的唯一密钥,它只能由硬件加密模块访问,而不会直接暴露给任何设备软件。

为了防止攻击者解密用户数据资产,所有在层次结构中用于密钥派生的密钥和信息都需要受到保护,可通过使用密钥加密密钥进行加密存储,也可销毁使用后的数据加密密钥或密钥加密密钥,在需要使用时重新生成或派生。另外,通过硬件对数据加密密钥或密钥加密密钥进行安全存储也是防止攻击者解密用户资产的一种方式(见安全功能要求 FPT_PHP.3)。

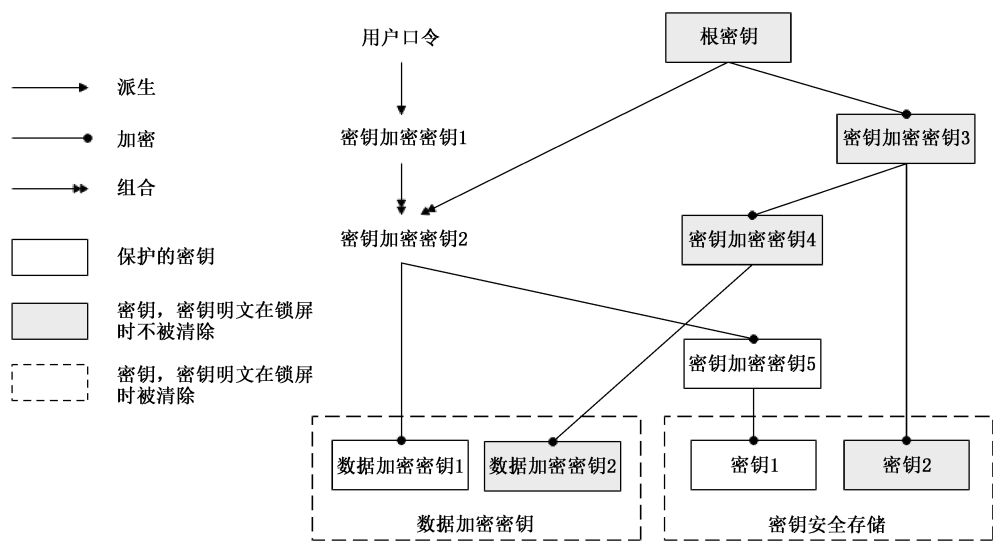


图 A.1 密钥层次结构

参 考 文 献

- [1] GB/T 18336.2 网络安全技术 信息技术安全评估准则 第2部分:安全功能组件
 - [2] GB/T 22186—2016 信息安全技术 具有中央处理器的 IC 卡芯片安全技术要求
 - [3] GB/T 25069—2022 信息安全技术 术语
 - [4] GB/T 30270—2024 网络安全技术 信息技术安全评估方法
 - [5] GB/T 30284—2020 信息安全技术 移动通信智能终端操作系统安全技术要求
 - [6] ISO/IEC 18033-1:2021 Information security—Encryption algorithms—Part 1:General
-

