ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1138—2014

信息安全技术
主机资源访问控制产品安全技术要求

Information security technology—
Security technical requirements for access control products of host resources

2014-03-10 发布　　2014-03-10 实施

中华人民共和国公安部　　发 布

目　　次

前言 …… Ⅲ
引言 …… Ⅳ
1　范围 …… 1
2　规范性引用文件 …… 1
3　术语和定义 …… 1
4　主机资源访问控制产品描述 …… 1
5　安全环境 …… 2
5.1　假设 …… 2
5.2　威胁 …… 2
5.3　组织安全策略 …… 3
6　安全目的 …… 3
6.1　产品安全目的 …… 3
6.2　环境安全目的 …… 4
7　安全功能要求 …… 4
7.1　访问控制所覆盖的主机资源 …… 4
7.2　主机资源管理 …… 4
7.3　访问控制策略 …… 4
7.4　访问控制 …… 4
7.5　访问限制能力 …… 5
7.6　访问控制策略下发 …… 5
7.7　访问控制策略不可旁路 …… 5
7.8　用户认证管理 …… 5
7.9　安全管理 …… 6
7.10　自身保护功能 …… 6
7.11　远程传输安全 …… 7
7.12　审计功能 …… 7
8　安全保证要求 …… 7
8.1　配置管理 …… 7
8.2　交付与运行 …… 8
8.3　开发 …… 8
8.4　指导性文档 …… 10
8.5　生命周期支持 …… 10
8.6　测试 …… 11
8.7　脆弱性评定 …… 12
9　技术要求基本原理 …… 12
9.1　安全功能要求基本原理 …… 12

9.2 安全保证要求基本原理 …… 14
10 等级划分要求 …… 14
10.1 概述 …… 14
10.2 安全功能要求等级划分 …… 14
10.3 安全保证要求等级划分 …… 15

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

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

本标准由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、浙江万赛软件科技有限公司、公安部第三研究所。

本标准主要起草人：宋好好、沈亮、俞优、胡维娜、顾健、顾玮、张笑笑、赵永亮。

引　言

本标准详细描述了与主机资源访问控制产品安全环境相关的假设、威胁和组织安全策略，定义了主机资源访问控制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资源访问控制产品应满足的安全技术要求，但对主机资源访问控制产品的具体技术实现方式、方法等不做要求。

信息安全技术
主机资源访问控制产品安全技术要求

1 范围

本标准规定了主机资源访问控制产品的安全功能要求、安全保证要求及等级划分要求。

本标准适用于主机资源访问控制产品的设计、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 界定的术语和定义适用于本文件。

4 主机资源访问控制产品描述

主机资源访问控制产品针对受控主机，统一分配用户的登录权限和对主机资源的访问权限，从而保证用户根据预先定义的访问控制策略对受控主机的资源(包括系统登录权限、文件和文件夹、外设接口、应用程序、进程等)进行访问，以此来保护主机资源不被未授权访问和使用。

主机资源访问控制产品一般由服务器、客户端和管理控制台三部分组成，由服务器下发访问控制策略到客户端。其保护的资产是主机资源，此外主机资源访问控制产品本身及其内部的重要数据也是受保护的资产。

图 1 是主机资源访问控制产品的一个典型运行环境。