●杨向明

# 论数字信息资源的网络安全

**摘 要** 网络安全可分为网络运行系统安全、网上系统信息安全、网上信息传播安全和网上信息内容安全。人为恶意攻击对网络安全的破坏具有智能性、严重性、隐蔽性和多样性。网络安全的目标是实现信息存储、交换的可靠、可用、保密、完整、不可否认和可控。解决网络安全问题,必须采用先进的技术、严格的管理,制订并严格执行法律、法规。参考文献 2。

**关键词** 信息资源 网络安全 危害性 安全目标 保障措施
**分类号** G250.73

**ABSTRACT** Network security includes the security of systems on the network, the security of system information on the network, the security of the information dissemination on the network and the security of information contents on the network. In this paper the author discusses the characteristics of malicious human attacks and the objectives of network security, and then proposes some solutions. 2 refs.

**KEY WORDS** Information resource. Network security. Harm. Security objective. Measure.
**CLASS NUMBER** G250.73

随着计算机网络的广泛使用和网络之间信息传输量的急剧增长,人们在得益于网络加快业务运作的同时,其上网的信息资源也遭到了不同程度的破坏,或被删除或被复制,数据的安全性和自身的利益受到了严重威胁。仅美国每年因为网络安全造成的经济损失就超过上百亿美元;在中国,利用计算机网络进行的各类违法行为以每年 30% 的速度递增。信息资源网络安全已成为重要的社会问题。

## 1 网络安全的定义及分类

网络安全的具体含义会随着"视角"的变化而变化。从用户(个人、企业等)的角度来说,他们希望涉及个人隐私或商业利益的信息在网络上传输时受到机密性、完整性和真实性的保护,避免其他人或对手利用窃听、冒充、篡改、抵赖等手段侵犯用户的利益和隐私,同时也避免其他用户的非授权访问和破坏。

从网络运行的管理者角度说,他们希望对本地网络信息的访问、读写等操作受到保护和控制,避免出现"陷门"、病毒、非法存取、拒绝服务和网络资源非法占用、非法控制等威胁,制止和防御网络黑客的攻击。

对安全保密部门来说,他们希望对非法的、有害的或涉及国家机密的信息进行过滤和防堵,避免机要信息泄露,避免对社会产生危害,对国家造成巨大损失。

从社会教育和意识形态角度来讲,网络上不健康的内容,会对社会的稳定和人类的发展造成阻碍,必须对其进行控制。

专家指出,从本质上来讲,网络安全就是网络上的信息安全,是指网络系统的硬件、软件及其系统中的数据受到保护,不受偶然的或者恶意的原因而遭到破坏、更改、泄露,系统连续可靠正常地运行,网络服务不中断。广义来说,凡是涉及到网络上信息的保密性、完整性、可用性、真实性和可控性的相关技术和理论都是网络安全所要研究的领域。网络安全涉及的内容既有技术方面的问题,也有管理方面的问题。技术方面主要侧重于防范外部非法用户的攻击,管理方面则侧重于内部人为因素的管理。如何更有效地保护重要的信息数据、提高计算机网络系统的安全性,已经成为所有计算机网络必须考虑和

必须解决的一个重要问题。

在不同环境和应用中的网络安全包括以下四种类型:

(1)运行系统安全:即保证信息处理和传输系统的安全。它侧重于保证系统正常运行,避免因为系统的崩溃和损坏而对系统存贮、处理和传输的信息造成破坏和损失,避免由于电磁泄漏产生信息泄露,干扰他人或受他人干扰。

(2)网络上系统信息的安全:包括用户口令鉴别,用户存取权限控制,数据存取权限、方式控制,安全审计,安全问题跟踪,计算机病毒防治,数据加密。

(3)网络上信息传播安全:即信息传播后果的安全。包括信息过滤等。它侧重于防止和控制非法、有害的信息进行传播,避免公用网络上大量自由传输的信息失控。

(4)网络上信息内容的安全:它侧重于保护信息的保密性、真实性和完整性。避免攻击者利用系统的安全漏洞进行窃听、冒充、诈骗等有损于合法用户的行为。本质上是保护用户的利益和隐私。

## 2 网络安全面临的威胁及其特性

面对新世纪纷繁复杂的网络世界,网络安全所面临的威胁来自很多方面,诸如黑客攻击、结构隐患、安全漏洞、安全缺陷等,并且随着时间的变化而变化。这些威胁可以宏观地分为人为威胁和自然威胁。本文重点讨论的还是人为的威胁。人为的恶意攻击是有目的破坏,可以分为主动攻击和被动攻击。主动攻击是指以各种方式有选择地破坏信息(如:修改、删除、伪造、添加、重放、乱序、冒充、病毒等)。被动攻击是指在不干扰网络信息系统正常工作的情况下,进行侦收、截获、窃取、破译和业务流量分析及电磁泄露等。人为恶意攻击具有以下特性:

(1)智能性:从事恶意攻击的人员大都具有相当高的专业技术和熟练的操作技能。他们的文化程度高,许多人是具有一定社会地位的部门业务主管。他们在攻击前都经过了周密的预谋和精心策划。

(2)严重性:涉及到金融资产的网络信息系统恶意攻击,往往会由于资金损失巨大,而使金融机构、企业蒙受重大损失,甚至破产。同时,也给社会稳定带来震荡。如美国资产融资公司计算机欺诈案,涉及金额20亿美元之巨,犯罪影响震荡全美。在我国也发生数起计算机盗窃案,金额在数万到数百万人民币,给相关单位带来了严重损失。

(3)隐蔽性:人为恶意攻击的隐蔽性很强,不易引起怀疑,作案的技术难度大。一般情况下,其犯罪的证据存在于软件的数据和信息资料之中,若无专业知识很难获取侦破证据。相反,犯罪行为人却可以很容易地毁灭证据。计算机犯罪的现场也不像传统犯罪现场那样明显。

(4)多样性:随着计算机互联网的迅速发展,网络信息系统中的恶意攻击也随之发展变化。出于经济利益的巨大诱惑,近年来,各种恶意攻击主要集中于电子商务和电子金融领域。攻击手段日新月异,新的攻击目标包括偷税漏税、利用自动结算系统洗钱以及在网络上进行商业间谍活动等等。

## 3 网络安全的实现目标

通俗地说,网络信息安全主要是指保护网络信息系统,使其没有危险、不受威胁、不出事故。从技术角度来说,网络信息安全的核心是通过计算机、网络、密码技术和安全技术,实现公用网络信息系统中传输、交换和存储的信息的可靠性、可用性、保密性、完整性、不可抵赖性、可控性等目标。

(1)可靠性:可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定的功能的特性。可靠性是系统安全的最基本要求之一,是所有网络信息系统的建设和运行目标。可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性、环境可靠性等方面。硬件可靠性最为直观和常见。软件可靠性是指在规定的时间内,程序成功运行的概率。人员可靠性是指人员成功地完成工作或任务的概率。人员可靠性在整个系统可靠性中扮演重要角色,因为系统失效的大部分原因是人为差错造成的。人的行为要受到生理和心理的影响,受到其技术熟练程度、责任心和品德等素质方面的影响。因此,人员的教育、培养、训练和管理以及合理的人机界面是提高可靠性的重要方面。环境可靠性是指在规定的环境内,保证网络成功运行的概率。这里的环境主要是指自然环境和电磁环境。

(2)可用性:可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时,允许授权用户或实体使用的特性,或者是网络部分受损或需要降级使用时,仍能为授权用户提供有效服务的特性。可用性是网络信息系统面向用户的安全性能。网络信息系统最基本的功能是向用户提供服务,而用户的需求是随机的、多方面的,有时还有时间要求。可用性一般用系统正常使用时间和整个工作时间之比来度量。

(3)保密性:保密性是网络信息不被泄露给非授权的用户或供其利用的特性。即防止信息泄漏给非授权个人或实体,信息只为授权用户使用的特性。保密性是在可靠性和可用性基础之上,保障网络信息安全的重要手段。

(4)完整性:完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性,它要求保持信息的原样,即信息的正确生成、正确存储和传输。

(5)不可抵赖性:不可抵赖性也称作不可否认性,即在网络信息系统的信息交互过程中,确信参与者的真实同一性。所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息,利用递交接收证据可以防止收信方事后否认已经接收到信息。

(6)可控性:可控性是对网络信息的传播及内容具有控制能力的特性。

## 4 网络安全系统的保障措施

要想达到网络安全的目的,必须同时从法规政策、管理、技术这三个层次上采取有效措施。高层的安全功能为低层的安全功能提供保护。任何单一层次上的安全措施都不可能提供真正的全方位安全与保密。因此应考虑从下面几个方面入手:

(1)先进的技术是网络安全与保密的根本保证。用户对自身面临的威胁进行风险评估,决定其所需要的安全服务种类,选择相应的安全机制,然后集成先进的安全技术,形成一个全方位的安全系统。网络安全是一项动态的、整体的系统工程。从技术上来说,网络安全由安全的操作系统、应用系统、防病毒、防火墙、入侵检测、网络监控、信息审计、通信加密、灾难恢复、安全扫描等多个安全组件组成。

应用防病毒技术,建立全面的网络防病毒体系;应用防火墙技术,控制访问权限,实现网络安全集中管理;应用入侵检测技术保护主机资源,防止内外网攻击;应用安全漏洞扫描技术探测网络安全漏洞,进行定期网络安全评估与安全加固;应用网站实时监控与恢复系统,实现网站安全可靠的运行;应用网络安全紧急响应体系,防范安全突发事件。近年来,特别是防火墙、网络版杀毒软件、SAN与NAS等网络存储等交叉技术的运用,为网络安全提供了强有力的后台保障。

(2)严格的安全管理。各用户单位应建立相应的网络安全管理办法,加强内部管理,建立合适的网络安全管理系统,建立安全审计和跟踪体系,提高整体网络安全意识。对人员的安全管理主要有:人事审查和录用、岗位和责任范围的确定、工作评价、人事档案管理、提升、调动和免职、基础培训等。

(3)国家和行业部门制订严格的法律、法规。计算机网络是一种新生事物,它的许多行为无法可依,无章可循,导致网络上计算机犯罪处于无序状态。面对日趋严重的网络犯罪,必须建立与网络安全相关的法律、法规,使非法分子慑于法律,不敢轻举妄动。

**参考文献**

1 孙家正主编.数字图书馆——新世纪信息技术的机遇与挑战国际研讨会论文集.北京:北京图书馆出版社,2002
2 杨向明.数字图书馆概论.北京:中国致公出版社,2001

**杨向明** 河南省图书馆副研究馆员。通讯地址:河南郑州。邮编450052。

(来稿时间:2003-05-06)