ICS 35.240
A 90

GA

中华人民共和国公共安全行业标准

GA/T 700—2007

信息安全技术　计算机网络入侵分级要求

Information security technology—Classification criterion for intrusion of computer network

2007-05-14 发布　　2007-07-01 实施

中华人民共和国公安部　　发布

前　言

本标准由公安部公共信息网络安全监察局提出。

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。

本标准主要起草人：沈亮、顾健。

信息安全技术　计算机网络入侵分级要求

1　范围

本标准规定了对计算机网络入侵分级的详细要求。

本标准适用于网络事件相关产品的设计和实现，对网络入侵进行的测试、管理也可参照使用。

2　术语和定义

下列术语和定义适用于本标准。

2.1

网络安全　network security

保护系统以及服务不受偶然或者恶意的破坏，保证系统可以连续可靠正常地运行，网络服务不被中断。

2.2

网络入侵　network intrusion

在网络上无意或恶意破坏网络安全的入侵或具有入侵企图的行为。

2.3

威胁　threat

入侵者潜在的、有预谋的、未经授权的致使系统不可靠或无法使用的能力。

2.4

机密性　confidentiality

对信息访问和公开的授权限制。

2.5

可用性　availability

信息能被及时和可靠的访问。

2.6

完整性　lntegrity

信息的可信和完整。

3　计算机网络入侵威胁

网络安全由机密性、可用性以及完整性三个安全属性组成。入侵者使用各种手段进行网络入侵，直接威胁到了这三个安全属性。

3.1　机密性

3.1.1　非授权访问

3.1.1.1　信息监听

入侵者使用非授权监听、截获等手段，对在未经保护网络中传输的信息的安全产生威胁。例如，网络中存在协议分析工具。

3.1.1.2　信息探测

入侵者使用主动的访问手段，对访问信息存在非授权读获取的威胁。根据入侵者希望获取信息的