ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1142—2014

信息安全技术
主机安全检查产品安全技术要求

Information security technology—
Security technical requirements for host security inspecting products

2014-03-14 发布　　2014-03-14 实施

中华人民共和国公安部　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：公安部计算机信息系统安全产品质量监督检验中心、公安部网络安全保卫局、蓝盾信息安全技术股份有限公司、公安部第三研究所。

本标准主要起草人：赵云、顾健、张俊兵、张奕、邱梓华、沈亮、张笑笑、宋好好、陆臻、俞优、陈彬。

引　言

本标准详细描述了与主机安全检查产品安全环境相关的假设、威胁和组织安全策略，定义了主机安全检查产品及其支撑环境的安全目的，通过基本原理论证安全功能要求能够追溯并覆盖产品安全目的，安全目的能够追溯并覆盖安全环境相关的假设、威胁和组织安全策略。

本标准基本级参照了GB/T 18336.3—2008中规定的EAL2级安全保证要求，增强级在EAL4级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

本标准仅给出了主机安全检查检查应满足的安全技术要求，但对主机安全检查产品的具体技术实现方式、方法等不做要求。

信息安全技术
主机安全检查产品安全技术要求

1 范围

本标准规定了主机安全检查产品的安全功能要求、安全保证要求及等级划分要求。

本标准适用于对主机安全检查产品的设计、开发及检测。

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。

GB 17859—1999 计算机信息系统 安全保护等级划分准则

GB/T 18336—2008(所有部分) 信息技术 安全技术 信息技术安全性评估准则

GB/T 25069—2010 信息安全技术 术语

3 术语和定义

GB 17859—1999、GB/T 18336—2008(所有部分)和GB/T 25069—2010界定的以及下列术语和定义适用于本文件。

3.1

代理 agent

安装在被检查的主机上，用于收集主机各项配置信息的组件。

3.2

管理控制台 management console

用于对收集到的配置信息进行集中存储和分析，并进行引擎管理、安全检查策略配置、报警管理、事件响应以及其他管理工作的组件。一个控制台可以管理多个引擎。

3.3

检查 inspect

通过引擎对主机的安全配置进行收集和分析，并在控制台集中显示的过程。

4 主机安全检查产品描述

产品由代理和管理控制台组成，根据预先定义的安全策略模版，通过管理控制台对安装了代理的主机进行安全性检查，代理收集数据，管理控制台分析数据并生成报告。达到发现其安全配置方面存在的问题的目的，此外主机安全检查产品本身及其内部的重要数据也是受保护的资产。

检查的项目常见的包括几个方面：配置检查，系统资源(CPU、内存、硬盘)，杀毒软件、进程、服务，系统共享资源，启动项，外围接口设备，系统账户，软件安装，硬件配置，网络连接，系统漏洞。

主机安全检查产品以C/S方式部署或者单机方式部署，并执行安全功能。其安全检查的目标是安装了引擎的主机。

图 1 是主机安全检查产品的一个典型 C/S 方式部署运行环境。

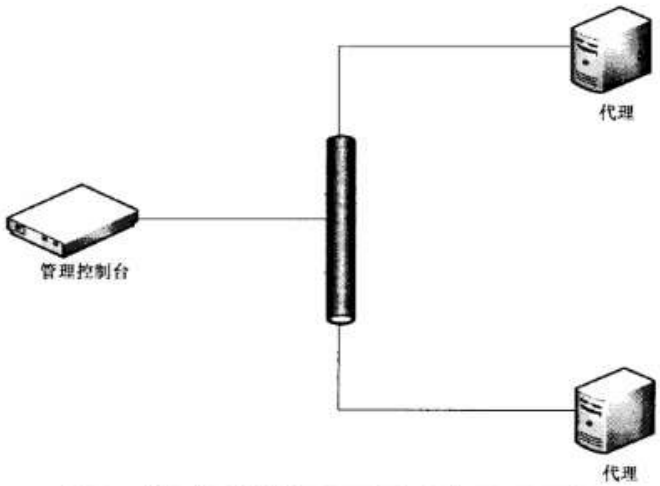

图 1 主机安全检查产品 C/S 方式部署运行环境

5 安全环境

5.1 假设

主机安全检查产品安全环境相关的假设如表 1 所示。

表 1 假设

假设名称	假设描述
物理访问	产品的处理资源应限定在受控的访问设备内，以防止未授权的物理访问。所有实施产品安全策略相关的硬件和软件都应受到保护，以免受非授权的物理更改
人员能力	授权管理员是无恶意的，训练有素的，并遵循管理员指南
连接性	产品的代理和管理控制台之间的网络是连通的，两者之间可以正常通讯
安全维护	当产品的应用环境发生变化时，应立即反映在产品的安全策略中并保持其安全功能有效

5.2 威胁

主机安全检查安全环境相关的威胁如表 2 所示。

表 2 威胁

威胁名称	威胁描述
配置不当	主机可能存在未被发现的安全配置方面的问题
失效	产品运行错误可能导致系统失去响应
非授权访问	恶意用户可能试图访问和使用产品提供的安全功能
暴力认证	恶意用户可能通过反复猜测鉴别数据的方法，从而获取管理员权限
信息泄漏	恶意用户可能浏览远程授权管理员和产品之间发送的安全相关信息

5.3 组织安全策略

主机安全检查安全环境相关的组织安全策略如表3所示。

表3 组织安全策略

组织安全策略名称	组织安全策略描述
审计	为追踪所有与安全相关活动的责任，与安全相关的事件应记录、保存和审查
安全管理	产品应为授权管理员提供管理手段，使其以安全的方式进行管理

6 安全目的

6.1 产品安全目的

表4定义了产品的安全目的。这些安全目的旨在对应已标识的威胁或组织安全策略。

表4 产品安全目的

产品安全目的名称	产品安全目的描述	对应的威胁或组织安全策略
主机安全检查	根据预先定义的安全策略模版，通过控制台对安装了引擎的主机进行安全性检查，发现其安全配置方面存在的问题	配置不当
稳定容错	产品应稳定运行，并具有一定容错性	失效
身份认证	在允许用户访问产品功能之前，产品应对用户身份进行唯一的标识和鉴别	非授权访问
鉴别失败处理	产品应具备安全机制防止恶意用户反复猜测鉴别数据	暴力认证
信息保密	如果产品允许通过相连网络对其进行远程管理，那么它应保证远程管理信息的保密性	信息泄漏
审计	产品应记录自身安全相关的事件，以便追踪安全相关行为的责任，并应提供方法审查所记录的数据	审计
安全管理	产品应向授权管理员提供以安全方式进行管理的有效手段	安全管理

6.2 环境安全目的

表5定义了非技术或程序方法进行处理的安全目的。5.1确定的假设被包含在环境安全目的中。

表5 环境安全目的

环境安全目的名称	环境安全目的描述	对应的假设或威胁
物理访问	产品的处理资源应限定在受控的访问设备内，以防止未授权的物理访问。所有实施产品安全策略相关的硬件和软件应受到保护，以免受非授权的物理更改	物理访问
人员能力	管理员是无恶意的，训练有素的，并遵循管理员指南	人员能力
连接性	主机安全检查产品应能够采集安装引擎主机的安全配置	连接性
安全维护	当产品的应用环境发生变化时，应立即反应在产品的安全策略中并保持其安全功能有效	安全维护

7 安全功能要求

7.1 策略制定

产品应能定制安全检查策略的检查项及响应处理方式，并提供方便的定制策略的方法，如：

a) 提供默认的安全检查策略模板，用户能够根据此策略模板进行主机安全检查；
b) 支持自定义安全检查策略模板；
c) 支持安全检查策略模板的导入、导出功能；
d) 提供安全检查策略定制向导功能；
e) 支持按计划任务执行安全检查策略。

7.2 检查功能

7.2.1 操作系统检查

产品应能对主机操作系统版本、补丁安装情况进行检查。

7.2.2 系统资源检查

产品应能对主机的 CPU、内存、硬盘、网络等系统资源当前使用情况进行检查。

7.2.3 杀毒软件检查

应能检查主机杀毒软件的使用状况，包括安装情况、运行状态和病毒库版本。

7.2.4 进程、服务检查

产品应能对主机进程、服务进行检查，包括：

a) 服务列表，包括服务的运行状态(如启动，停止等)；
b) 运行的进程；
c) 指定服务、进程的状态变化。

7.2.5 系统共享资源检查

产品应能检查主机上设置为共享的文件夹，包括：

a) 当前共享文件夹列表；
b) 共享文件夹的变化。

7.2.6 启动项检查

产品应能检查主机的启动项。

7.2.7 外围接口设备使用检查

产品应能检查主机串口、USB 口、软驱、光驱等外围接口设备的使用情况。

7.2.8 操作系统账户检查

产品应能对系统账户进行检查，包括：

a) 默认账户是否重命名；
b) guest 账户是否禁用；

c) 账户锁定策略是否设置；
d) 口令复杂度策略是否设置。

7.2.9 软件安装检查

产品应能对主机安装的软件情况进行检查。

7.2.10 硬件配置检查

产品应能对主机硬件配置情况进行检查。

7.2.11 网络连接检查

产品应能对主机的网络连接情况进行检查(如网卡、Wifi、蓝牙等)。

7.2.12 操作系统漏洞检查

产品应能对主机的系统漏洞进行检查。

7.3 基线功能

产品应提供基线功能，具有包括：

a) 对主机的各种配置信息进行收集，并记录为主机的基线值(即主机当前的状态信息快照)，包括：主机的硬件信息，软件安装情况、服务运行状态、共享文件夹和外围接口使用情况等信息；
b) 定时对主机的各项配置进行检查，与基线值进行比较，查看是否发生变化；
c) 基线变化检查的时间间隔和基线值的内容可由授权管理员设置。

7.4 响应功能

7.4.1 报警事件

产品应能针对下列事件发送报警信息：

a) 硬盘空闲空间小于管理员设置的监测阀值；
b) CPU、内存占用率超过管理员设置的监测阀值；
c) 操作系统共享文件夹发生变化；
d) 系统存在高危风险漏洞。

7.4.2 报警方式

产品应能通过一定的方式进行报警(如弹出窗口、短信、电子邮件等)。

7.4.3 其他响应措施

产品应能对指定事件进行响应，响应方式至少包括以下的一种：

a) 软件清理；
b) 漏洞修复；
c) 除以上之外的其他措施。

7.5 检查结果分析

7.5.1 结果导入导出

产品应能对检查结果进行导入、导出。

7.5.2 结果报告

产品应能对检查结果进行分析并形成报告，报告包含下列内容：

a) 主机的检查结果；

b) 对主机检查结果的统计；

c) 根据检查的信息，对主机存在的风险进行分析的结果。

7.5.3 定制报告

报告应能根据用户要求进行定制。

7.6 稳定性和容错性

产品稳定性和容错性要求如下：

a) 主界面不应失去响应或非正常退出；

b) 进度不应停滞不前；

c) 检查任务应可随时停止。

7.7 集中管理

应提供对多台安装了引擎的主机进行集中管理的能力，能提供主机监测策略的统一定制，并可以分发到相应主机上。

7.8 标识与鉴别

7.8.1 用户标识

7.8.1.1 属性定义

产品应为每个管理角色规定与之相关的安全属性，例如管理角色标识、鉴别信息、隶属组、权限等。

7.8.1.2 属性初始化

产品应提供使用默认值对创建的每个管理角色的属性进行初始化的能力。

7.8.1.3 唯一性标识

产品应为用户提供唯一标识。同时将用户的身份标识与该用户的所有可审计能力相关联。

7.8.2 身份鉴别

7.8.2.1 基本鉴别

产品应在执行任何与管理员相关功能之前鉴别用户的身份。

7.8.2.2 鉴别数据保护

产品应保证鉴别数据不被未授权查阅或修改。

7.8.2.3 鉴别失败处理

当对用户鉴别失败的次数达到指定次数后，产品应能终止用户的访问。

7.8.2.4 超时锁定或注销

产品应具有登录超时锁定或注销功能。在设定的时间段内没有任何操作的情况下，终止会话，需要再次进行身份鉴别才能够重新操作。最大超时时间仅由授权管理员设定。

7.9 安全管理

7.9.1 安全功能管理

产品应允许授权管理员对产品进行以下管理：

a) 查看安全属性；
b) 修改安全属性；
c) 启动、关闭全部或部分安全功能；
d) 制定和修改各种安全策略。

7.9.2 安全角色管理

产品应能对管理员角色进行区分：

a) 具有至少两种不同权限的管理员角色，例如操作员、安全员、审计员等；
b) 根据不同的功能模块，自定义各种不同权限角色，并可对管理员分配角色。

7.9.3 可信管理主机

若控制台提供远程管理功能，产品应能对可远程管理的主机地址进行限制。

7.9.4 数据传输安全

产品的各组件间通过网络进行数据传输时，应对通信数据采取保密传输；若控制台提供远程管理功能，应采取保密措施防止其被未授权截取。

7.10 审计

7.10.1 审计事件

产品应能记录以下事件：

a) 管理员鉴别成功和失败；
b) 安全检查策略的制定和修改；
c) 产品的启动和关闭。

记录内容应包括：事件发生的日期和时间、主体、客体、事件描述和事件结果。

7.10.2 审计跟踪管理

管理员应能存储、删除和清空审计记录。

7.10.3 可理解的格式

审计记录的内容应能为人所理解。

7.11 升级功能

产品应提供以下升级能力：

a) 支持策略库、服务程序的更新；
b) 至少采取一种安全机制，保证升级的时效性，例如自动升级，更新通知等手段。

8 安全保证要求

8.1 配置管理

8.1.1 部分配置管理自动化

配置管理系统应提供一种自动方式来支持产品的生成，通过该方式确保只能对产品的实现表示进行已授权的改变。

配置管理计划应描述在配置管理系统中所使用的自动工具，并描述在配置管理系统中如何使用自动工具。

8.1.2 配置管理能力

8.1.2.1 版本号

开发者应为产品的不同版本提供唯一的标识。

8.1.2.2 配置项

开发者应使用配置管理系统并提供配置管理文档。

配置管理文档应包括一个配置清单，配置清单应唯一标识组成产品的所有配置项并对配置项进行描述，还应描述对配置项给出唯一标识的方法，并提供所有的配置项得到有效维护的证据。

8.1.2.3 授权控制

开发者提供的配置管理文档应包括一个配置管理计划，配置管理计划应描述如何使用配置管理系统。实施的配置管理应与配置管理计划相一致。

开发者应提供所有的配置项得到有效地维护的证据，并应保证只有经过授权才能修改配置项。

8.1.2.4 产生支持和接受程序

开发者提供的配置管理文档应包括一个接受计划，接受计划应描述用来接受修改过的或新建的作为产品组成部分的配置项的程序。

配置管理系统应支持产品的生成。

8.1.3 配置管理范围

8.1.3.1 配置管理覆盖

配置管理范围至少应包括产品实现表示、设计文档、测试文档、指导性文档、配置管理文档，从而确保它们的修改是在一个正确授权的可控方式下进行的。

配置管理文档至少应能跟踪上述内容，并描述配置管理系统是如何跟踪这些配置项的。

8.1.3.2 问题跟踪配置管理覆盖

配置管理范围应包括安全缺陷，确保安全缺陷置于配置管理系统之下。

8.2 交付与运行

8.2.1 交付程序

开发者应使用一定的交付程序交付产品，并将交付过程文档化。

交付文档应描述在给用户方交付产品的各版本时，为维护安全所必需的所有程序。

8.2.2 修改检测

交付文档应描述如何提供多种程序和技术上的措施来检测修改，或检测开发者的主拷贝和用户方所收到版本之间的任何差异。还应描述如何使用多种程序来发现试图伪装成开发者，甚至是在开发者没有向用户方发送任何东西的情况下，向用户方交付产品。

8.2.3 安装、生成和启动程序

开发者应提供文档说明产品的安装、生成和启动的过程。

8.3 开发

8.3.1 功能规范

8.3.1.1 非形式化功能规范

开发者应提供一个功能规范，功能规范应满足以下要求：

a) 使用非形式化风格来描述产品安全功能及其外部接口；
b) 是内在一致的；
c) 描述所有外部接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节；
d) 完备地表示产品安全功能。

8.3.1.2 充分定义的外部接口

功能规范应包括安全功能是完备地表示的合理性。

8.3.2 高层设计

8.3.2.1 描述性高层设计

开发者应提供产品安全功能的高层设计，高层设计应满足以下要求：

a) 表示是非形式化的；
b) 是内在一致的；
c) 按子系统描述安全功能的结构；
d) 描述每个安全功能子系统所提供的安全功能性；
e) 标识安全功能所要求的任何基础性的硬件、固件或软件，以及在这些硬件、固件或软件中实现的支持性保护机制所提供功能的一个表示；
f) 标识安全功能子系统的所有接口；
g) 标识安全功能子系统的哪些接口是外部可见的。

8.3.2.2 安全加强的高层设计

开发者提供的安全加强的高层设计应满足以下要求：

a) 描述产品的功能子系统所有接口的用途与使用方法，适当时提供效果、例外情况和错误消息的细节；
b) 把产品分成安全策略实施和其他子系统来描述。

8.3.3 安全功能实现的子集

实现表示应当无歧义而且详细地定义安全功能，使得无须进一步设计就能生成安全功能。实现表示应是内在一致的。

8.3.4 描述性低层设计

开发者应提供产品安全功能的低层设计，低层设计应满足以下要求：

a) 表示是非形式化的；
b) 是内在一致的；
c) 按模块描述安全功能；
d) 描述每个模块的用途；
e) 根据所提供的安全功能性和对其他模块的依赖关系两方面来定义模块间的相互关系；
f) 描述每个安全策略实施功能是如何被提供的；
g) 标识安全功能模块的所有接口；
h) 标识安全功能模块的哪些接口是外部可见的；
i) 描述安全功能模块所有接口的用途和用法，适当时提供效果、例外情况和错误消息的细节；
j) 把产品分为安全策略实施模块和其他模块来描述。

8.3.5 非形式化对应性证实

开发者应提供产品安全功能表示的所有相邻对之间提供对应性分析。

对于产品安全功能所表示的每个相邻对，分析应阐明，较为抽象的安全功能表示的所有相关安全功能，应在较具体的安全功能表示中得到正确且完备的细化。

8.3.6 非形式化产品安全策略模型

开发者应提供安全策略模型，安全策略模型应满足以下要求：

a) 表示是非形式化的；
b) 描述所有能被模型化的安全策略的规则与特征；
c) 包含合理性，即论证该模型相对所有能被模型化的安全策略来说是一致的，而且是完备的；
d) 阐明安全策略模型和功能规范之间的对应性，即论证所有功能规范中的安全功能对于安全策略模型来说是一致的，而且是完备的。

8.4 指导性文档

8.4.1 管理员指南

开发者应提供管理员指南，管理员指南应与为评估而提供的其他所有文档保持一致。

管理员指南应说明以下内容：

a) 管理员可使用的管理功能和接口；
b) 怎样安全地管理产品；
c) 在安全处理环境中应被控制的功能和权限；
d) 所有对与产品的安全操作有关的用户行为的假设；
e) 所有受管理员控制的安全参数，如果可能，应指明安全值；
f) 每一种与管理功能有关的安全相关事件，包括对安全功能所控制实体的安全特性进行的改变；
g) 所有与管理员有关的 IT 环境安全要求。

8.4.2 用户指南

开发者应提供用户指南，用户指南应与为评估而提供的其他所有文档保持一致。

用户指南应说明以下内容：

a) 产品的非管理员用户可使用的安全功能和接口；
b) 产品提供给用户的安全功能和接口的使用方法；
c) 用户可获取但应受安全处理环境所控制的所有功能和权限；
d) 产品安全操作中用户所应承担的职责；
e) 与用户有关的 IT 环境的所有安全要求。

8.5 生命周期支持

8.5.1 安全措施标识

开发者应提供开发安全文档。

开发安全文档应描述在产品的开发环境中，为保护产品设计和实现的保密性和完整性所必需的所有物理的、程序的、人员的和其他方面的安全措施，并应提供在产品的开发和维护过程中执行安全措施的证据。

8.5.2 开发者定义的生命周期模型

开发者应建立一个生命周期模型对产品的开发和维护进行的必要控制，并提供生命周期定义文档描述用于开发和维护产品的模型。

8.5.3 明确定义的开发工具

开发者应明确定义用于开发产品的工具，并提供开发工具文档无歧义地定义实现中每个语句的含义和所有依赖于实现的选项的含义。

8.6 测试

8.6.1 测试覆盖

8.6.1.1 覆盖证据

开发者应提供测试覆盖的证据。

在测试覆盖证据中，应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能是对应的。

8.6.1.2 覆盖分析

开发者应提供测试覆盖的分析结果。

测试覆盖的分析结果应表明测试文档中所标识的测试与功能规范中所描述的产品的安全功能之间的对应性是完备的。

8.6.2 测试：高层设计

开发者应提供测试深度的分析。

深度分析应证实测试文档中所标识的测试足以证实该产品的功能是依照其高层设计运行的。

8.6.3 功能测试

开发者应测试安全功能，将结果文档化并提供测试文档。

测试文档应包括以下内容：

a) 测试计划，应标识要测试的安全功能，并描述测试的目标；

b) 测试过程，应标识要执行的测试，并描述每个安全功能的测试概况，这些概况应包括对于其他测试结果的顺序依赖性；
c) 预期的测试，结果应表明测试成功后的预期输出；
d) 实际测试结果，应表明每个被测试的安全功能能按照规定进行运作。

8.6.4 独立测试

8.6.4.1 一致性

开发者应提供适合测试的产品，提供的测试集合应与其自测产品功能时使用的测试集合相一致。

8.6.4.2 抽样

开发者应提供一组相当的资源，用于安全功能的抽样测试。

8.7 脆弱性评定

8.7.1 误用

8.7.1.1 指南审查

开发者应提供指导性文档，指导性文档应满足以下要求：
a) 标识所有可能的产品运行模式(包括失败或操作失误后的运行)、它们的后果以及对于保持安全运行的意义；
b) 是完备的、清晰的、一致的、合理的；
c) 列出关于预期使用环境的所有假设；
d) 列出对外部安全措施(包括外部程序的、物理的或人员的控制)的所有要求。

8.7.1.2 分析确认

开发者应提供分析文档论证指导性文档是完备的。

8.7.2 产品安全功能强度评估

开发者应对指导性文档中所标识的每个具有安全功能强度声明的安全机制进行安全功能强度分析，并说明安全机制达到或超过定义的最低强度级别或特定功能强度度量。

8.7.3 脆弱性分析

8.7.3.1 开发者脆弱性分析

开发者应执行脆弱性分析，并提供脆弱性分析文档。

开发者应从用户可能破坏安全策略的明显途径出发，对产品的各种功能进行分析并提供文档。对被确定的脆弱性，开发者应明确记录采取的措施。

对每一条脆弱性，应有证据显示在使用产品的环境中，该脆弱性不能被利用。

8.7.3.2 独立的脆弱性分析

开发者应提供文档证明经过标识脆弱性的产品可以抵御明显的穿透性攻击。

8.7.3.3 中级抵抗力

开发者应提供文档证明产品可以抵御中级强度的穿透性攻击，并提供证据说明对脆弱性的搜索是系统化的。

9 技术要求基本原理

9.1 安全功能要求基本原理

表6说明了安全功能要求的充分必要性的基本原理，即每个产品安全目的都至少有一个安全功能要求与其对应，每个安全功能要求都至少解决了一个产品安全目的，因此安全功能要求是充分和必要的。表6中的“√”即表明对应关系。

表6 安全功能要求基本原理

项目	主机安全检查	稳定容错	身份认证	鉴别失败处理	信息保密	审计	安全管理
操作系统检查	√						
系统资源检查	√						
杀毒软件检查	√						
进程、服务检查	√						
系统共享资源检查	√						
启动项检查	√						
外围接口设备使用检查	√						
操作系统账户检查	√						
软件安装检查	√						
硬件配置检查	√						
网络连接检查	√						
操作系统漏洞检查	√						
基线功能							√
报警事件							√
报警方式							√
其他响应措施							√
结果导入导出							√
结果报告							√
定制报告							√
稳定性和容错性		√					
集中管理							
属性定义			√				
属性初始化			√				
唯一性标识			√				√
基本鉴别			√				√
鉴别数据保护			√		√		
鉴别失败处理				√			
超时锁定或注销			√				
安全功能管理	√						√
安全角色管理	√						√

表 6（续）

项目	主机安全检查	稳定容错	身份认证	鉴别失败处理	信息保密	审计	安全管理
可信管理主机			√				√
数据传输安全					√		
审计事件						√	
审计跟踪管理						√	
可理解的格式						√	
升级功能	√						

9.2 安全保证要求基本原理

安全保证要求参照了 GB/T 18336.3—2008 中的相关要求。

10 等级划分要求

10.1 概述

按照主机安全检查的安全功能要求强度，将主机安全检查安全功能要求划分成基本级和增强级；安全保证要求基本级参照了 EAL2 级安全保证要求，增强级在 EAL4 级安全保证要求的基础上，将脆弱性分析要求提升到可以抵御中等攻击潜力的攻击者发起的攻击。

10.2 安全功能要求等级划分

主机安全检查产品的安全功能要求等级划分如表 7 所示。

表 7 主机安全检查产品安全功能要求等级划分表

安全功能要求		基本级	增强级
策略制定		7.1 a)、b)	7.1
检查功能	操作系统检查	7.2.1	7.2.1
	系统资源检查	7.2.2	7.2.2
	杀毒软件检查	—	7.2.3
	进程、服务检查	7.2.4 a)、b)	7.2.4
	系统共享资源检查	7.2.5 a)	7.2.5
	启动项检查	—	7.2.6
	外围接口设备使用检查	7.2.7	7.2.7
	操作系统账户检查	—	7.2.8
	软件安装检查	7.2.9	7.2.9
	硬件配置检查	7.2.10	7.2.10
	网络连接检查	7.2.11	7.2.11
	操作系统漏洞检查	—	7.2.12
基线功能		7.3	7.3

表 7（续）

安全功能要求			基本级	增强级
响应功能	报警事件		7.4.1 a)、b)	7.4.1
	报警方式		7.4.2	7.4.2
	其他响应措施		—	7.4.3
检查结果分析	结果导入导出		7.5.1	7.5.1
	结果报告		7.5.2 a)、b)	7.5.2
	定制报告		—	7.5.3
稳定性和容错性			7.6	7.6
集中管理			7.7	7.7
标识与鉴别	用户标识	属性定义	7.8.1.1	7.8.1.1
		属性初始化	7.8.1.2	7.8.1.2
		唯一性标识	7.8.1.3	7.8.1.3
	身份鉴别	基本鉴别	7.8.2.1	7.8.2.1
		鉴别数据保护	7.8.2.2	7.8.2.2
		鉴别失败处理	—	7.8.2.3
		超时锁定或注销	—	7.8.2.4
安全管理	安全功能管理		7.9.1	7.9.1
	安全角色管理		—	7.9.2
	可信管理主机		—	7.9.3
	数据传输安全		—	7.9.4
审计	审计事件		7.10.1 a)	7.10.1
	审计跟踪管理		7.10.2	7.10.2
	可理解的格式		7.10.3	7.10.3
升级功能			—	7.11

10.3 安全保证要求等级划分

主机安全检查产品的安全保证要求等级划分如表 8 所示。

表 8 主机安全检查产品安全保证要求等级划分表

安全保证要求			基本级	增强级
配置管理	部分配置管理自动化		—	8.1.1
	配置管理能力	版本号	8.1.2.1	8.1.2.1
		配置项	8.1.2.2	8.1.2.2
		授权控制	—	8.1.2.3
		产生支持和接受程序	—	8.1.2.4
	配置管理范围	配置管理覆盖	—	8.1.3.1
		问题跟踪配置管理覆盖	—	8.1.3.2

表 8（续）

安全保证要求			基本级	增强级
交付与运行	交付程序		8.2.1	8.2.1
	修改检测		—	8.2.2
	安装、生成和启动程序		8.2.3	8.2.3
开发	功能规范	非形式化功能规范	8.3.1.1	8.3.1.1
		充分定义的外部接口	—	8.3.1.2
	高层设计	描述性高层设计	8.3.2.1	8.3.2.1
		安全加强的高层设计	—	8.3.2.2
	安全功能实现的子集		—	8.3.3
	描述性低层设计		—	8.3.4
	非形式化对应性证实		8.3.5	8.3.5
	非形式化产品安全策略模型		—	8.3.6
指导性文档	管理员指南		8.4.1	8.4.1
	用户指南		8.4.2	8.4.2
生命周期支持	安全措施标识		—	8.5.1
	开发者定义的生命周期模型		—	8.5.2
	明确定义的开发工具		—	8.5.3
测试	测试覆盖	覆盖证据	8.6.1.1	8.6.1.1
		覆盖分析	—	8.6.1.2
	测试：高层设计		—	8.6.2
	功能测试		8.6.3	8.6.3
	独立测试	一致性	8.6.4.1	8.6.4.1
		抽样	8.6.4.2	8.6.4.2
脆弱性评定	误用	指南审查	—	8.7.1.1
		分析确认	—	8.7.1.2
	产品安全功能强度评估		8.7.2	8.7.2
	脆弱性分析	开发者脆弱性分析	8.7.3.1	8.7.3.1
		独立的脆弱性分析	—	8.7.3.2
		中级抵抗力	—	8.7.3.3

中华人民共和国公共安全
行 业 标 准
信息安全技术
主机安全检查产品安全技术要求
GA/T 1142—2014

*

中国标准出版社出版发行
北京市朝阳区和平里西街甲2号(100029)
北京市西城区三里河北街16号(100045)

网址 www.spc.net.cn
总编室:(010)64275323 发行中心:(010)51780235
读者服务部:(010)68523946

中国标准出版社秦皇岛印刷厂印刷
各地新华书店经销

*

开本 880×1230 1/16 印张 1.5 字数 34 千字
2014年6月第一版 2014年6月第一次印刷

*

书号:155066·2-27073 定价 24.00 元

GA/T 1142-2014

打印日期:2014年6月20日 F009A