数据加密在计算机网络安全的应用

赵海宽
北京达佳互联网科技有限公司　北京市　100085

摘　要：随着人类经济的增长和科学技术的飞速进步，计算机技术和网络迅速渗透到我们生活的方方面面，各种网络安全事件时有发生，由此造成用户经济损失增加。在这种情况下，为提高网络技术的安全性，相关计算机安全专家和技术专家也加强了安全性的改进研究，包括数据加密技术，提高了信息传输的安全性，为保护计算机安全作出了重大贡献，下面将对其进行详细讨论和分析。

关键词：数据加密；计算机网络安全；初始端到终端加密

Application of data encryption in computer network security

Haikuan Zhao
Beijing Dajia Internet Technology Co., Ltd. (Beijing) 100085

Abstract: with the growth of human economy and the rapid progress of science and technology, computer technology and network have rapidly penetrated into all aspects of our lives. Various network security incidents have occurred from time to time, resulting in increased economic losses of users. In this case, in order to improve the security of network technology, relevant computer security experts and technical experts have also strengthened the research on security improvement, including data encryption technology, which has improved the security of information transmission and made significant contributions to the protection of computer security, which will be discussed and analyzed in detail below.

Keywords: data encryption; Computer network security; Initial end-to-end encryption

前言

近年来，随着我国国民经济的快速增长和全球经贸往来的频繁，我国的计算机技术和网络水平也获得了相当大的发展和提升，因此计算机技术和网络技术得到了迅速的应用，为我们的现代工作和生活带来诸多便利。这在一定程度上提高了中国企业经济市场的发展效，也改变了我们现代生活和娱乐的结构和方式，将我们带入了现代化、电脑化和娱乐化的网络时代，人们的日常生活和工作越来越多地与计算机和互联网相连。然而，由于计算机网络科学技术的飞速发展和提高，网络安全面临着诸多危险。尤其是近年来，黑客攻击、网络经济交易、公司文件泄露等，严重危害了人们的工作和生活。为遏制此类网络犯罪，震慑网络黑客，计算机安全技术人员和相关专家加强了网络安全技术的研究与开发，开发和借鉴了各种网络安全技术和软件。数据加密技术是最重要的网络安全技术之一。本文讨论了数据加密技术在计算机安全中的应用，简要介绍了威胁计算机安全的因素和数据加密技术的概念，然后分析了它们在网络安全中的应用。

一、数据加密技术的概念和类型

数据加密技术是防止泄漏或入侵的信息加密技术。这种数据加密技术主要是基于加密原理，通过添加密钥和加密功能来移动和替换信息。这种数据加密的方法可以保证信息的传输不被他人泄露，从而保证了信息的机密性和安全性。具体实现流程如图1所示。

数据加密有两种类型：对称数据加密和非对称数据加密。两者都具有相同的加密原理——加密和解密信息以保护其安全性和完整性[1]。使用同一组解密密钥，后

者是指使用不同的解密密钥发送和接收信息。

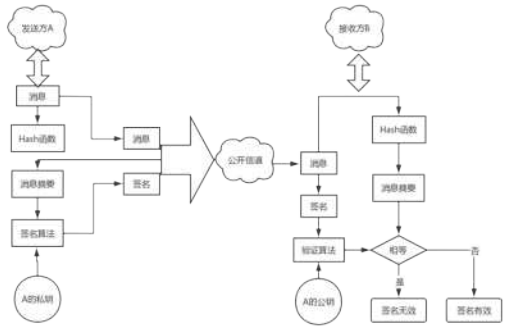

图1 数字签名操作流程

二、计算机网络安全中数据加密应用的分类

（一）初始端到终端加密

在计算机网络安全管理中，初始端到终端加密是一种应用广泛的加密技术。在传输计算机网络信息数据的过程中，文件总是以加密的形式存在。如果文件未达到终点，则无法有效解码。即使节点损坏，也完全不会影响保护工作的质量，不会造成重要的用户数据信息受损。在管理计算机网络安全的过程中，初始端到终端加密技术的最大优点是设计简单、易于维护、应用成本低。在设计初始端到终端加密技术应用架构时，相关技术人员应了解初始端到终端加密系统的运行只应提供初始端到终端和初始端到终端的加解密服务，不需要考虑传输的中间环节。网络非法人员不能窃取它们之间传输的信息，即使是ISP也无法访问流量数据。

（二）连接加密

连接加密技术也称为互联网加密技术，其本质是指在两个网络节点之间的通信连接中对数据传输进行安全加密的功能，以有效提高计算机网络用户数据传输的安全性和可靠性。控制加密网络的计算机安全应用程序通过在传输前加密信息来工作，最终到达目标连接点。在计算机网络安全中合理应用连接加密技术，可以帮助网络安全管理人员有效解决暴露的传输线路和源点的安全问题，大大提高管理网络安全的水平。但是，连接加密也存在密钥分发效率低、加解密效率低等缺点。另外，在使用连接加密技术的过程中，需要保证连接两端的加密同步，这对计算机网络的性能提出了更高的要求，需要更多的资源成本[2]。

（三）节点加密

节点加密技术广泛应用于计算机网络的数据传输阶段，可以帮助人们有效解决各种信息安全问题。节点加密技术在计算机网络安全原理中的应用是使用密码设备通过节点连接到节点机器，对密码进行解密和加密，然后只有发送方信息和接收方信息中的数据。可以使用密码、特定信息内容进行解锁，从而将数据信息被传输的风险降到最低。节点加密要求以清晰的方式提供标头和路由信息，以便中间节点可以接收信息。与连接加密技术相比，它们有一些相似之处，不仅可以保护计算机网络通信链路中数据传输的安全，中间节点也可以被解码和加密。不同之处在于，加密节点必须以明确的方式提供标头和路径信息，以便中间节点能够获取信息来处理消息，这对于网络犯罪分子分析通信服务非常不便。

三、使用数据加密技术对计算机网络安全的主要影响

基于社会发展的新时代，人们越来越依赖计算机技术的使用，无论是在日常生活中，还是在学习和工作中，都会选择使用计算机网络技术来大大提高学习和劳动的效率。然而，计算机网络的发展也带来了各种安全隐患，威胁着用户的切身利益。例如，近年来网络安全问题频发，企业和个人用户的重要数据被泄露或破坏，严重影响了我国计算机网络产业的和谐健康发展。

（一）计算机网络安全软件漏洞

多用户、计算机网络、同步和操作系统的进程将不同的主机网络系统组合成一个数据包，同时接收和传输信息和数据，计算机网络连接很容易出错，以及出现各种漏洞，由于这些程序和命令同时工作，网络防御薄弱，更容易引发网络入侵攻击。

（二）计算机网络病毒

计算机网络病毒也对计算机安全构成严重威胁，计算机网络病毒传播迅速、规模庞大，难以根除，如果计算机文件信息或软件病毒被感染，所有相关软件或连接的计算机也会被感染，对整个计算机系统造成严重破坏。

（三）计算机网络服务器信息泄露

许多计算机服务器后台的系统并不完善，如果错误没有及时纠正，或者程序存在问题，就会导致部分服务器相关信息泄露，从而对信息安全造成网络破坏。

（四）对计算机网络系统的干扰

网络不安全的最后一个因素是非法入侵计算机网络系统。通常，网络黑客通过一些非法手段窃取网络用户、密码、IP地址等信息，然后窃取和使用与该工具相关的信息。

四、计算机网络安全问题的主要原因

在当前我国计算机产业的建设和发展中，大量的计算机用户经常遇到计算机网络安全的各种问题，影响到

企业和个人的利益。造成计算机网络安全问题的原因很多，不仅与计算机用户本身有关，还与计算机网络管理环境有关。无论是企业还是个人在运行和使用计算机网络的过程中，都必须学会规范使用计算机操作，加强加密技术的学习和使用，以充分保证网络运行的安全性和可靠性。

（一）计算机数据库管理存在差距

随着计算机技术的普及，各行各业的人们开始密切关注管理计算机网络安全。一些正规企业在日常管理计算机数据信息的工作中，会使用先进的加密技术进行保护。提高用户数据和信息的使用安全性和可靠性。值得注意的是，计算机数据管理系统在数据处理方面有其独特的运作方式，在当前运行中会面临各种风险，在很大程度上威胁着用户计算机网络的安全和稳定。特别是一些企业采用分级管理系统进行计算机数据库系统的设计和管理，对计算机数据库系统的安全性提出了更高的管理要求[3]。一旦计算机数据库系统出现安全漏洞，就会威胁到用户计算机网络的安全使用。在当今的网络环境中，网络黑客的恶意攻击手段越来越多，他们可以通过各种渠道、网络安全事件干扰和攻击计算机用户的数据库，造成巨大损失。

（二）计算机网络安全水平低

市场上用户电脑的组成主要由两部分组成，第一个是硬件，第二个是软件。硬件系统包括主机、显示器和电源，软件包括计算机网络和相关应用。为了发挥计算机系统的总价值，计算机用户需要加强计算机软件系统的安全更新和维护。软件系统的安全运行水平关系到整个计算机系统的正常稳定运行。尽管中国计算机市场的网络安全防护工作水平有所提高，但仍有大量用户计算机网络安全水平不高，缺乏科学规范的计算机网络系统设置，导致计算机系统遭受网络病毒的入侵，由于用户的网络安全等级低，无法准确有效地识别网络病毒和非法程序，从而使计算机网络系统瘫痪。有鉴于此，计算机网络用户应引入和合理使用先进的数据加密技术，配合专业的杀毒软件和合理的防火墙技术，完善系统，降低计算机安全管理风险。

五、数据加密在计算机网络安全中的应用

（一）信息技术数据签名认证的应用

在网络安全管理中，数据签名信息技术认证的应用原则是将端口加密技术和连接加密技术相结合，最大限度地提高网络信息传输过程计算机的安全性和可靠性。借助基于数据签名信息技术的认证应用，可以对用户信息数据进行安全加密。数据接收方必须通过解密密钥获得目标信息的有效数据。该技术广泛应用于有一定市场的大中型企业，如银行卡支付、纳税等。数据签名信息技术认证涉及两种具体方法，一种是密码认证，另一种是数字认证。申请密码认证相对简单方便，不涉及数据信息的处理。数字验证是一种基于数字证书的加密技术，可以解密计算机网络提供的信息，验证数字签名，保证用户信息传输的安全性和完整性[4]。图 2 显示了创建和验证数字签名的过程。

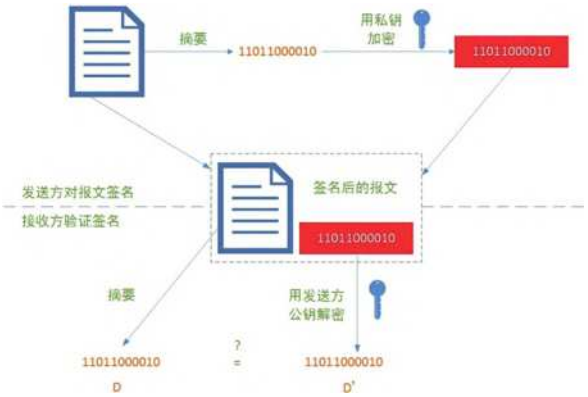

图2 数签名的制作和验证过程

应用数字签名加密技术的过程如下：(1)消息的发送者可以使用摘要算法生成待加密信息的数据摘要；(2)消息的发送者有效地使用自己的私钥对信息数据进行汇总，完成加密操作；(3)消息的发送者将消息数据和签名消息的摘要发送给接收者；(4)接收方对收到的消息使用相同的摘要算法接收新消息；(5)接收者使用消息发送者的公钥查看签名消息的摘要。 成功解密消息后，可以查看发件人的消息，并且消息摘要是完整且准确的。

（二）对称和非对称加密应用

在计算机安全管理中，数据加密技术主要分为两类：对称加密、非对称加密。管理员可以根据网络安全管理的需要选择加密技术。例如，当主体是特定情况，需要依靠计算机网络传输数据和信息时，工作人员应合理使用加密技术。但是，如果主体没有及时确定，那么在计算机网络信息和数据的传输和处理中，就需要科学地应用非对称加密技术。无论采用何种加密技术，首要目的都是保护数的完整性和安全性。对称加密技术在计算机网络安全管理中得到了广泛的应用，因为对称加密在添加相同密钥时具有简单方便的优点。使用对称加密时，计算机网络安全管理人员可以根据现状合理使用DES、AES、3DES等加密算法[5]。无论使用哪种加密算法，发送方和接收方都能收到相同的密钥，加解密工作效率高。适用于长消息数据的安全传输。非对称加密技术和对称

加密技术最大的区别在于有两个密钥，一个是公钥，一个是私钥。应用非对称加密技术的原理是用私钥对原始数据信息进行加密，所以解密时要使用公钥。非对称加密技术在计算机网络安全应用中的最大优势在于使用简单方便，能够科学有效地预防和控制网络攻击者解密密码，防止此重要信息泄露到私人数据中或被销毁。

六、加密技术在计算机网络安全管理中的应用设计

（一）应用要求

在设计加密技术应用的过程中，相关人员首先要了解数据机密性的本质设计要求，必须使用加密技术有效、高效地了解日常可读文本的成本，这样一来当用户在利用互联网进行数据信息传递时，即便是被数据信息被非法分子所盗取，也不会丢失重要数据。尽管该过程会被犯罪分子恶意混淆数据信息，但对用户数据本身的粗略计算还是仍然相对完整。

（二）科学选择应用算法

网络信息安全已经成为计算机行业人士非常关心的话题，加密技术的设计与应用是计算机网络管理中必不可少的内容，人们经常使用的加密技术之一是密码技术，根据密钥类型区别可以分为两种，一种是对称密钥系统，一种是公钥系统。在计算机网络安全管理的应用中，对称密钥系统具有加解密效率高、解密难度较大等优点，但其缺点是对安全密钥存储的依赖程度较高。一旦密钥泄露，将直接威胁到用户的数据信息。公钥系统的优点是安全性比较高，但缺点一般是密钥长，运行速度慢。此外，网络安全管理者在实践中还可以选择RSA、MD5、DES等加密算法。RSA公钥加密算法作为一种双密钥非对称密码体制，广泛应用于计算机网络安全管理。它可以高效地生成私钥和公钥对，可以最大限度地提高数据加密安全性，还可以应用于数字签名级别，具有很好的定制范围。作为一种单向加密算法，MD5加密算法有两个明显的特点。首先，加密后的两条明文数据可能不相同。其次，每条明文数据的结果在加密后必须保持不变。MD5加密算法应用过程主要基于位补全和转换。相关人员应对数据长度进行附加位运算和附加运算，然后恢复和加载各种参数，对传输的数据进行转换处理，最后提取密文结果。

（三）加密系统密钥的科学管理

在计算机网络安全管理中，加密系统的基本设计要素是加密算法和密钥管理相关技术人员需要了解，不同的公式和规则将指定加密和明文之间的切换方法。在密钥管理中，密钥是控制和解码算法的重要信息。在普通计算机应用的前提下，需要更完整的应用方案。在应用加密算法的过程中，公钥生成由应用程序完成，重要数据信息操作的保密处理可以基于公钥完成。本文以对称AES加密算法的设计和使用为例。网络安全管理员使用该加密算法对文件打包模块进行加密，并可以随机生成合适的密码，完成查询和评估数据信息权限。只要计算机用户拥有最高权限，并且可以获取到每个文件中的相应密码，如果计算机用户想要解密加密的文件系统，那么他必须首先处理服务器用户名和密钥操作，管理模块还会将用户权限、信息等真实有效写入到计算机数据库中，计算机用户验证后可申请相应权限的密码，充分保证了信息查询的合法性。

结束语：

总而言之，在当今快速发展的计算机网络行业中，保护计算机网络用户数据的信息尤为重要。网络安全管理人员需要及时转变管理理念，创新和完善计算机网络安全管理模式，充分认识合理使用加密技术提高管理水平的重要性。网管人员要学会将计算机网络信息管理的具体条款和要求与科学、良好的数据签名信息验证技术、对称加密和非对称加密技术的灵活运用等相结合，确保能够最大限度地发挥网络信息加密技术的价值，以及实际维护用户的合法权益，避免重要数据信息泄露和损坏。

参考文献

[1]曹建华. 数据加密技术在计算机网络安全中的应用探讨[J]. 网络安全技术与应用, 2018(2):2.

[2]韩冬. 数据加密技术在计算机网络安全中的应用[J]. 中国新通信, 2021, 23(19):2.

[3]刘馨泽. 数据加密技术在计算机网络安全中的应用价值[J]. 电子技术与软件工程, 2018(9):1.

[4]蔡勇. 办公室计算机网络安全中数据加密技术分析与研究[J]. 数码世界, 2018, 000(012):124.

[5]杨森智. 计算机网络安全中数据加密技术的应用研究[J]. 电脑编程技巧与维护, 2018(1):3.

作者简介：赵海宽（1994.3），男　汉，陕西省西安市，本科，高级研发工程师/Java开发，主要从事互联网金融系统开发相关工作。