网络安全的发展与研究

钟昊洋
江苏信哲软件科技有限公司

[摘　要]当今社会是信息化、现代化的发展时代，互联网技术的应运而生给社会进步与发展提供了条件。但同时网络安全问题也受到社会各界的关注。所以重视我国计算机网络安全发展，重视网络安全系统建设，根据计算机网络的特点以及后期的影响进行分析和探讨，使得计算机网络的优势特点体现出来，更好的服务于社会。

[关键词]计算机；网络安全；发展趋势
【DOI】10.12252/j.issn.2096-6261.2021.12.365

互联网对人们的生活以及工作的影响巨大，近年来也在社会各个产业领域当中取得了突破性进展。互联网给人们的生活带来了极大的便利，也改变了人们的娱乐形式。但计算机网络安全问题呈现逐年上升的趋势，由于网络中信息内容海量，一旦受到不法分子侵害，很容易出现公民信息以及财产等的损失。因此重视计算机网络安全，成为公民基本权益基础保障条件。

1 网络安全技术的特点

1.1网络保护层面不断增加

网络安全涉及的内容和形式比较复杂，如果以网络系统构建为依据积极对保护层面进行深入分析和界定，那么保护层面所涉及的内容相对狭窄，只能够对简单的数据资料进行搜集和整理，大部分工作集中于信息资料的输送和保护。在采取不同保护手段时工作效率比较低，只能够从物理层面进行解密和加密，这种传统的网络维护方式在实践中需要投入大量人力、物力和财力，网络维护成本较高，无法更好地满足语言现代化发展的实际需求。随着我国计算机技术水平不断提升，各类信息技术与现有网络安全技术紧密结合，我国需要积极实现外部链接保护的有效运行与发展。在网络时代，各行各业实现网络商业化发展趋势，由此形成的网络运行模式更为复杂，商务网络、信息对话、信息传输、信息交流中所涉及的安全保护工作越来越繁琐。以安全保护为切入点的网络安全技术，必须立足于人们日益增长的物质文化需求，加强业务发展与网络需求之间的联动，不断提升技术水平，加强对网络安全技术的创新与研究，实现网络市场秩序稳定发展。

1.2保护内容在不断增加

新时代，人们的生活质量和水平不断提高，对网络应用也提出了多样化、个性化需求。为了更好地推动市场经济稳定发展，我国必须加强网络安全技术的保护与研究，了解不同保护内容及保护范围，通过对市场经济运行模式的界定来拓宽现有的保护范围，实现内容的丰富化多元化。结合相关统计资料不难发现，网络安全技术的应用范围主要以视频信息的监控与访问管理为依据。这种模式会直接窃取数据，同时也会到其他病毒的侵害和影响，管理人员需要结合各类网络危险行为进行分析，加强对网络信息的筛选，及时修复系统漏洞。此外，管理人员要进行应急备份和应急通讯，了解不同内容的操作要求，通过不断增加网络安全技术内涵来实现网络安全产业的稳步发展。

1.3主动防御功能增强

传统的网络安全保护功能主要以被动接受为主，大部分运行方式侧重于对病毒入侵及攻击方式的研究，直接在网络中寻求相应的防御技术，达到前期阻挡的目的。这种被动的网络防御技术在实践中存在诸多不足及缺陷，相比之下，主动出击的安全监测及危险信息防御技术则能更好地提高网络安全。主动防御立足于当前网络，构建完善的数据模型，加强对正常模型及网络数据的深入分析，并在此基础上选择匹配度较高的安全网络技术，使各类网络安全问题得到有效解决。网络安全技术在主动防御过程中，产生许多新的攻击手段和攻击技术，并呈现不断优化和升级的趋势，这些能够为网络信息资产的有效保护与利用提供依据，从而降低各类网络安全风险。

2 网络中存在的安全问题

Intemnet采用TCP/IP协议。所以TCP/IP协议本身存在的.缺陷导致了Intermet 的不安全。虽然TCP/IP协议具有互连能力强。网络技术独立、支持多种应用协议等特点，但是，由于该协议在制定时，没有考虑安全因素，因此协议中存在很多安全问题"。主要有：

（1）TCP/IP协议数据流采用明文传输，特别是在使用FTP.TELNET和HTP时。用户的帐号，口令都是以明文方式传输，因此数据信息很容易被在线窃听、篡改和伪造。

（2）源地址，TCP/IP协议是用IP地址来作为网络节点的唯一标识，面节点的IP地址又不是完全固定的，因此攻击者可以在一定范围内直接修改节点的IP地址，冒充某个可信节点的IP地址进行攻击。

（3）路由选择信息协议攻击，RIP协议用来在局域网中发布动态路由信息，它是为局域网中的节点提供一致路由选择和可达性信息面设计的。但节点对收到的信息不进行真实性检查。因此攻击者可以在网上发布错误路由信息。利用ICMP的重定向信息欺骗路由器或主机，实现对网络进行攻击。

3 我国计算机网络安全现状

就目前而言，我国最普遍使用的网络安全技术有三种，如下所示。

3.1.1网络数据加密技术

该技术主要是通过密钥或密函的方式保护计算机网络信息数据。无论是信息数据的接收者还是发送者，都必须要利用密钥或者密函，同时管理互联网中的各种相关信息数据。用户在对网络数据加密以后，便能实现对网络信息数据的保护。并且，加密技术还能够对用户的真实信息数据进行获取。而要实现与数据信息的联通，也必须要通过用户的真实数据才行，如此一来，便能够对网络信息数据进行动态的保

护。密钥和密函这样的网络数据加密技术可防止用户的信息泄露，使互联网安全技术稳定性提高之外，还能够使计算机网络安全的安全性得到提升。

3.1.2网络防火墙技术

防火墙技术也是实现网络信息安全的一种重要安全技术，能够对互联网之间的各种信息通讯行为进行监督和管理。从某种意义上讲，防火墙技术就是一种能够为可信任网络开路，而为不信任网络添设屏障的技术，进而实现对影响计算机网络安全性和稳定性因索的有效控制。当有病毒或者黑客入侵计算机网络系统时，防火墙便能够对所要保护的数据进行阻拦，以限制其和互联网之间的访问，进而使其躲避那些有可能的来自互联网的各种攻击，有效保护计算机网络信息数据安全。可见，对防火墙技术而言，其关键就在于内网和外网之间所设置的屏障，这一屏障能够对内网的安全进行有效保护。比如，用户通过互联网传输数据时，防火墙就会按照用户所设定的程序或软件监控那些正在传输的数据，一旦有网络攻击出现，便会立即启用防火墙，将其拦截在外，进而防止互联网中的重要信息数据被泄露出去，以实现对用户信息安全的保护。

3.1.3数据备份恢复技术

数据信息对互联网的运行和发展发挥着非常重大的作用，如果没有对数据进行备份，或者没有使用数据恢复技术，那么储存在互联网中的各种信息数据就不能够得到有效保护。当这些信息数据遭到蓄意破坏或者直接丢失之时，如果数据不能够恢复，则将会给用户带来极大的损失。因此，对计算机网络中的数据进行备份和恢复操作时非常有必要的。因此便有了数据备份和恢复技术，其就是利用较为先进的各种网络技术，保护计算机网络中的各种信息数据。该技术是将一些重要的网络信息数据存储至计算机硬盘之中，计算机的服务器磁盘阵列便会对这些信息数据自动进行备份，就算是系统崩溃或者被意外丢失，服务器也能够将这些信息数据恢复到之前的状态。所以，广大用户还是要对那些比较重要的数据进行备份，以免重大意外造成重要数据丢失的情况发生。

3.1.4入侵检测技术

在计算机网络安全的防范领域，入侵检测技术也是-种必不可少的网络安全防范技术。其中的IDS入侵检测系统能够监测和控制网络的各种进入和出入行为，并且，对其所实施的管理和控制都是自动化的。该技术在对计算机中的网络信息进行监控的过程中，一旦发现又可以行为存在，该技术便会限制其行为，自动对那些可能引起风险的因素进行分析，隔断所有存在安全隐患的信号，做出及时预警，以使相关人员引起高度重视。在具体的防范过程中，经常会收到一些存在安全隐患的邮件，这些邮件中所存在的猜测口令便很有可能成为破坏计算机网络安全的因素。

3.2现有计算机网络安全技术的局限性

计算机网络安全技术的类型不同，其所发挥的功能也就不同，但这些技术都有一个共同点，即对计算机网络安全进行保护，对计算机网络安全的发展发挥着至关重要的作用。但是，由于技术本身和其他外在因素的影响，我国现有的计算机网络安全技术仍旧存在一定的局限性，具体如下。

（1）对网络数据加密技术而言，该技术主要分为两种，一是磁盘加密技术，二是文档加密技术，但无论是其中哪-种，都不可避免地存在不稳定的加密弊端，进而无法对其信息数据保密属性进行有效判断，直接影响信息数据的安全性。

（2）对网络防火墙技术而言，其局限性主要体现在计算机的内部互联网网络之上，该技术对互联网内网和外网之间所存在差异的辨别程度较低，所以，如果用户仅仅只依靠防火墙技术对计算机网络进行保护，是很难保障其安全的。就算一些用户使用了防火墙技术，但是由于其对该技术的了解并不深入，即便防火墙拦截了相关的怀疑网站，还是有部分用户选择忽略，仍旧允许其进入，最终造成了信息泄露的后果。

（3）对计算机备份和恢复技术而言，尽管该技术能够保证--些重要的数据信息不被丢失，但是其在具体的运行过程中抵御风险的能力仍旧偏低。通常情况下，普通用户都不会对信息数据进行备份，不仅仅是因为人们的信息数据安全意识不强，还因为该技术的普及和应用程度不高。

4 计算机网络安全的未来发展趋势

互联网技术发展将会随着时间的推移不断深化，因此对网络安全进行保护，需要将计算机技术急性提升，保证两者的共同提升与协调性。我国计算机网络未来的发展走向将队现阶段的网络安全问题突破，并将安全技术进行深入研究。从计算机网络安全技术的识别与分类阶段来看，需要先将安全技术进行分类，搞清楚不同的技术内容所针对的安全隐患问题，将具体的数据信息进行分析，这样经过匹配与分类之后，在面对不同的问题进行安全技术搜索，针对不同的计算机行为特征，进而将网络攻击进行预警，高效保护计算机系统。

总结

计算机网络安全本身所体现出来的多元性、严重性和壁垒性都是造成其影响因素众多的原因，不仅仅计算机侵袭病毒、网络系统设计和网络结构会对计算机网络安全造成影响，网络管理机制的不健全和黑客的攻击行为等也是影响计算机网络安全的重要因素。就目前而言，我国主要的网络安全管理技术主要有四种，分别是网络数据加密技术、防火墙技术、数据备份恢复技术以及入侵检测技术，虽然这些技术能够在一定程度上对计算机网络安全进行保护，但其在具体应用过程中所表现出来的弊端也是不可忽略的。在未来，我国计算机网络安全的发展将会朝着更好的趋势发展，对计算机网络安全内容的分析将会更加深入、将会构建出更好的硬件支撑平台、其技术的主动防御性能将会加强等都是未来我国计算机网络安全的发展趋势。

参考文献

[1]王艳华.大数据挖掘技术在网络安全中的应用与研究[J].电子世界，2019（23）：61-62.

[2]郭杰华.大型水电站电力监控系统网络安全态势感知系统应用与研究[J].科技创新与应用，2019（35）：163-164.

[3]张翔宇，路来顺.工业控制系统网络安全分析与研究[J].网络空间安全，2019，10（05）：114-120.