电 信 终 端 产 业 协 会 标 准

TAF-WG4-AS0048-V1.0.0:2019

移动智能终端防非授权刷机能力技术要求

Mobile Intelligent Terminal Technical Requirements for Anti-unauthorized Flash Capability

2019 -12 -26 发布　　2019 -12 - 26 实施

电信终端产业协会　　发 布

目　　次

前　言

本标准按照 GB/T 1.1-2009给出的规则起草。

本标准由电信终端产业协会提出并归口。

本标准起草单位：中国信息通信研究院、北京小米移动软件有限公司

本标准主要起草人：乜聚虎、江小威、周圣炎、赵驰、杜云、汪薇薇、詹维骁、董雾

引　　言

随着移动智能终端设备的广泛普及和应用，移动智能终端操作系统的安全性和防刷机能力越来越重要。目前市场上存在的非授权刷机行为，对用户和终端厂商都造成了巨大的损失。终端设备在销售流通环节，被刷入篡改过的操作系统，预置大量未经安全审核和充分测试的劣质应用，甚至被植入病毒和后门程序，对用户的正常使用，数据隐私安全以及厂商的声誉造成极坏的影响。本标准的制定，旨在提高移动智能终端防止非授权刷机的能力，防范非授权刷机所导致的各种问题。

本标准的基本原则是：移动智能终端应当能够防范智能移动终端流通过程中的非法授权刷机行为。本标准并不规定具体的实现方法和措施，以利于创新和发展。本标准从安全启动能力要求，刷机管控能力要求，防降级能力要求，算法和密钥安全能力要求，漏洞修复能力要求 5 个层面对移动终端防非授权刷机能力提出了要求，并从实施效果，实现难度等方面对防非授权刷机安全能力进行了分级。

本标准是针对移动智能终端销售流通环节的非授权刷机行为提出的能力技术要求，对终端厂商开放给终端用户的刷机能力和管控措施等不做要求。

移动智能终端防非授权刷机能力技术要求

1 范围

本标准规定了移动智能终端防非授权刷机能力的技术要求，包括安全启动能力要求，刷机控制能力要求，防降级能力要求，算法和密钥安全能力要求，漏洞修复能力要求等，并对安全能力进行了分级。本标准适用于各种制式的移动智能终端，但不适用于特殊行业、专业终端（比如个人电脑），但可做参考引用。

2 规范性引用文件

3 术语、定义和缩略语

3.1 术语和定义

3.1.1 移动智能终端操作系统 operator system of smart mobile terminal

移动智能终端最基本的系统软件，它控制和管理移动智能终端各种硬件和软件资源，并提供应用程序开发接口。

3.1.2 非授权刷机

在未经许可的情况下，绕过移动智能终端安全机制，更改或者替换操作系统的行为；在未经过用户同意的情况下，绕过用户的密码保护，对操作系统进行更改或清空用户数据的行为。

3.1.3 OTA

OTA（Over－the－Air Technology）空中下载技术。是通过移动通信（GSM 或 CDMA）的空中接口对 SIM 卡数据及应用进行远程管理的技术。在移动智能终端系统上的 OTA 一般是指通过网络接口下载操作系统升级数据并进行安装的技术。

3.1.4 数字签名 digital signature

附在数据单元后面的数据，或对数据单元进行密码变换得到的数据。允许数据的接受者验证数据的来源和完整性，保护数据不被篡改、伪造，并保证数据的不可否认性。

3.2 缩略语

CNNVD	China National Vulnerability Database of Information Security	中国国家信息安全漏洞库
CNVD	China National Vulnerability Database	国家信息安全漏洞共享平台

4 移动智能终端防非授权刷机能力框架及目标

4.1 移动智能终端安全能力框架

移动智能终端防非授权刷机能力主要由安全启动能力、刷机控制能力、防降级能力、算法和密钥安全能力、漏洞修复要求五部分构成。

4.2 移动智能终端安全目标

4.2.1 安全启动目标

移动智能终端安全启动目标是从软硬件等层面保证移动智能终端只运行合法来源的程序和数据。

4.2.2 刷机控制目标

刷机控制的目标是确保移动智能终端操作系统的代码和数据的安全，保证操作系统仅在授权的情况下被更改和替换。

4.2.3 防降级安全目标

防降级安全目标是要保证移动智能终端系统运行最新的操作系统，具备禁止替换和运行旧版本系统的能力，不受旧版本已知安全漏洞的影响。

4.2.4 算法和密钥保护目标

算法和密钥保护的目标是确保防非授权刷机安全机制所使用的算法和密钥具有足够的安全强度，能够经受一般的穷举和密码分析等攻击手段。

4.2.5 漏洞修复要求目标

漏洞修复要求的目标是保证移动智能终端操作系统不含有任何已知的，能够破坏防非授权刷机能力的安全漏洞。

5 移动智能终端防非授权刷机能力要求

5.1 基本要求

移动智能终端设备应当具备防止系统被非授权刷机的能力。移动智能终端设备可能支持多种刷机方式，用于工厂生产、售后维修、开发调试，以及用户正常升级系统，移动智能终端应当具备对所有刷机方式的控制能力，防止被非法利用。

移动智能终端设备应当具备检测操作系统完整性，识别操作系统来源合法性，以及检测操作系统版本正确性的能力。对于非法来源、无法验证完整性或者版本错误的操作系统，应当能够识别，并根据策略采取必要的措施，如拒绝运行，或者告知用户等。

移动智能终端实现防非授权刷机能力的算法和密钥应当具有足够的安全强度以抵抗可能的穷举和密码分析等攻击方式。操作系统应当及时修复已知的能够破坏防非授权刷机能力的安全漏洞。

5.2 安全启动能力

对移动智能终端设备启动代码和操作系统代码及数据进行完整性校验，验证代码和数据来源合法性。

5.2.1 信任根不可篡改

完整性校验以及来源合法性校验的信任根应当保存在只读存储器等不可被篡改、删除的软硬件环境当中。

5.2.2 启动代码的安全校验

移动智能终端的操作系统引导启动代码和数据应当能够通过数字签名等技术进行完整性和来源合法性校验。如果无法通过校验，应根据产品策略采取适当措施，如拒绝启动，或者告知用户等。

5.2.3 操作系统的安全校验

移动智能终端操作系统代码和数据应当能够进行完整性和来源合法性的校验。如果无法通过校验，应根据产品策略采取适当措施，如拒绝启动，或者告知用户等。

5.3 刷机控制能力

移动智能终端的刷机方式，按照用途和方式一般可以分为以下两类：1）OTA，用于正常的版本升级迭代，可以包括在线OTA和本地安装包升级（卡刷）；2）工厂镜像刷机，主要用于工厂生产和开发调试，如fastboot，edl等刷机方式。移动终端应当能够对所有刷机方式进行严格控制，防止设备在销售流通环节被非授权刷机。

5.3.1 OTA 升级控制

5.3.1.1 OTA 升级完整性和来源合法性检查

OTA升级之前，应当对升级包的完整性和来源合法性进行校验，仅允许安装经过验证的升级包。

5.3.1.2 OTA 升级版本检查

OTA升级之前，应当能够识别升级包的版本，并能够根据当前系统版本、目标系统版本和升级策略决定是否允许升级。

5.3.2 工厂刷机方式控制

移动智能终端应当对所有工厂刷机方式具有权限控制能力，例如通过账号权限、硬件设备等，能够识别并阻止非授权的刷机行为。

5.4 防降级能力

具备防止操作系统及启动代码版本降级的能力。

5.4.1 禁止版本回退的能力

移动智能终端应该具备识别、阻止旧版本的软件通过各种刷机方法被刷入系统的能力。厂商可以根据自己的升级策略，选择是否允许版本的回退。

5.4.2 基于软件的防降级能力

移动智能终端能够通过本地保存的版本信息或者网络请求的方式等软件方案，识别当前运行版本是否发生降级。如发现降级，应该根据策略采取适当措施， 如拒绝继续执行，或者告知用户等。

5.4.3 基于硬件的防降级能力

通过不可篡改的硬件保存启动代码和操作系统的版本信息，能够准确识别当前版本是否发生降级。当前软件版本低于硬件中保存的版本时，应该根据策略采取适当措施， 如拒绝继续执行，或者告知用户等。

5.5 算法和密钥强度

防非授权刷机安全机制所使用的密钥和相关密码算法，应当具有足够的安全强度抵抗已知的攻击方法，不应当使用已被证实存在弱点的密码算法，如 md5，DEA。

5.6 操作系统漏洞修复

操作系统及其启动代码，在量产阶段，应当及时修复CNVD、CNNVD等公布的刷机相关安全漏洞。按照不同安全等级，需满足以下要求之一。

5.6.1 普通漏洞修复速度

修复CNVD、CNNVD等已公布9个月的刷机相关安全漏洞。

5.6.2 较快漏洞修复速度

修复CNVD、CNNVD等已公布6个月的刷机相关安全漏洞。

5.6.3 快速漏洞修复速度

修复CNVD、CNNVD等已公布3个月的刷机相关安全漏洞。

6 移动智能终端防非授权刷机安全能力分级

6.1 概述

移动智能终端所支持的防非授权刷机安全能力划分为三个等级，第三等级是最高等级：
一级：基本的安全启动能力，普通漏洞修复速度
二级：软件防降级能力，较快漏洞修复速度
三级：硬件防降级能力，快速漏洞修复速度

6.2 防非授权刷机安全能力分级

根据移动智能终端所支持的防非授权刷机安全能力的程度，将移动智能终端防非授权刷机安全能力自低到高划分为三个等级。在每一个等级定义了移动智能终端在相应等级对应的安全能力的最小集合，即移动智能终端必须支持该集合中的所有安全能力才能标识为该级别：

防非授权刷机能力		防非授权刷机能力等级		
		一级	二级	三级
1.	5.2.1 基于硬件的信任根	√	√	√
2.	5.2.2 启动代码的安全校验	√	√	√
3.	5.2.3 操作系统的安全校验	√	√	√
4.	5.3.1.1 OTA 升级完整性和来源合法性检查	√	√	√

5.	5.3.1.2 OTA 升级版本检查	√	√	√
6.	5.3.2 工厂刷机方式控制			√
7.	5.4.1 禁止版本回退		√	√
8.	5.4.2 基于软件的防降级能力		√	
9.	5.4.3 基于硬件的防降级能力			√
10.	5.5 算法和密钥强度	√	√	√
11.	5.6.1 修复公布 9 个月的漏洞	√		
	5.6.2 修复公布 6 个月的漏洞		√	
	5.6.3 修复公布 3 个月的漏洞			√

附 录 A
（规范性附录）
标准修订历史

修订时间	修订后版本号	修订内容

附 录 B
（资料性附录）
附录

参 考 文 献