计算机网络安全与加密技术研究

周鹏轩　刘浏
宿迁学院

[摘　要]随着通信技术的迅速发展，计算机网络技术在生活中的得到广泛应用，网络安全问题也日益受到重视。网络攻击行为给信息化设备带来的破坏严重影响了经济生产和人们的日常生活。而计算机网络加密技术是当前计算机安全保障的重要手段，也是计算机安全领域的热门研究课题。本文从计算机网络安全漏洞的类型和加密技术两个角度展开探讨，讨论了预防和监视计算机网络安全漏洞的策略。

[关键词]计算机网络安全；安全漏洞；防范策略
【DOI】10.12252/j.issn.2096-627X.2020.03.714

计算机网络的迅速发展，极大地方便了人们的日常工作，同时也带来了信息安全隐患。计算机网络的安全与脆弱性是一个普遍现象。计算机网络安全问题和漏洞问题是共同存在的两个问题，给人们的生产生活带来了重要影响。计算机网络安全是一门综合性比较强的学科，加密技术是对信息数据进行加密处理，通过信息编码隐藏真实信息，同时对危险因素进行检测，以保障信息安全，防止信息被窃取，对计算机网络系统进行了有效保护。为了充分发挥计算机网络的优势，防范计算机安全隐患，我们有必要对加密技术进行研究。因此，相关研究人员必须正确认识计算机网络安全漏洞，采取适当措施防范和管窥，以确保网络安全。本文以网络安全漏洞的防范和监控为切入点，论述了应用网络加密安全防护技术的各项措施，对计算机网络安全加密技术展开了深入探讨。

一、网络安全漏洞的含义

随着时代的发展，网络安全问题日益突出，计算机网络安全漏洞是造成网络安全问题的重要因素。计算机网络安全漏洞是指在协议、软件、硬件的具体实现或系统安全策略上存在的缺陷，这种缺陷往往是由于攻击者在没有任何授权的情况下对系统和设备进行访问或破坏而造成的。计算机网络安全漏洞的影响作用非常广，影响到计算机软件、路由器、防火墙，甚至操作系统本身。一些不法分子很容易利用这些软硬件自身存在的漏洞进行攻击，各类计算机病毒也能通过这些漏洞进行渗入和传播，造成计算机系统的破坏或者信息的泄密。在当今社会，计算机网络技术发展迅速，计算机网络的破坏方式也呈现出多样化的特点，为了防范计算机安全问题，加密技术也不断升级。

二、网络安全漏洞的类型

（一）IP地址被盗

IP地址被盗用是一种常见的网络安全问题，不法分子通过未经授权的网站来掩饰身份，破坏使用者的网络资源，给使用者带来巨大的经济或者信息数据算式。因为IP位址通常拥有很高的权限，如果IP地址被窃取，对于计算机的破坏作用很强，会严重损害使用者的合法权益，危及整个计算机网络的安全。

（二）计算机病毒

计算机病毒也是一种普遍的安全漏洞，它是由人为写出的恶意程序，把它附着在程式码上，对计算机网络产生破坏。因为计算机病毒对于载体的适用度很高，因此非常适合携带，一旦计算机被病毒感染，病毒还能在计算机内进行自我繁殖，对计算机的正常适用造成极大的威胁。

（三）OSOS与Network协议的缺陷

一般而言，操作系统本身带有某种固有缺陷，同时新的操作系统功能的应用会间接地导致操作系统的安全问题，包括控制混乱、操作系统陷害、输入和输出非法访问和不完全中介等。TCP/IP技术通常无法准确识别IP的源头，并且缺少内部监控机制，所以常常会被黑客利用 TCP/IP来获取 TCP的序列码，从而给计算机用户带来重大损失。

（四）拒绝服务攻击

“拒绝服务”是指黑客通过攻击用户的计算机，导致其计算机的正常服务被拒绝，无法提供相应的服务。拒绝服务攻击的基本远离就是通过发送大量的服务请求到用户的计算机上，使用户的计算机系统资源被堵塞，从而无法响应用户的正常业务需求，进而产生拒绝服务。该攻击覆盖了服务器、路由设备、互联网宽带资源。

三、计算机网络安全问题的产生原因

计算机网络安全问题的成因通常可以归类为两大类：第一个类别是根据计算机自身的划分展开分类，一般可以分为：硬件、软件、操作系统方面的漏洞；第二类是按照使用者的身份来划分，一般分为两类，其一是使用者的安全意识不强，其二是人为恶意攻击。

（一）计算机网络软体存在的安全问题

软件漏洞通常被不法分子用来进行恶意攻击。相关数据显示，在计算机网络安全漏洞中，计算机软件漏洞超过一半，若不能及时修补计算机网络软件的安全漏洞，将会导致计算机软件遭到攻击。计算机网络软件之安全性问题，往往被视为网络安全问题之源头，尤其是当某些使用者获得机密信息后，会产生相当数量的网络诈骗事件。

（二）计算机网络操作系统存在安全漏洞

计算机网络本身具有共享和交互的特点，为了响应用户的需求，必须扩大网络的规模，开发新的应用程式，这势必会导致网络的安全问题。通常情况下，一台计算机的网络使用愈久，其安全隐患便会显露出来。链路是计算机网络的基础，在对各类网络文件进行处理时，不可避免地会遇到文件和系统的安全问题。例如物理安全性、协议安全性等。这些风险都会造成信息资源的损失，从而造成网络的瘫痪。

（三）用户对网络安全的认识不足

当前，由于用户对网络安全的缺乏了解，致使用户的账号信息泄漏，从而对计算机的安全问题的例子不及其实。由于对计算机安全意识不高，因此对计算机的安全问题并不十分重视。此外，由于缺少相关的技术标准，使得网络的监测与维护变得非常困难。

（四）恶意攻击

目前，恶意攻击已经成为影响计算机网络安全的一个重要因素。一般认为，人为的恶意攻击有两类，一种是主动的，一种是被动的。主动的人为恶意攻击通常会破坏计算机的信号，而被动的人为破坏计算机的重要资料。人为的恶意攻击，常常会造成数据的泄漏，造成信息资源的破坏和损失。人为的恶意侵入是为了窃取计算机相关数据，而使用远程方式进行计算机操作时，经常会遭到黑客等恶意攻击。同时，病毒的扩散也会

对计算机网络的安全造成极大的威胁。

四、计算机网络的安全监控与对策

随着人类的进步，计算机网络也变得越来越庞大，越来越复杂。为了进一步提高计算机网络的安全性，必须全面了解计算机网络的安全性，才能掌握网络安全。

（一）信息隐藏技术的使用

信息隐藏技术是计算机网络安全技术中最基础的一种保密技术，它可以通过对用户的身份认证和访问控制来及时阻止非法用户的入侵，将用户重要的信息转化为非法用户无法窃取的信息，从而有效地保护用户的网络安全。同时，信息隐藏技术还可以将用户的信息隐藏在信息中，让非法入侵者无法识别信息，进而无法窃取信息。因此，信息隐藏技术对提高计算机网络安全具有十分重要的意义。

（二）存储加密技术使用

信息泄露是计算机网络安全的另一个隐患，采用存储加密技术使信息在存储过程中处于加密状态，进而保证信息的安全性，一般通过密文存储和存储控制来实现。密文存储主要侧重于信息加密算法的转换，可重新设置加密模块，并创新加密密码，保证网络信息存储的安全。而存储控制则偏重于对外来者信息进行审查，检验其是否具有审查资格和权限，进而防止非法入侵者盗用网络信息。

（三）传输加密技术使用

计算机网络在处理信息和传输信息方面起着重要作用。个人和企业的某些信息需要保密，方式信息在传输过程中出现泄漏非常重要。因此，信息在传输过程中也需要加密技术的保护。第一种是线路加密，主要是根据计算机网络的信息传输线路，设置不同的加密技术来识别和保护信息，但是很容易忽略信号源，这是线路加密的弊端。另一种是端对端加密技术，主要是在发送端发送的时候，将信息加密，然后以不可识别的方式发送到互联网上。

（四）消息摘要加密技术

在计算机网络安全中，信息摘要加密技术是信息管理与加密技术的重要组成部分。比如，计算机用户发送了个人文件或者消息，那么消息的摘要就会被加密，而使用私密密钥加密的方式则会变成一个数字签名，这样就可以保证消息不会被入侵者看到，而接收到消息的人，则需要用一种固定的方法来解密。同时，接收者还可以比较信息摘要，观察信息摘要是否在传输过程中被篡改，正确解读信息摘要，同时保证信息摘要的完整性。

（五）完整性鉴别技术

完整性识别技术，通过一系列举措，识别出接受信息和使用信息者。同时，通过审核接收者所持有的密码，密匙的正确性和数据，只有满足了信息设置的参数和标准，才能够被允许阅读，这样才能够保证信息的安全，这也是加密技术发挥作用的关键，可以保护信息不外泄。

（六）密匙管理机密技术

计算机网络安全信息复杂多样，每一种信息都有不同的管理方法，其中密匙就成了最基础，也是最重要的一种管理方式，可以保证信息的安全，保证信息不会被盗取。因此，在计算机网络安全加密技术中，密匙是核心技术。而且密匙使用的介质主要是U盘，也是比较方便的加密技术。

（七）确认加密技术

计算机网络安全与保密技术相结合，可以有效地防止信息被窃取。所有的信息和技术，都需要经过严格的加密。也就是说，确认加密技术可以限制信息的范围，防止信息被篡改和伪造。同时，也可以审查信息的合法性，让发布信息的人无法否认自己发出的信息，从而审查信息的来源。确认加密有三种方式，一种是消息确认，第二种是身份确认，第三种是数字签名。

（八）链路加密技术的应用

链路加密技术是网络系统中的一种在线加密技术，在数据传输前对信息进行加密处理，充分利用网络技术的优势，保证信息传输过程的安全性。不同节点在接收到相关信息后进行解码，在下一链路传输时对数据重新加密，这也保证了信息数据传输的安全高效性。链路加密技术能够对信息数据进行多重加密，满足了现代计算机网络信息传输的要求，有效地提高了数据传输的安全性。为能够发挥这项技术的功能作用，用保证链路两端的加密效果，合理地利用其他链路，提高数据的传输效率。

（九）节点数据加密技术的应用

节点加密技术要求点对点线路两端的加密设施同步，同时对信息数据进行加密处理，把数据放入安全板块，再进行加密处理，从而提高计算机自动化保护水平。当计算机系统受到病毒入侵时，利用节点数据加密技术中心的保护功能模块，对所传输的信息进行加密处理，以保证各节点能够准确地提供信息内容。如果节点的信息内容比较直接，很容易受到网络攻击，从而影响到该技术的应用效果，因此必须加强节点加密以有效地控制信息泄露。

（十）数据库加密技术的应用

随着计算机网络技术的迅速发展使得信息数据处理质量和分析水平得到了极大的提高，通过建立网络数据库，可以对各种类型的信息数据进行保存和管理，为其他工作提供了方便。为了保证数据的安全和完整性，必须对数据库进行加密处理，以提高数据安全管理水平。主要通过设置访问权限来保护数据安全，并设置相应的密码，用户在查询和使用数据库信息之前，必须经过安全验证，并具有相应的权限才能进入系统，从而有效地保护相关数据信息。

（十一）防火墙安全保密技术的应用

防火墙技术在保护计算机网络信息安全方面起到了重要作用，其能够有效分离内网与外网，形成安全保护屏障，控制非法入侵。防火墙技术应用了计算机硬件设备，将硬件与先进软件技术相结合，营造安全的网络环境， 对计算机网络系统中的信息数据进行针对性保护。防火墙技术的合理运用可以抵御病毒攻击，防止出现信息泄露的情况，通过安全隐患扫描可及时发现危险因素和网络攻击，并作出有效应对。防火墙技术在使用期间，应将就计算机后台中的软件关闭，以免出现病毒从端口入侵的情况。对不安全、不清楚的网址能够及时检测出来并进行安全提示，可规范计算机使用人员的访问行为，以此降低网络安全问题出现。

结语

加密技术是当前计算机网络安全保障中的一项重要技术，通过对数据信息的加密处理，可保障计算机网络安全，为用户提供安全、稳定的网络环境。要正确认识加密技术及其应用，我们需要了解加密技术的类型、原理，了解其应用要点，并实现各项技术的合理运用，以此降低网络安全隐患造成的威胁。还要加强对加密技术的深入研究与分析，并注重持续改进与完善，从互联网整体安全发展的角度出发进一步提高加密技术的功能作用。

参考文献：

[1]岳超.计算机网络安全中数据加密技术的应用研究[J].信息与电脑（理论版）,2018（17）:187-188+191.