ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 403.2—2014
代替 GA/T 403.2—2002

信息安全技术
入侵检测产品安全技术要求
第2部分:主机型产品

Information security technology—
Security technical requirements for intrusion detection products—
Part 2: Host－based products

2014-03-24 发布　　2014-03-24 实施

中华人民共和国公安部　　发布

中华人民共和国公共安全
行业标准
信息安全技术
入侵检测产品安全技术要求
第2部分：主机型产品
GA/T 403.2—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.gb168.cn
服务热线：400-168-0010
010-68522006
2014年5月第一版
*
书号：155066·2-27090

目　　次

前　言

GA/T 403《信息安全技术　入侵检测产品安全技术要求》分为两个部分：

——第1部分：网络型产品；

——第2部分：主机型产品。

本部分为GA/T 403的第2部分。

本部分按照GB/T 1.1—2009给出的规则起草。

本部分代替GA/T 403.2—2002《信息技术　入侵检测产品安全技术要求　第2部分：主机型产品》，与GA/T 403.2—2002相比主要技术变化如下：

——标准名称修改为《信息安全技术　入侵检测产品安全技术要求　第2部分：主机型产品》；

——增加了主机型入侵检测产品描述(见第4章)；

——增加了安全环境，包括假设、威胁和组织安全策略(见第5章)；

——增加了安全目的，包括产品安全目的和环境安全目的(见第6章)；

——删除了主机型入侵检测产品的性能要求(见2002年版的第7章)；

——删除了数据库支持(见2002年版的6.1.5.5)；

——修改了安全功能要求的内容(见第7章，2002年版的第8章)；

——增加了技术要求基本原理，包括安全功能要求基本原理和安全保证要求基本原理(见第9章)。

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。

本部分由公安部网络安全保卫局提出。

本部分由公安部信息系统安全标准化技术委员会归口。

本部分起草单位：公安部计算机信息系统安全产品质量监督检验中心、蓝盾信息安全技术股份有限公司、公安部第三研究所。

本部分主要起草人：宋好好、吴其聪、李毅、顾健、胡维娜、赵云、杨辰钟。

本部分所代替标准的历次版本发布情况为：

——GA/T 403.2—2002。

引　言

GA/T 403的本部分详细描述了与主机型入侵检测产品安全环境相关的假设、威胁和组织安全策略，定义了主机型入侵检测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。

本部分基本级参照了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。

本部分仅给出了主机型入侵检测产品应满足的安全技术要求，但对主机型入侵检测产品的具体技术实现方式、方法等不做要求。

信息安全技术
入侵检测产品安全技术要求
第2部分:主机型产品

1 范围

GA/T 403的本部分规定了主机型入侵检测产品的安全功能要求、安全保证要求及等级划分要求。

本部分适用于主机型入侵检测产品的设计、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 主机型入侵检测产品描述

主机型入侵检测产品以系统日志、应用程序日志等作为数据源,或者通过其他手段(如监督系统调用)从所在的目标主机收集信息进行分析,从而发现异常行为的入侵检测系统。主机型入侵检测产品通常为单机版,安装在受监测的主机上。

5 安全环境

5.1 假设

主机型入侵检测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