计算机网络安全防范技术分析

周 瑞
天津天永高速公路有限公司，天津 301600

[摘要]随着信息技术和计算机网络的迅速社会经济发展和迅速发展，信息安全方面出现了新的挑战。网络本身是开放的，直接影响 it 数据的安全性。它分析了计算机网络的安全问题，并提出了确保计算机网络安全的具体预防措施。
[关键词]计算机网络；安全技术；风险保护
DOI：10.33142/sca.v5i3.6211 中图分类号：TP393.08 文献标识码：A

Analysis of Computer Network Security Technology

ZHOU Rui
Tianjin Tianyong Expressway Co., Ltd., Tianjin, 301600, China

Abstract: With the rapid socio-economic development and rapid development of information technology and computer network, new challenges have emerged in information security. The network itself is open, which directly affects the security of it data. It analyzes the security problems of computer network, and puts forward specific preventive measures to ensure the security of computer network.
Keywords: computer network; safety technology; risk protection

引言

计算机网络技术的应用受到内部和外部环境的影响，一些计算机用户对网络使用的安全性缺乏认识，从而在使用网络时造成了安全问题。网络安全的主要目的是保护网络数据，确保安全使用计算机，防止信息泄漏，并充分利用计算机网络技术。

1 计算机网络安全状况分析

近年来，计算机网络技术迅速发展，互联网在日常生活中已变得十分明显，但在现阶段，它带来了严重的安全风险，直接影响到其正常使用。美国联邦调查局的调查数据表明，计算机网络安全问题每年在美国造成 75 亿美元的损失，尤其是随着计算机网络技术的发展和传播，每 20 分钟发生一次恶意入侵。我们的内部计算机网络也是如此，在该网络中，一些黑客仍然试图通过打破防火墙来获取利益，特别是在银行系统、证券系统等方面。，具有许多计算机网络问题。我国与计算机有关的犯罪率也有所上升，这种犯罪的严重性也在不断增加。与此同时，我们的大部分基本信息技术都来自国外，因此我们的信息网络技术带来了严重的安全问题。在这方面，提高计算机网络的安全性。

1.1 黑客恶意攻击

通过多方面的信息和了解，我们知道，黑客经常入侵计算机，这种恶意攻击在公众心目中已变得非常普遍，黑客入侵的消息并不那么令人吃惊。大多数黑客拥有强大的计算能力，并熟悉计算机网络中最敏感和最脆弱的区域。他们经常使用计算机作为窃取、复制、拦截、编辑或删除重要信息的主要工具。一旦学校网络受到黑客的攻击和攻击，大量数据或秘密就会丢失，给学校造成巨大损失。这种情况只适用于学校，如果国家内部信息被非法入侵者破坏，损失将是不可预测的。黑客的恶意入侵可以说是影响计算机网络安全的主要因素之一。

1.2 计算机网络病毒

作为方案的一部分，计算机网络病毒往往是人为制造的，通过计算机网络或计算机设备传播。对于未安装防毒软件的计算机，网络病毒相对隐藏，允许用户通过浏览网站或下载软件访问计算机，从而导致计算机运行不稳定、个人信息大规模泄漏甚至崩溃随着科学技术的发展，计算机网络病毒越来越多地被隐藏起来，大大降低了被计算机入侵软件检测到的可能性，预示着它们的破坏力会增加。

1.3 非法入侵要素

非法入侵的主要因素是窃取 IP 地址或使用特殊密码入侵计算机。对于计算机用户来说，IP 地址是非常重要的信息，如果 IP 地址不正确或被更改，则它基本上是非法的。当然，这些 IP 地址已被黑客更改或窃取，这不仅是因为他们具有专业的技术技能，而且是因为他们具有强烈的反检测意识，这是普通计算机用户无法检测到的。海盗利用该程序作为一种手段，建立一个特别程序，非法窃取原始 IP 地址，并在未检测到的计算机上窃取其中包含的信息。密码入侵的形式是检查计算机系统的弱点，因为许多计算机无法访问网络或没有安装防御软件。

2 计算机网络安全技术内容

2.1 数据加密技术

作为计算机网络安全技术分析的一部分，数据加密是数据安全可以保证的关键技术。数据加密领域的研究和发展已持续了一段时间，传统的编码技术，主要是重新编码，使用

技术手段隐藏用户数据，以确保用户的安全。科技进步不能再满足当今网络信息发展的要求，不能仅仅为了确保安全而隐藏客户信息，还必须利用传统技术加强对防黑客功能的研究，防止客户信息被犯罪分子滥用因此，有必要分析数据传输和数据保留的加密技术，并分别研究不同类型的加密技术。

2.2 防火墙生产

这是计算机网络技术的一个重要组成部分，包括硬件和软件防火墙技术研究。从本质上讲，这种技术起到了隔离的作用，在一定程度上有助于组织外部网络访问公司内部网络，作为 it 和公司网络发展的一部分，及时解决数据传输问题，并确保实时监控运行情况此外，防火墙技术通过计算机网络地址过滤数据包，确保网络技术的安全，防止内部信息泄露，并隔离优先信息。

3 计算机网络安全方面的技术改进

3.1 无磁盘网络的技术作用

因为根据定义，不必在工作站用户端上安装硬碟机，所以所有资料都是透过伺服器来处理，而伺服器是在网路上设计的，其工作内容是特定的，因此不仅必须配合工作站本身的运作方式，而且必须配合系统的运作方式。例如：PXE 是英特尔开发的远程控制技术的英文缩写，用于通过网络远程启动计算机，使用网络适配器的启用芯片连接服务器并下载数据以启动系统。使用无磁碟网路技术可避免硬碟故障，而 it 网路速度则是磁碟机的二至三倍。使用无 PXE 磁盘的工作站也不会消耗服务器处理器和粮食计划署等资源。

3.2 加强防火墙保护

我们使用的计算机已经包含大量防火墙软件，在某种程度上，这些软件可能阻止我们发布废物广告和使用废物处理软件。防火墙技术可以过滤异常服务，为计算机用户提供更好的用户体验。防火墙技术(Internet 防火墙)还可以控制网络访问和访问，包括所有防火墙访问，以及在某些可疑用户访问时自动发出警报。防火墙技术是用户上网的第一个安全屏障，因此应予以加强，以提高效率，确保计算机网络的安全。

3.3 防止病毒和黑客入侵

对于目前使用的计算机，它们抵御黑客和某些先进病毒的能力非常薄弱，因此，有关部门应开发先进技术，以更好地抵御黑客和病毒的入侵。在发生入侵时，用户可以使用特殊的入侵检测系统，在使用防火墙后保护计算机系统的内部安全，并确保计算机网络不会出现异常行为；关于计算机病毒，需要根据病毒类型开发多种防病毒技术。随着计算机病毒的不断更新，计算机病毒控制技术将 Internet 病毒预防软件和微型计算机病毒预防软件结合起来，使计算机病毒一旦进入计算机，就无法再躲藏起来。通过引进新的检测技术和确保计算机网络的正常使用，提高计算机网络的安全性。

3.4 充分利用防火墙

今天，防火墙是全球计算机网络用户的基本技术。其主要目的是通过软件和硬件的组合，在网络内外和不同应用领域之间建立一个安全网关，以防止非法侵入计算机网络。人们不难理解，所谓的防火墙技术包括隔离计算机、有效区分公共网络和内部网络、仅允许授权访问、自动拒绝未经授权的恶意访问、作为防止病毒甚至黑客攻击的第一步，以及提供支持和

3.5 计算机加密处理

重要文件或数据可以加密。一般来说，当前的计算机加密可分为两类：文档加密和数字签名加密。根据功能的不同，文件加密和数字签名加密分为三类：数据传输、数据完整性确认和数据存储。数字签名加密有助于识别和验证电子记录，并有助于维护数据的保密性、完整性和不可逆转性。正确使用加密确保信息安全，使用算法处理数据或文件，将数据或文件转换为通常读取的代码，只有正确的密钥才能显示数据或文件的颜色。

3.6 采用加强身份查验的方法

这是为防御蓄意攻击而采取的积极步骤。身份认证主要是双向的。Web 环境复杂，身份认证是一种重要的认证方法。在当今最安全的身份验证方法中，可以将软件和硬件结合起来，以有效地解决安全性和易用性问题。对于物理身份验证，用户请求的数字证书和密钥分别存放在存储和传输系统中，从而有效地确保了可靠性和安全性。

3.7 其他网络安全措施

随着信息技术的发展，云计算技术，移动互联网设备，无线网络等这是计算机化的新方向。对于云计算来说，其主机组的安全性是一个主要问题。常见做法包括虚拟化云网络资源、隔离物理和虚拟网络以及访问控制；对于移动互联网设备，重点更多地放在通过安全证书和升级保护系统等措施确保智能终端的安全；此外，考虑到当前的无线网络安全问题及其存在，应采取诸如无线网络访问控制、数据加密和 MAC 过滤等安全措施，并应避免使用诸如网络安全等数据安全措施。

3.8 加强对计算机安全网络的监管

为了有效地改进安全计算机网络系统的正常运作，有必要不断改进安全计算机网络的监管制度，并确保安全计算机网络的监管以法律规则为基础。建立对安全计算机网络的有效控制和管制制度是提高安全计算机网络性能的关键，但仅仅依靠安全计算机网络监测系统并不总是足够的。因此，要全面加强对计算机安全网络的管制，首先必须对计算机用户进行培训，提高他们对网络安全的认识，并使他们能够通过适当的步骤使用计算机；第二，有必要对安全计算机网络的管理者进行培训，使他们认识到其工作的重要性，从而使他们能够在工作中承担更大的责任，并充分参与计算机网络的监管工作。最后，为了确保安全

信息系统的有效运作，必须制定信息技术系统维护政策，要求工作人员定期进行测试，及时查明安全信息系统运作的内在风险，为安全信息系统的有效运作奠定坚实的基础

3.9 提高计算机网络系统的安全性，避免不必要的风险

网络时代的变化为信息技术带来了巨大的机遇和挑战。为了有效地加强计算机网络的安全，专家们需要提高技能，并制定适应新时代危险的解决办法。网络安全监测技术目前是我国确保计算机有效运行的最有效技术之一。它能够及时检测计算机中的病毒或某些故障，一旦网络安全检测技术检测到计算机中存在病毒或故障，它就会通知计算机用户并及时采取补救措施。因此，为了使用户能够迅速发现使用计算机的问题，需要在软件上安装计算机网络安全监测系统，并定期更新和测试计算机网络安全监测系统，以确保因此，显而易见的是，信息技术人员只有跟上时代的发展，不断学习新的信息技术，才能有效地提高信息技术网络的安全。

3.10 加强对用户的网络安全教育

网络用户作为计算机的物理操作者，对计算机网络的安全产生了重大影响，网络用户，特别是担任关键职位的用户，自然会受到安全意识的影响。总的来说，由于计算机网络系统运作的复杂性，履行专业职能的计算机操作员应在就职前接受职业培训，以帮助他们了解可能涉及的各种具体行动的危险阶段、目标和操作另一方面，对于网络的普通用户来说，有必要通过多种渠道开展提高认识活动，强调预防网络安全的重要性和计算机网络安全的危险，这将使用户能够更好地了解自己业务的安全

3.11 建立网络安全监管制度

目前，在短期内很难填补信息技术操作系统的空白。为了解决系统缺陷造成的网络安全问题，必须建立基于计算机操作系统的计算机网络监测机制，以便对计算机在复制、传输、共享和修改数据方面的行为进行全面的实时监测计算机操作系统监控和扫描有助于提前发现和纠正系统故障，包括更新系统补丁程序。即使海盗在计算机操作系统中发现漏洞，监控系统也能够快速检测和拦截异常情况，防止黑客入侵网络。此外，还确保了数据安全，因为监测计算机网络有助于监测与数据有关的业务，防止非法操作和其他对计算机网络安全至关重要的操作。

3.12 强调网络安全的技术应用

目前，网络安全技术的应用是确保计算机网络安全的最有效办法，要充分发挥网络安全技术的功能，确保计算机网络的安全，就必须积极引进这方面的先进技术，并使这些技术适应需要例如，在大数据时代，计算机系统对数据访问和处理的要求越来越高，传统防火墙系统的许多缺陷越来越明显，用户可以选择应用智能人工防火墙系统，在这种情况下，防火墙 文件存在安全风险，如果防火墙发现访问网络的过程不确定，则询问用户问题并为他们提供决策参考信息。 在数据泄漏方面，可以使用智能加密系统管理文档安全，使用 256 位高强度加密算法实时加密文档，并向用户提供文件访问限制服务，以减少数据泄漏的可能性。

3.13 加强网络安全管理

从网络安全监管者的角度来看，预防网络安全问题不仅取决于网络用户本身，而且也是推进网络安全管理的必要条件。目前，网络安全监管机构可以采用云计算数据处理技术，从而有效和安全地管理计算机数据，并建立一个全面和系统的网络安全管理系统，为业务提供业务指导和工作标准。

4 结论

总之，在计算机网络技术迅速发展的背景下，必须更加重视网络安全。计算机的使用方式有助于提高对网络安全的认识，更好地管理网络安全，并减少因操作原因引起的网络安全问题。设计网络安全体系结构，加强信息安全管理等并确保网络安全运行。

[参考文献]

[1]张永刚.计算机网络信息技术安全及防范对策的思考[J].信息与电脑(理论版),2019(11):215-216.
[2]智淑敏,智慧.计算机网络通信安全中数据加密技术的应用[J].信息与电脑(理论版),2019(11):219-220.
[3]李伟.入侵检测技术在计算机网络安全维护中运用[J].国际公关,2019(6):210.
[4]徐大海.大数据时代背景下计算机网络安全防范应用与运行分析[J].计算机产品与流通,2020(6):33-34.
[5]姜可.谈大数据时代的计算机网络安全及防范措施[J].计算机产品与流通,2020(6):42.

作者简介：周瑞（1986-）女，毕业院校：天津理工大学，专业：软件工程.