ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1144—2014

信息安全技术
非授权外联监测产品安全技术要求

Information security technology—Security technical requirements for unauthorized external connection monitoring 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 …… 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　非授权外联监测产品描述 …… 1
5　安全环境 …… 2
5.1　假设 …… 2
5.2　威胁 …… 3
5.3　组织安全策略 …… 3
6　安全目的 …… 4
6.1　产品安全目的 …… 4
6.2　环境安全目的 …… 4
7　安全功能要求 …… 5
7.1　受控主机管理 …… 5
7.2　非授权外联监测 …… 5
7.3　响应处理 …… 5
7.4　组件安全 …… 6
7.5　安全管理 …… 6
7.6　审计功能 …… 7
8　安全保证要求 …… 8
8.1　配置管理 …… 8
8.2　交付与运行 …… 9
8.3　开发 …… 9
8.4　指导性文档 …… 10
8.5　生命周期支持 …… 11
8.6　测试 …… 11
8.7　脆弱性评定 …… 12
9　技术要求基本原理 …… 13
9.1　安全功能要求基本原理 …… 13
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。

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、厦门市美亚柏科信息股份有限公司、公安部第三研究所。

本标准主要起草人：邹春明、俞优、陆磊、吴其聪、陆臻、顾健、陈奋、张永光。

引　言

本标准详细描述了与非授权外联监测产品安全环境相关的假设、威胁和组织安全策略，定义了非授权外联监测产品及其支撑环境的安全目的，论证了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。

本标准仅给出了非授权外联监测产品应满足的安全技术要求，但对非授权外联监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
非授权外联监测产品安全技术要求

1 范围

本标准规定了非授权外联监测产品的安全功能要求、安全保证要求和等级划分要求。

本标准适用于非授权外联监测产品的设计、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界定的以及下列术语和定义适用于本文件。

3.1

非授权外联 unauthorized external connection

受保护的网络内部主机在安全策略允许之外与非授权网络的互联行为，连接方式包括但不限于双网卡、modem、ADSL、无线网卡等。

3.2

代理 agent

软件程序，能够接受服务器管控，实现对主机的非授权外联行为的监控。

3.3

受控主机 controlled host

安装了代理，能够接受服务器管控的主机。

4 非授权外联监测产品描述

非授权外联监测产品通常以C/S方式部署，包括服务器和代理两部分。可通过服务器对受控主机下发策略，监测或阻断受控主机在安全策略允许之外联接非授权网络的行为，并且能够对其及时定位，代理能够将监测结果以及告警信息发送到服务器。

非授权外联监测产品工作的网络环境主要有两类：一类为孤立网络，该网络与其他网络物理隔离，通常认为该网络内主机若通过一定的途径联接到其他网络即为非授权外联；第二类为受控网络，该网络与其他网络逻辑上可访问，但对其他网络的访问行为是受控和/或可审计的，若该网络内的主机通过安