ICS 35.020
A 90

GA

中华人民共和国公共安全行业标准

GA/T 1252—2015

公安信息网
计算机操作系统安全配置基本要求

Fundamental requirements for computer operating system security configuration of police information network

2015-05-26 发布　　2015-05-26 实施

中华人民共和国公安部　　发 布

前　言

本标准按照 GB/T 1.1—2009 给出的规则起草。

本标准由公安部科技信息化局提出。

本标准由公安部计算机与信息处理标准化技术委员会归口。

本标准起草单位：公安部科技信息化局、国家信息中心、公安部第三研究所、上海辰锐信息科技公司。

本标准主要起草人：李江、刘蓓、许涛、刘爱江、李新友、邵旭东、陈家明。

公安信息网
计算机操作系统安全配置基本要求

1 范围

本标准规定了公安信息网计算机终端和服务器操作系统的身份鉴别、访问控制、资源控制、入侵防范、剩余信息清除、应用安全和安全审计等安全配置基本要求。

本标准适用于公安信息网计算机终端和服务器操作系统的安全管理。

2 缩略语

下列缩略语适用于本文件。

IPC:进程间通信(Inter Process Communication)

RPC:远程过程调用协议 (Remote Procedure Call Protocol)

SNMP:简单网络管理协议(Simple Network Management Protocol)

SYN-ACK:同步-确认(Synchronous-Acknowledgement)

WIFI:无线保真(Wireless Fidelity)

3 身份鉴别配置基本要求

身份鉴别配置应符合如下基本要求:

a) 限制账户连续登录操作系统失败次数,超过该次数后锁定账户;

b) 设置超过非法登录次数限制后锁定账户的时间;

c) 设置操作系统账户口令:

   1) 有足够的长度;

   2) 包括大小写字母、数字或特殊字符;

   3) 设置有效期;

d) 可视情启用生物特征识别或证书认证等多种身份鉴别方式;

e) 在系统从休眠或挂起状态唤醒时提示输入口令。

4 访问控制配置基本要求

访问控制配置应符合如下基本要求:

a) 禁用操作系统的来宾账户和无用的内置账户,如任何人账户(Everyone)和产品支持账户(Support);

b) 禁止匿名账户访问操作系统;

c) 重命名操作系统默认账户名称,禁用账户的默认口令;

d) 限制具有远程访问、卷维护任务、枚举账户信息、设定进程优先级、更改计算机内部时钟、调试系统程序、驱动安装或监视系统性能等权限的账户范围;

e) 在远程访问时启用安全通道功能。