



中华人民共和国公共安全行业标准

GA/T 1540—2018

信息安全技术 个人移动终端安全管理产品测评准则

Information security technology Testing and evaluation criteria for personal mobile terminal security management products

2018 - 12 - 27 发布

2018 - 12 - 27 实施

中华人民共和国公安部 发布

目 次

前言	II
1 范围	3
2 规范性引用文件	3
3 术语和定义	3
4 缩略语	4
5 受检要求	4
5.1 检验周期	4
5.2 测试用例要求	4
5.3 资料要求	4
6 功能要求	4
6.1 产品安装卸载	4
6.2 病毒防护与处置	4
6.3 系统检测与优化	5
6.4 备份与恢复	6
6.5 隐私保护	6
6.6 流量监控	6
6.7 通信拦截	7
6.8 防盗保护	7
6.9 产品更新	7
6.10 兼容性	7
6.11 自身安全	8
7 测试方法	8
7.1 总体说明	8
7.2 测试环境与工具	8
7.3 产品安装卸载	8
7.4 病毒防护与处置	8
7.5 系统检测与优化	9
7.6 备份与恢复	10
7.7 隐私保护	11
7.8 流量监控	11
7.9 通信拦截	12
7.10 防盗保护	12
7.11 产品更新	12
7.12 兼容性	13
7.13 自身安全	13
8 报告格式	13
9 评级方法	15

前 言

本标准按照GB/T 1.1-2009给出的规则起草。

本标准由公安部网络安全保卫局提出。

本标准由公安部信息系统安全标准化技术委员会归口。

本标准起草单位：国家计算机病毒应急处理中心、公安部十一局七处、天津市公安局网络安全保卫总队、北京网秦天下科技有限公司、北京金山安全软件有限公司、腾讯科技（深圳）有限公司、北京奇虎科技有限公司、北京安管佳科技有限公司、卡巴斯基技术开发(北京)有限公司、南开大学、江苏通付盾信息安全技术有限公司、恒安嘉新（北京）科技股份公司、北京启明星辰信息安全技术有限公司、北京奇虎科技有限公司、北京天融信科技有限公司。

本标准主要起草人：陈建民、刘彦、张俊兵、祝国邦、黄一斌、杜振华、杨键、张韞菁、张瑞、曹鹏、冯军亮、孟彬、王文一、李尘一、张楠、张华锐、矫日明、石磊、关鹏、贾春福、张振伟、崔婷婷、徐雨晴、郭颖、王龔。

信息安全技术 个人移动终端安全管理产品测评准则

1 范围

本标准规定了个人移动终端安全管理产品的受检要求、功能要求、测试方法、报告格式及评级方法。本标准适用于个人移动终端安全管理产品的开发和检测。

2 规范性引用文件

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

GA 243-2000 计算机病毒防治产品评级准则

GA/T 757-2008 程序功能检验方法

GA 849-2009 移动终端病毒防治产品评级准则

3 术语和定义

GA 243-2000、GA/T 757-2008、GA 849-2009界定的以及下列术语和定义适用于本文件。

3.1

个人移动终端 personal mobile terminal

个人使用的便携式电子设备，包括智能手机、平板电脑等。

3.2

个人移动终端安全管理产品 personal mobile terminal security management product

用于管理个人移动终端，保护个人计算环境安全的产品。

3.3

移动终端合规性 mobile terminal compliance

移动终端应符合国家制定的安全策略。

3.4

恶意行为 malicious behavior

未经用户授权，访问移动终端中的信息，并将获取的信息通过移动终端信息交互功能向特定目标发送；未经许可调用移动终端的各种功能，窃取用户隐私，系统破坏等。

3.5

系统优化 system optimization

对个人移动终端系统进行垃圾文件清理、开机自启程序管理、紧急关闭第三程序、文件管理、磁盘管理等一系列的优化功能。

3.6

流量监控 data traffic monitor

对个人移动终端联网流量进行监控，并监控当前联网程序和以往联网记录。

3.7

信息业务 information service

通信系统提供的通信终端之间，或者通信终端与其他信息实体之间进行文字、图片信息收发的业务。

3.8

垃圾信息 spam text

内容违法违规或违背手机用户主观意志并且在客观上对用户造成工作生活上骚扰或者用户权益上侵害的信息。

4 缩略语

下列缩略语适用于本文件。

SMS: 短消息 (Short Messaging System)

MMS: 彩信 (Multimedia Messaging Service)

WAP: 无线应用协议 (Wireless Application Protocol)

WLAN: 无线局域网 (Wireless Local Area Networks)

URL: 统一资源定位符 (Uniform Resource Locator)

5 受检要求

5.1 检验周期

检验机构对程序版本发生重大升级或名称发生改变的个人移动终端安全管理产品应进行检验；同时，可以根据安全威胁的发展情况对个人移动终端安全管理产品进行专项检验。

5.2 测试用例要求

受检企业应提交其产品检验用的测试用例。

5.3 资料要求

本项要求包括：

- a) 受检企业应提交产品研发人员的个人简历；
- b) 受检企业应提交产品的中文使用说明书；
- c) 受检企业应提交核封完整的正式产品。

6 功能要求

6.1 产品安装卸载

产品应能正常安装和正常卸载。

6.2 病毒防护与处置

6.2.1 病毒防护途径

产品应能检测并阻断通过以下途径入侵的病毒样本：

- a) 网络；
- b) 外部设备。

6.2.2 病毒检测能力

产品对病毒样本库中的样本至少能检测其中的85%。

6.2.3 病毒清除能力

产品对病毒样本库中的样本至少能清除其中的80%。

6.2.4 误报率

产品对误报样本库中的样本的误报率不能高于0.1%。

6.2.5 备份功能

产品清除病毒时，应具有备份染毒文件的功能。

6.2.6 恶意 URL 拦截

产品应根据预设规则对恶意的URL进行拦截。

6.2.7 配置功能

产品应具备以下配置功能：

- a) 自定义路径扫描；
- b) 计划扫描。

6.3 系统检测与优化

6.3.1 系统状态检测

产品应能检测以下内容的系统状态：

- a) 应用安装情况；
- b) 内存使用情况；
- c) 自启动应用；
- d) 垃圾文件；
- e) 磁盘剩余空间。

6.3.2 系统优化

产品应能优化以下系统性能：

- a) 释放系统内存；
- b) 自启动项设置；
- c) 垃圾文件清除。

6.3.3 电源管理

产品应能按以下内容对移动终端的电池使用状况进行检测和管理：

- a) 检测应用程序耗电情况；
- b) 自动或手动设置省电模式。

6.4 备份与恢复

6.4.1 本地备份与恢复

产品应能备份和恢复以下内容：

- a) 通讯录；
- b) 信息；
- c) 通话记录；
- d) 日历。

6.4.2 网络备份与恢复

产品应提供以下网络备份方式：

- a) 同系统平台；
- b) 跨系统平台。

6.5 隐私保护

6.5.1 信息访问权限控制

产品能对应用程序访问涉及用户个人隐私的行为进行报警并记入日志：

- a) 位置信息；
- b) 通话；
- c) 短信彩信；
- d) 通讯录；
- e) 历史记录；
- f) 相册。

6.5.2 应用程序使用权限控制

产品应能对用户使用应用程序的行为进行权限控制。

6.5.3 隐私空间设置

用户能设置隐私空间，用于加密存储隐私数据。

6.6 流量监控

6.6.1 流量实时监控

产品应能对移动终端的网络流量进行实时监控，并可以在移动终端上进行实时的显示。

6.6.2 流量按周期统计

产品应能对移动终端的网络流量监控数据可以按照天、月等周期进行统计查询。

6.6.3 流量按应用统计

产品应能对移动终端的网络流量监控数据可以按照应用程序进行统计和查询。

6.6.4 流量套餐设置与超额提示

产品应根据用户使用的流量套餐进行限额设置，并在达到阈值时进行提示。

6.6.5 应用程序联网控制

产品应对应用程序的联网行为进行控制。

6.7 通信拦截

6.7.1 垃圾信息拦截

产品应对垃圾信息进行智能的拦截并进行提示。

6.7.2 恶意来电拦截

产品应对恶意来电有效的识别，并进行记录和提示。

6.7.3 黑白名单拦截

产品应将自定义的电话号码、号码特征串添加到黑白名单中，并根据黑白名单智能拦截。

6.8 防盗保护

6.8.1 设备锁定

产品应能锁定被盗的移动终端。

6.8.2 回传被盗设备信息

产品应能回传以下信息：

- a) 位置信息；
- b) 通话记录；
- c) 被盗设备当前号码；
- d) 摄像头拍照信息。

6.8.3 远程数据擦除

产品应能远程擦除被盗终端上的指定信息。

6.9 产品更新

6.9.1 病毒库更新

产品应支持手动或自动的方式进行升级，对病毒库、策略文件进行更新，且支持增量升级。

6.9.2 程序更新

产品应支持手动或自动的方式进行程序更新，且支持增量升级。

6.10 兼容性

6.10.1 支持主流机型

产品应支持主流的移动终端机型，并能正常地安装、使用、卸载。

6.10.2 支持主流系统版本

产品应支持主流的移动终端系统版本，并能正常地安装、使用、卸载。

6.11 自身安全

6.11.1 开机自动启动

产品应能在系统启动时自动加载。

6.11.2 防止异常终止进程

产品应能保障正常运行，防止被第三方程序结束进程。

6.11.3 防止异常卸载

产品应能防止异常卸载。

7 测试方法

7.1 总体说明

测评方法与技术要求意义对应，它给出具体的测评方法来验证个人移动终端安全管理产品是否达到技术要求中所提出的要求。它由测试环境、测试工具、测试方法和预期结果四个部分构成。

7.2 测试环境与工具

测试环境是接入无线网络的移动终端设备及网络。

测试工具有移动智能终端、用例库、控制软件。

7.3 产品安装卸载

产品应能正常安装及卸载：

a) 测试方法：

- 1) 将产品安装文件通过数据线传输到移动终端设备内存中并安装；
- 2) 通过移动终端设备设置中的应用程序管理手动卸载产品。

b) 预期结果：

- 1) 产品正常安装后，可以打开产品界面并可使用各项功能；
- 2) 产品正常卸载后，在应用程序里找不到该产品。

7.4 病毒防护与处置

7.4.1 病毒防护途径

产品应能检测并阻断通过以下途径入侵的病毒样本：

a) 测试方法：

- 1) 通过网络将病毒样本传输到本地内存中；
- 2) 通过外部设备将病毒样本传输到本地内存中。

b) 预期结果：

- 1) 产品能够检测通过网络传输的病毒样本，发出报警；
- 2) 产品能够检测通过外部设备传输的病毒样本，发出报警。

7.4.2 病毒检测能力

产品应能对病毒样本库中的样本进行检测：

- a) 测试方法：将测试病毒样本库用数据线传输到移动终端设备内存中，并启动病毒扫描功能扫描移动终端设备内存；
- b) 预期结果：产品对病毒样本库中的样本至少能检测其中的 85%。

7.4.3 病毒清除能力

产品应能对病毒样本库中的样本进行清除：

- a) 测试方法：进行 7.4.2 a) 测试并执行病毒清除操作；
- b) 预期结果：产品对病毒样本库中的样本至少能清除其中的 80%。

7.4.4 误报率

产品应能对病毒误报样本库中的样本进行误报检测：

- a) 测试方法：将测试病毒误报样本库用数据线传输到移动终端内存中，并启动病毒扫描功能扫描移动终端内存；
- b) 预期结果：产品不会对误报样本库中的样本产生误报。

7.4.5 备份功能

产品应能对染毒文件进行备份：

- a) 测试方法：打开产品的病毒样本备份功能，进行 7.4.3 测试后，查看产品的病毒备份区；
- b) 预期结果：备份区里存储被清除前的样本文件，并可将其还原。

7.4.6 恶意 URL 拦截

产品应能对恶意的 URL 进行拦截：

- a) 测试方法：配置产品恶意 URL 拦截功能，用系统内置浏览器访问恶意地址连接；
- b) 预期结果：产品报警提示，并阻断访问请求。

7.4.7 配置功能

产品应根据需求进行配置：

- a) 测试方法：
 - 1) 配置指定病毒扫描路径扫描系统；
 - 2) 设定病毒计划扫描条件。
- b) 预期结果：
 - 1) 产品能按照指定的扫描路径进行病毒扫描；
 - 2) 触发计划扫描条件时，产品能进行病毒扫描。

7.5 系统检测与优化

7.5.1 系统状态检测

产品应能检测系统状态：

- a) 测试方法：
 - 1) 通过产品检测应用程序安装情况，查看检测结果；
 - 2) 通过产品查询内存使用情况，查看检测结果；

- 3) 通过产品查询自启动应用, 查看检测结果;
- 4) 通过产品查询系统垃圾文件, 查看检测结果;
- 5) 通过产品查询磁盘剩余空间, 查看检测结果。

b) 预期结果:

- 1) 产品能够显示已经安装的应用程序及占用磁盘空间大小;
- 2) 产品能够显示进程中的程序名称及内存占用大小;
- 3) 产品能够显示开机自启动程序的情况;
- 4) 产品能够显示系统中垃圾文件的情况;
- 5) 产品能够显示当前系统磁盘剩余存储空间。

7.5.2 系统优化

产品应能进行系统性能优化:

a) 测试方法:

- 1) 进行 7.5.1 a) 2) 测试, 并执行产品中内存清理动作;
- 2) 进行 7.5.1 a) 3) 测试, 设置关闭自启动程序并重启移动终端;
- 3) 进行 7.5.1 a) 4) 测试, 并执行产品中垃圾文件清理动作。

b) 预期结果:

- 1) 产品能结束进程中的应用程序, 并释放内存空间;
- 2) 移动终端重启后, 被关闭的自启动程序未启动;
- 3) 产品能清除系统垃圾文件, 并释放磁盘空间。

7.5.3 电源管理

产品应能对电池使用状况进行检测和管理:

a) 测试方法:

- 1) 通过产品查询应用程序耗电情况, 查看检测结果;
- 2) 设置自动或手动省电模式。

b) 预期结果:

- 1) 产品能够显示应用程序耗电情况;
- 2) 产品能进行自动或手动省电设置, 并提示省电数值。

7.6 备份与恢复

7.6.1 本地备份与恢复

产品应能进行本地备份和恢复:

a) 测试方法:

- 1) 使用产品将通讯录备份到文件, 删除通讯录内所有联系人后, 从备份文件中恢复通讯录;
- 2) 使用产品将信息备份到文件, 删除所有信息后, 从备份文件中恢复信息;
- 3) 使用产品将通话记录备份到文件, 删除所有的通话记录后, 从备份文件中恢复通话记录内容;
- 4) 使用产品将日历备份到文件, 删除所有的日历内容后, 从备份文件中恢复日历内容。

b) 预期结果:

- 1) 产品能成功备份和恢复通讯录内容;
- 2) 产品能成功备份和恢复信息内容;

- 3) 产品能成功备份和恢复通话记录;
- 4) 产品能成功备份和恢复日历内容。

7.6.2 网络备份与恢复

产品应能通过网络进行备份和恢复:

- a) 测试方法:
 - 1) 使用产品将通讯录和信息备份到远程服务器端,删除移动终端通讯录和信息中的所有内容后,从远程服务器端恢复通讯录和信息;
 - 2) 使用产品将通讯录和信息备份到远程服务器端,在使用不同系统平台的设备上恢复。
- b) 预期结果:
 - 1) 产品能完整备份和恢复通讯录和信息内容;
 - 2) 产品能完整备份,并在不同系统平台的设备上恢复通讯录和信息内容。

7.7 隐私保护

7.7.1 信息访问权限控制

产品应能对应用程序访问涉及用户个人隐私的行为进行检测:

- a) 测试方法:
 - 1) 启动测试应用程序,查看该应用程序能否访问用户位置信息;
 - 2) 启动测试应用程序,查看该应用程序能否访问通话记录;
 - 3) 启动测试应用程序,查看该应用程序能否访问短信彩信;
 - 4) 启动测试应用程序,查看该应用程序能否访问通讯录;
 - 5) 启动测试应用程序,查看该应用程序能否访问历史记录;
 - 6) 启动测试应用程序,查看该应用程序能否访问相册。
- b) 预期结果:产品能中断以上行为并提示报警。

7.7.2 应用程序使用权限控制

产品应能对用户使用应用程序的行为进行控制:

- a) 测试方法:在产品界面中设置用户对应用程序访问的权限;
- b) 预期结果:应用程序需要授权访问。

7.7.3 隐私空间设置

产品应能对数据进行隐私设置:

- a) 测试方法:在产品界面中设置隐私空间及相应授权,并将数据添加进隐私空间;
- b) 预期结果:访问隐私空间需要授权访问,未授权无法访问隐私空间。

7.8 流量监控

产品应能对网络流量进行监控:

- a) 测试方法:
 - 1) 查看产品的流量监控功能;
 - 2) 在产品中设定流量套餐,并校正当前已用流量到阈值;
 - 3) 禁止某项应用程序使用网络连接。
- b) 预期结果:

- 1) 产品能显示当前剩余流量、周期使用流量统计、各应用程序使用流量统计；
- 2) 当用户的流量使用到达阈值时进行提示；
- 3) 被禁止的应用程序无法进行网络连接。

7.9 通信拦截

产品应能对通信进行拦截：

- a) 测试方法：
 - 1) 向被测设备发送垃圾短信；
 - 2) 向被测设备拨打恶意来电；
 - 3) 将指定号码添加到黑名单和白名单中。
- b) 预期结果：
 - 1) 产品能拦截垃圾短信；
 - 2) 产品能拦截恶意来电；
 - 3) 产品能按照黑白名单策略进行通讯。

7.10 防盗保护

7.10.1 设备锁定

产品应能锁定移动终端：

- a) 测试方法：激活产品的防盗功能，检测终端锁定情况；
- b) 预期结果：移动终端无法正常使用。

7.10.2 回传被盗设备信息

产品应能回传被盗设备信息：

- a) 测试方法：
 - 1) 通过使用安全号码的移动终端查询被盗设备位置信息；
 - 2) 通过使用安全号码的移动终端查询被盗设备通话记录；
 - 3) 通过使用安全号码的移动终端查询被盗设备当前号码；
 - 4) 通过使用安全号码的移动终端查询被盗设备在锁定时拍摄的照片。
- b) 预期结果：
 - 1) 在使用安全号码的移动终端上能收到被盗设备的位置信息；
 - 2) 在使用安全号码的移动终端上能收到被盗设备的通话记录；
 - 3) 在使用安全号码的移动终端上能收到被盗设备的当前号码；
 - 4) 在使用安全号码的移动终端上能收到被盗设备在锁定时拍摄的照片。

7.10.3 远程数据擦除

产品应能远程擦除指定信息：

- a) 测试方法：通过使用安全号码的移动终端发送指令，擦除被盗设备上的指定数据；
- b) 预期结果：被盗设备上的指定数据全部被删除。

7.11 产品更新

产品应能进行更新：

- a) 测试方法：

- 1) 在产品界面中执行病毒库更新，检查病毒库版本号；
 - 2) 在产品界面中执行程序文件更新，检查程序版本号；
 - 3) 分别使用全量升级和增量升级的方式进行更新。
- b) 预期结果：
- 1) 确认病毒库已经更新到最新版本；
 - 2) 确认程序已经更新到最新版本；
 - 3) 增量升级减少了数据量，提高了更新速度。

7.12 兼容性

产品应具有良好的兼容性：

- a) 测试方法：
- 1) 使用不同型号，不同屏幕分辨率的移动终端安装被测产品；
 - 2) 使用不同系统版本的移动终端安装被测产品。
- b) 预期结果：
- 1) 产品能正常安装，各项功能正常使用；
 - 2) 产品能正常安装，各项功能正常使用。

7.13 自身安全

产品应具有良好的自身安全性：

- a) 测试方法：
- 1) 设置产品开机自动启动，重新启动移动终端；
 - 2) 使用第三方任务管理器，终止被测产品的程序进程；
 - 3) 使用第三方任务管理器卸载被测产品。
- b) 预期结果：
- 1) 产品能在系统启动时自动加载；
 - 2) 被测产品的程序进程不能被中止；
 - 3) 被测产品卸载失败。

8 报告格式

产品检验结果及评分表格式见表1。

表1 产品检验结果及评分表

序号	检测项目		检验结果	分数	备注
1	产品安装卸载 (2分)	产品正常安装和完全卸载		2	
2	病毒防护与处置 (20分)	病毒防护途径	网络		3
3			外部设备		3
4		病毒检测能力			3
5		病毒清除能力			3
6		误报率			1

7		备份功能		1	
8		恶意URL拦截		2	
9		配置功能	自定义扫描路径	2	
10			计划扫描	2	
11	系统检测与优化 (18分)	系统状态检测	应用程序安装情况	2	
12			内存使用情况	2	
13			自启动应用	2	
14			垃圾文件	2	
15			磁盘剩余空间	2	
16		系统优化	释放系统内存	2	
17			自启动项设置	2	
18			垃圾文件清除	2	
19		电源管理	耗电查询	1	
20			省电模式设置	1	
21	备份与恢复 (10分)	本地备份与恢复	通讯录	2	
22			信息	2	
23			通话记录	2	
24			日历	1	
25		网络备份与恢复	同系统平台	2	
26			跨系统平台	1	
27	隐私保护 (16分)	信息访问权限控制	位置信息	2	
28			通话记录	2	
29			短信彩信	2	
30			通讯录	2	
31			历史记录	2	
32			相册	2	
33		应用程序使用权限控制	2		
34	隐私空间设置	2			
35	流量监控 (9分)	流量实时监控统计	2		
36		流量周期监控统计	1		
37		应用程序流量监控统计	2		
38		流量套餐设置与超额提示	2		
39		应用程序联网控制	2		
40	通信拦截 (9分)	垃圾信息拦截	3		
41		恶意来电拦截	3		
42		黑白名单拦截	3		
43	防盗保护 (8分)	设备锁定		2	
44		回传被盗设备信息	位置信息	1	
45			通话记录	1	
46			被盗设备当前号码	1	
47			摄像头拍照信息	1	

48		远程数据擦除		2	
49	产品更新 (3分)	病毒库更新		1	
50		程序更新		1	
51		增量、全量更新		1	
52	兼容性 (2分)	支持主流机型		1	
53		支持主流系统版本		1	
54	自身安全 (3分)	开机自动启动		1	
55		防止异常终止进程		1	
56		防止异常卸载		1	

9 评级方法

本项要求包括：

- a) 按表 1 规定的检验项目对受检产品进行评分；
- b) 受检产品未满足检验项目要求,则该项分值为零, 满足检验项目要求,则该项分值按表 1 计算；
- c) 按受检产品所得总分数确定产品的级别, 级别划分见表 2。

表2 产品检验结果及评分表级别划分

序号	分值	级别
1	71-80分	一级
2	81-90分	二级
3	90分以上	三级