Computer System Networking and Telecommunications
计算机系统网络和电信，2019,1(2)
ISSN:2661-3719 (Print); 2661-3727 (Online)

Problems and Countermeasures of Computer Network Security in the Era of Big Data

Wenjing YAO Zhengde BAO Yawen TANG
School of Computer and Software, Jincheng College, Sichuan University, Chengdu, 611731

Abstract

The 21st century is an information age. The information age has bred big data technology, big data technology has facilitated the people's production and life, accelerated the development of social economy and so on, but, The explosion of data and information will often bring network security problems. These security problems greatly affect the normal use of big data technology and block the development of big data technology to a certain extent. This paper discusses the issue of network security in big data's era, and puts forward the prevention scheme for the corresponding problems.

Key Words

Big Data, Virus Infection, Network Security Technology

DOI:10.18686/jsjxt.v1i2.706

大数据时代下计算机网络安全问题及防范对策

姚文静 鲍正德 唐娅雯
四川大学锦城学院计算机与软件学院，四川成都，611731

摘 要

21 世纪是信息化时代，信息化时代孕育滋生了大数据技术，大数据技术便捷了人民的生产生活，加速了社会经济等方面的发展，但是，数据信息的爆炸话往往会带来网络的安全问题，这些安全问题很大程度上影响了人们对大数据技术的正常使用，对大数据技术发展有一定阻塞。本文就大数据时代下网络安全问题进行讨论，并且对于相应的问题提出防范方案。

关键词

大数据；病毒感染；网络安全技术

1.引言

大数据应用以及计算机网络技术伴随着互联网技术的发展而快速发展，数据信息主键渗透进生产生活，数据信息在为人们提供便捷、有效的生活方式的同时也存在一定的安全问题。大数据时代下，原有的网络安全技术不足以支撑现阶段计算机网络安全的需求，所以，网络被攻击的频率日益增加，导致网络安全脆弱，用户信息被泄露。网络安全的脆弱性给人们生产生活以及大数据技术发展带来不少不利的影响，所以为了让大数据技术有更好的发展，也为了人们的生产生活更为高效、便捷，就要增强网络防范，提高数据信息的安全性。

2.计算机网络安全及安全现状

2.1 网络安全

在使用计算机网络的过程中，信息安全以及控制安全属于网络安全的范畴。用户使用网络的过程中，不仅要按要求完成用户身份验证，同时计算机技术人员还要根据网络安全的标准，严格控制用户的操作访问。为了保证用户在互联网上的信息数据安全，计算机技术人员必须加强对计算机网络安全的关注，能够及时的发现并且修护网络安全问题对计算机造成的破坏，同时减少不法分子利用计算机网络随意监视他人信息，盗取他人私密信息的机会。在计算机网络安全问题泛滥的情况下，

想要确保计算机网络在大数据时代下发挥应有的作用，就必须不断提升计算机网络安全的防护水平。

2.2 安全现状

计算机网络的使用使得用户的生产生活有了便捷性与高效性，但是如果没有按照网络安全的相关规定来使用，而是随意使用，这将会提高计算机网络的使用安全风险。用户在使用网络的过程中，缺乏网络安全意识，不仅滋生利益会受损，还有可能会出现侵害他人利益的情况。另一方面，计算机网络安全管理发展的速度慢于计算机网络发展的速度，这就使得安全管理远远落后于计算机网络的发展。例如，黑客利用网络漏洞肆意获取用户个人信息，盗取商业机密，做违法的事情，如果网络监管不到位，就会造成数据信息的泄露，让网络成为罪犯的帮凶，造成不可估量的后果。

3.大数据时代下引发计算机网络安全的因素

3.1 计算机系统存在漏洞

计算机在发展的过程中，会根据用户的使用习惯和用户需求，不断地对系统的网络进行维护升级，但是无论计算机系统维护者如何进行修复维护，计算机系统依旧会存在漏洞。与此同时，用户在使用计算机下载和安装相关软件时，都会因为一些操作不当带来安全隐患。计算机系统的自身漏洞预防起来其实并不难，但是用户因为下载安装软件的一系列不规范的操作，以及缺乏安全意识，而产生的漏洞对计算机安全产生的隐患较大。这会造成计算机网络安全等级的下降，增加了网络安全防护技术开展的难度[1]。

3.2 网络病毒感染

计算机在不断进步与发展的同时，计算机病毒也在日益增加，网络病毒对计算机的网络安全造成了很大的威胁。例如 1971 年发现爬行者 Creeper 病毒，它的传播方式是不断复制，不断膨胀，最终把计算机硬盘塞满。确切的来说病毒程序就是一段恶意代码，病毒的传播性与可复制性对计算机来说是恶梦般的存在，破坏应用程序，威胁信息安全，更有甚者，直接造成计算机的瘫痪。

3.3 网络结构不安全

互联网网络体系庞大，是一种网间网的技术形式。在人们利用一台计算机设备与另一局域网当中的主机障碍通信联系之时，往往其互相间的数据传输要经过多个机器设备的多重转发[2]。如果攻击者攻击这条转发路径上的一台主机，就可以窃取到用户的信息，随意散步所剽窃的信息，这对用户的网络安全性有很大危害。

3.4 网络管理不当

通常情况下，计算机网络在运行的过程当中，为了运行的安全稳定性，就需要网络用户对网络进行一些必要的管理，但是网络管理方面存在很多不足，例如网络用户对漏洞不重视，修复漏洞不及时，网络用户意识不足，对网络管理缺乏科学性的认知性。同时《网络安全法》在关于网络漏洞方面制定的条例还不完善。这些网络管理方面的不足，会增大网络安全问题发生的概率，增加网络被攻击的的风险性。

3.5 TCP/IP 协议较为脆弱

互联网的基础协议是 TCP/IP 协议，TCP/IP 协议是面向公众完全公开的，所以任何人都可以了解其中内容，这一点就对计算机网络的安全性是一个打击，网络上的有心之人一旦掌握了该架构的特点，再利用其中的安全缺陷来将开展攻击行为，窃取网络用户私密信息，做违法之事，这样就会给网络用户带来很大的伤害，这一方面的因素也是导致计算机网络引发安全问题的原因之一。

4.大数据背景下计算机网络安全技术防护应用

大数据背景下计算机网络安全防护技术的应用方面需要技术人员依照现有的网络安全漏洞，展开有针对性的解决方针，对网络进行有效的安全防护，从而提高计算机网络安全系数。

4.1 计算机网络安全保密技术

目前计算机网络加密主要采用的技术是 DES 和 RSA，这些技术基本上实现了信息数据的安全加密性，同时提高了计算机网络的保密等级。

拿 DES 保密技术来举例，DES 是对称的加密技术，它的工作原理是在通信过程中，通信双方要约定相同的 key，在双方的源头用 key 对信息进行 DES 加密，以密码的形式传输，约定的 key 到达目的地后进行解密，从而提高密码的安全性，同时也增强了计算机网络安全性。

4.2 计算机网络入侵与检测技术

各种各样的网络安全问题的产生，以及网络安全措施的不利，引发了入侵检测的研究。入侵检测是指通过监视各种操作，分析、审计各种数据和现象来实现检测入侵行为的过程，它是一种积极的和动态的安全防御技术[3]。

入侵检测技术分为两个方面，一方面使用异常检测技术，全面分析计算机用户的上网行为，同时构建检测模型，以此为基底，如若发现异常，说明有非法入侵行为，这样便于计算机技术人员及时维护网络安全。另一方面，构建病毒入侵的数据库，统计现有的病毒特征，一发现入侵行为可以迅速匹配数据库，节约时间，提高维护效率，对入侵进行有效的制止[4]。

4.3 计算机网络漏洞扫面技术

计算机漏洞扫描技术是一项关于计算机网络安全方面的重要技术，该技术可以检测计算机网络中的网络设备以及终端设备的安全问题，如果存在漏洞风险，就可以及时检测出来。计算机网络漏洞扫描技术可以查询网络的盲点，将非法入侵信息进行总结，这些信息是网络安全防护工作的重要依据，从而提高计算机网络安全的可维护性。

5.大数据背景下计算机安全的防范对策

5.1 加强病毒防控管理

防控病毒是保障计算机网络安全性的必要措施，病毒一旦产生，在网络环境中传播速度快，繁殖能力强，对计算机网络安全性危害巨大。在计算机网络中，病毒的传播还有很大的随机性以及不确定性，光是这一点就大大提高了网络病毒防控的难度。所以，对于网络病毒要集中式、统一式管理，做好病毒数据库，相应的病毒预防软件要自动更新并且安装。

5.2 强化身份认证与加密技术

安全防护通常会采用一些加密手段，一般常用的单纯数字加密模式安全性较低，很容易被破解，所以应当采用数字与字母相结合的方式来加密，提高密码的难度，提高加密技术的安全性。与此同时，指纹识别技术、虹膜识别技术的发展也为网络安全加密技术提供了有利条件，这些技术使得密码更复杂，更难以解密，通过这一系列技术对计算机网络安全提供多层保护。

5.3 提高操作人员的网络安全意识

在整个计算机网络应用的途中，对整个安全性影响较大其实是计算机操作人员的意识与操作，所以强化计算机操作人员的安全防范意识，正确认识到病毒、木马的危害，规范计算机操作，这可以大大提高计算机网络的安全性。同时计算机操作人员要丰富计算机网络安全的相关知识，提高操作能力，遇到问题能够及时解决。提高计算机网络的安全可靠性，减少因为人为操作而带来的风险，保障计算机网络的正常使用[5]。

6.结束语

在大数据背景下，不论是计算机用户还是计算机操作人员都要充分了解到计算机网络的安全性，这样有利于网络安全的开展。对于计算机用户来说，提高计算机网络安全意识，合理保护自身权益，规范网络行为是至关重要的；对计算机操作人员来说，准确处理计算机网络安全问题，提供有针对性的解决政策，从而保障计算机网络的安全进行，提高网络质量是尤其重要的。

参考文献

[1]王鑫.计算机网络安全技术在大数据时代的探讨[J].科技创新与应用,2017(12):102.
[2]薛凌麒.计算机网络安全技术的问题及解决方法[J].电子技术与软件工程,2017(08):227.
[3]薛永鹏. 一种新的数据库入侵检测模型的设计[D].
[4]张传勇.基于大数据时代下的网络安全问题分析[J].网络安全技术与 应用，2015（1）：101-101.
[5]董大庆.计算机网络安全技术的影响因素与防范措施[J].中国新通信,2017,19(19):109.

作者简介

第一作者：姚文静（1998-）汉族，四川成都人，本科，四川大学锦城学院，研究方向:大数据技术
第二作者（通讯作者）：鲍正德（1989-），男，汉，黑龙江哈尔滨，研究生，四川大学锦城学院，研究方向：电子商务。
第三作者：唐娅雯（1999-），女，汉，四川省资阳市，本科，四川大学锦城学院，研究方向：信息管理、J2EE