

## Analysis on Network Information Security Guarantee System

Zhenyu WANG

Xinjiang Radio and Television Network Co., Ltd., Urumqi, Xinjiang, 830000

### Abstract

With the rapid development of information technology, the Internet has become an inseparable part of people's life, work and learning, and has a profound impact on our modern society. In particular, computer information systems, which use communication networks to achieve interconnection, data through the Internet for remote transmission, remote access and resource sharing process, hackers and illegal elements are also using them to implement network penetration, secret theft and even attack. With the increasing level of Internet informatization in all walks of life, the security of network information is becoming more and more important, and people are paying more and more attention to it. This paper mainly elaborates the main contents of network information security, and discusses the construction of network information security guarantee system from three aspects of security technology, laws and regulations and management system.

### Key Words

Network Information Security, Authentication Technology, Encryption Technology, Guarantee System

DOI:10.18686/jsjxt.v1i2.629

## 浅谈网络信息安全保障体系

王振宇

新疆广电网络股份有限公司, 新疆, 乌鲁木齐, 830000

### 摘要

在信息技术飞速发展的今天, 互联网已经成为人们生活、工作和学习密不可分的一部分, 并且深刻的影响着我们的现代社会。特别是计算机信息系统, 其利用通信网络实现互联互通, 数据通过互联网进行远程传输、远程访问和资源共享的过程中, 黑客和不法分子也在利用其实施网络渗透、窃密甚至攻击。随着社会各行各业互联网信息化水平越来越高, 网络信息的安全问题也越来越重要, 越来越被人们所关注。文章主要阐述了网络信息安全的主要内容, 并从安全技术、法律法规和管理制度三个方面来探讨网络信息安全保障体系的构建。

### 关键词

网络信息安全; 认证技术; 加密技术; 保障体系

### 1. 引言

随着“互联网+”等现代信息技术的发展, 互联网与传统行业融合发展, 互联网信息技术深度融合于个人、经济、社会等各领域之中, 随之而来的网络安全事件频发, 网络渗透、网络攻击成为了热门词汇, “互联网+”融合发展的程度越深, 网络攻击造成的影响和破坏也就越大。网络信息安全不仅关系到个人信息安全, 更关系到国民经济和国家安全稳定。所以网络信息安全是一个复杂的综合性问题, 高速发展的信息技术为网络安全管理增加了难度, 如何有效保障网络信息安全成为值得深思的重要问题。

### 2. 网络信息安全的主要内容

网络信息安全是一门涉及计算机科学、网络技术、通信技术、密码技术、信息安全技术、应用数学等多种学科的综合学科。随着网络与信息化技术发展及现实环境的变化, 网络信息安全已从物理与技术属性的“硬安全”向媒介属性的“软安全”延伸, 它主要是指要保护网络环境下系统的硬件、软件和相关数据的安全, 防止网络系统遭到破坏或泄露数据信息, 使系统能够正常可靠安全运行。由于网络信息安全问题对当前社会覆盖涉及面太广, 其性质常会偏离其本真含义, 甚而出现了泛化特别是泛政治化的倾向, 所以首先要清晰的认识和理解网络信息安全的主要内容和研究范畴。总之, 所谓

网络信息安全就是指基于网络的互联互通和运作而涉及的物理线路和连接安全、网络系统的安全、操作系统及数据库的安全、应用服务的安全和人员管理的安全等。

随着计算机、通信技术的迅猛发展,计算机信息系统已广泛应用并渗透到社会各个行业和领域,人们对它的依赖性越来越大。在政治、军事、经济、科学技术、商业等领域中,重要的信息资源是通过计算机网络进行输入、处理、存储、传递,给人们提供迅速、高效的各种信息服务,如果不重视网络信息系统的保护,不加强信息安全保障体系的构建,安全漏洞可能会造成企业巨大的经济损失甚至威胁企业的生存,国家的机要信息资源势必容易被非法窃取、毁坏,将可能造成国民经济的巨大损失甚至国家安全的严重危害。网络信息安全是一个关系到国家安全和主权、社会稳定和经济发展的重要问题,所以必须加强网络信息安全保障体系的构建,保护对其发展壮大至关重要的信息资产,保护信息的私密性、完整性、真实性和可靠性的需求已经成为全社会发展最优先考虑的问题之一。

### 3. 构建网络信息安全保障体系

网络信息安全保障体系的构建主要着眼在安全技术、法律法规和管理制度三个方面。技术是前提,法律是保障,制度是规范,各方面互相联系,互相制约,构成有机整体,网络信息安全本身就是一个全方位综合治理的问题,各方面发展都要加强和提高,不断推动安全技术的发展、法律法规的健全和管理制度的完善。

#### 3.1 网络信息安全技术方面

技术是网络信息安全保障体系的基础和前提。网络病毒与反病毒、侵害与反侵害的斗争,主要是体现在技术方面。所以抓好信息安全的技術环节,将会有效遏制网络犯罪。目前安全技术主要采用以下几种关键技术手段。

##### (1) 网络认证技术

由于网络用户的不断增加和技术的日新月异,有些别有用心的人通过黑客技术进行信息非法窃取、毁坏,危害网络安全。认证技术是防止主动攻击的重要技术,目的就是检查网络信息的统一性,检查信息发送者身份的真伪,判定身份是否具有真实性和合法性,再根据判定结果来授权发送者是否能访问信息资源。目前主要的认证技术有身份认证、消息认证以及数字签名等。

认证系统在网络信息安全系统中非常重要,虽然它是最基础的安全服务,但是其他的安全技术服务都要以认证系统的安全为前提,也是网络信息安全的第一道防线,如果认证系统遭到攻击入侵,将导致其他安全技术措施可能无法发挥作用,认证系统也是黑客入侵的首选目标,所有对网络认证技术的安全要高度重视。

##### (2) 网络防火墙技术

尽管近年来各种网络安全技术不断涌现,但目前防

火墙仍是网络系统安全保护中最常用的技术之一。防火墙系统可以是软件,也可以是硬件。防火墙处于被保护网络和其他网络的边界,接收进出于被保护网络的数据流,可以防止外部网络对内部网络中重要信息的非授权访问,并根据防火墙所配置的访问控制策略进行过滤或控制,防火墙系统不仅能够保护网络资源不受外部的侵入,而且还能够拦截被保护网络向外传送保密信息。常见的防火墙技术有基于代理服务技术、包过滤技术等,这些技术可有效提升网络的安全性。

##### (3) 网络信息加密技术

网络信息加密技术主要是在网络上信息传输时,在发送端对信息进行加密,利用一定的加密算法,将明文转换成密文,再在信息的接收端对信息进行解密还原,这样就能够阻止非法用户获得和截取原始数据,从而确保网络信息的保密性。

目前密码技术主要有常规密码和公钥密码。在常规密码中,收信方和发信方使用相同的密钥,即加密密钥和解密密钥是相同或等价的。比较著名的常规密码算法如美国的 DES 及其各种变形 Triple DES、GDES、IDEA 等,其中被广泛使用影响最大的是 DES 密码。常规密码的优点是有很强的保密强度,但其密钥必须通过安全的途径传送。在公钥密码中,收信方和发信方使用的密钥互不相同,而且几乎不可能从加密密钥推导解密密钥。比较著名的公钥密码算法有 RSA、背包密码、椭圆曲线、ElGamal 算法等等。最有影响的公钥密码算法是 RSA,它能抵抗到目前为止已知的所有密码攻击。公钥密码的优点是可以适应网络的开放性要求,尤其可方便的实现数字签名和验证。但其算法复杂,加密数据的速率较低。当然在实际应用中人们通常将常规密码和公钥密码结合在一起使用,比如:利用 DES 或者 IDEA 来加密信息,而采用 RSA 来传递会话密钥。

##### (4) 灾备恢复机制

保障网络信息安全还有一项必要的措施就是建立合理可靠的数据备份和恢复机制。美国的 9.11 事件凸显了信息备份的重要性。在该事件中,一些企业的核心数据库,包括大量贸易协议、交易记录等档案信息由于没有进行异地备份而再无法得到恢复,由此造成的损失难以估量。此次事件之后,各行业都提高了对信息备份制度的重视。在 9.11 事件发生之前,尽管备份数据也是一项必要任务,但其执行过程并不那么精确或规律。但是,它现在已经成为一项必须实现的工作,实现数据库异地备份的各种数据灾备技术如 Oracle 数据库的 DataGuard、GoldGate 等在近十几年得到了快速发展和普及。”美国位于华盛顿的国家医学图书馆将其数据信息通过网络远程备份到宾夕法尼亚州,之所以选择该州,是因为通过统计发现那里发生地震的概率最小,可见其对数据备份的重视程度。灾备机制对于安全性遭受损害的数据信息的恢复至关重要。

### 3.2 法律法规的健全

建立健全网络信息安全的法律法规主要体现在建立网络信息安全管理中主体、责任、义务等方面,主要阐述法律的目标和原则,明确网络中各个主体的权利及义务,建立网站身份认证,实施网络后台实名制,保护网络主体的隐私权,推进网络信息保密制度,完善行政机关对网络信息安全的监管程序等。

鉴于网络社会更新发展速度快而规范立法滞后的特点,可建立专门保护网络商业信息安全以及网络个人信息安全的单行法。例如可以通过立法保障电子支付等各个方面的网络信息安全问题,保障个人的信息安全,及时处理网络发展、网络监管和网络服务中存在的问题,完善网络信息安全的相关条款。

各企事业单位要按照网络与信息安全的有关法律、法规规定和工作要求,制定并组织实施本单位网络与信息安全管理规章制度。要明确网络与信息安全工作中的各种责任,规范计算机信息网络系统内部控制及管理制

### 3.3 管理制度的完善

网络信息安全不仅涉及到技术和立法,重要的是管理,要通过加强和完善管理制度来提升重要网络信息的安全性。为了适应信息技术的迅速发展以及信息安全的突出需求,国际上许多标准化组织和机构很早就开始了信息安全标准的研究和制定来加强网络信息安全管理,如美国的国防部 DOD (Department Of Defense), 国际标准化组织 ISO 等。早在 2014 年中国就成立了“中央网络安全和信息化领导小组”,说明国家高度重视网络安全和信息化工作,同时要求工业和信息化部、公安部做好网络安全及相关信息安全管理,维护国家信息安全,监督处理网络安全舆情,建设国家信息安全保障体系。

制定和完善网络安全管理制度是明确网络信息系

统中管理人员的权限、职责,制定人员管理制度,同时也要完善网络使用权限、身份认证、防火墙、数据备份等基本安全措施,制定计算机信息系统管理制度。加强信息安全技术人员管理,完善管理制度,落实责任制,同时加强网络信息安全管理从业人员综合素质,提高网络安全防护技术能力,加强管理人员网络安全意识,将网络信息安全工作管理水平迈上新的台阶,以适应信息技术高速发展的现实需要。

### 4. 结束语

构建网络信息安全保障体系是一项系统工程,是要从安全技术、法律法规、管理制度等各方面逐步构建和发展完善的复杂过程,但网络信息安全保障工作无论对个人信息、企业发展还是对社会稳定、国民经济发展和国家安全来说都至关重要,我们一定要对网络信息安全工作高度重视,总而言之,“没有网络安全就没有国家安全,没有信息化就没有现代化”,在新环境下网络安全形势日益严峻,为了国家和社会稳定,我们要提高对网络信息安全的重视程度,加强对网络信息安全技术研究、增强网络信息的安全意识,重视网络信息安全技术应用,建立健全完善法律法规,加强信息安全管理,保障网络信息的安全。

### 参考文献

- [1] 林法. 计算机网络信息安全及防护策略研究[J]. 网络安全技术与应用, 2014 (01).
- [2] 李飞. 加强网络信息安全的技术保障[J]. 信息与电脑(理论版), 2015 (7).
- [3] 徐明, 刘端阳. 网络信息安全 [M]. 西安电子科技大学出版社, 2015. 07.