Transactions on Computer Science and Technology
Volume 11 Issue 1, 2024, PP. 1-5

The Application of Data Encryption Technology in Computer Network Security

Jinfang Zhang
Shanghai Penxi Semiconductor Co., Ltd., Shanghai, 201206, China

Abstract

The rapid development of information technology has accelerated the arrival of the Internet era. As a representative of information technology, computer network technology has been increasingly applied in many industries and has become a commonly used tool in people's lives and work. The application of computer networks not only improves management efficiency, but also raises some security issues, such as network viruses and information leaks. It is particularly important to choose reasonable data encryption techniques to ensure computer network security. This article combines the actual situation of computer network security management and conducts research on the application of data encryption technology in computer network security, aiming to further promote the development of computer network technology.

Keywords: Data Encryption Technology; Computer Network Security; Application

数据加密技术在计算机网络安全中的运用

张津芳
上海朋熙半导体有限公司，上海 201206

摘 要：信息技术的高速发展加速了互联网时代的到来，计算机网络技术作为信息技术中的代表，在诸多行业中的应用日益深入，成为人们生活和工作中的常用工具。计算机网络的应用不仅提升了管理效率，也引发了一些安全问题，如网络病毒、信息泄露等。为保障计算机网络安全，选用合理的数据加密技术显得尤为重要。本文结合计算机网络安全管理的实际情况，对数据加密技术在计算机网络安全中的运用展开研究，旨在进一步推进计算机网络技术的发展。

关键词：数据加密技术；计算机网络安全；运用

引言

网络技术的应用推进了人们工作模式和生活模式的转变，为人民的日常生活创造了极大的便利，对于促进经济社会的建设与发展具有重要意义。但网络技术的应用是一把双刃剑，在提高效率的同时也引发了一些网络安全问题，各类漏洞被不法分子利用谋取利益，造成了巨大的损失，传统的数据加密技术的加密模式逐渐难以满足计算机网络安全管理的实际需求，加强对数据加密技术的管理和应用显得尤为重要，成为计算机网络安全管理中的关键任务。

1 数据加密技术的概述及构成

数据安全是网络安全的重中之重，2022 年中国数据安全行业产值为 88.3 亿元，同比增长 26.69%，2015 年至 2022 年复合增长率为 28.22%。作为信息数据安全中的核心技术，数据加密技术基于密码学相关技术的原理对海量的信息和数据进行加密、解密和识别操作，利用加密算法将明文数据信息转化为安全性较高的密文，接收者在接收到数据后，利用解密逻辑或密钥对加密的数据进行解密，从而提高计算机网络系统中数据传输的安全性和隐蔽性，当不法分子入侵电脑系统后，缺乏相应的解密密钥，无法知悉信息的具体内

容，进而达到保护数据安全的理想目标，结合计算机网络安全管理的实际情况来看，主要可以细分为链路加密、非对称加密、对称加密和节点加密等技术。

数据加密算法是加密技术中的核心，面对不同的加密场景，可细分为 DES 算法、MES 算法、RSA 算法等，DES 算法能够将网络信息加密为特定的 64 位秘密电文，开展 8 位密文的检测与奇数偶数检验，具有一定的迭代性；MES 算法与其他的加密算法相比，相对较为稳定，能够将数据明文输入到 IP，随后转移到 64 位密文，在各类加密工作中的应用较为广泛；RSA 算法一般由两个密钥组合而成，是业界认可的加密算法，在密钥的生成过程中，随机选定两个质数，随后将两个数相乘，得到相应的乘积，随后基于欧拉函数的结果，得出加解密的密文密钥。

2 计算机网络的常见安全风险

2.1 系统漏洞

在当前时代下，数据共享技术的应用日益深入，计算机在和互联网终端相连后能够进行数据和信息的上传、查看、下载，为人们的日常生活和工作创造了便利，但是互联网具备一定的开放性特点，若不加强防范，容易造成互联网病毒的传播，引发严重的网络安全问题，造成巨大的经济损失。结合计算机的软硬件来看，不同类型的软硬件计算机往往都存在一定的系统漏洞，因此网络安全管理人员在后期的计算机使用过程中，一方面要逐步完善网络认证的安全等级，另一方面也要修补软硬件的相关缺陷，主要涉及互联网的防火墙、路由器，操作系统的客户端，应用软件等。

2.2 网络病毒

网络病毒也是一种典型的外部安全威胁，主要以恶意网站、恶意软件为媒介，对计算机网络安全造成威胁，一般被设置于计算机上，在计算机启动后，利用网络进行传播，盗取个人和企业的信息和数据，获得盈利。结合网络病毒的发展情况来看，该类威胁的隐蔽性较强，在日常的使用过程中，难以发现潜伏的网络病毒，一些用户在访问互联网的过程中就默认进入了网络病毒程序，再加上网络病毒的传染速度非常快，往往会在短时间内扩散至多个计算机设备，进而造成巨大的经济损失。

2.3 非法入侵

一些不法分子利用系统漏洞进行非法入侵，是网络安全的主要威胁，主要体现为个人信息丢失、非法登录、传播病毒和拒绝网络服务等。结合以往的调研数据来看，数据信息失窃的重要原因在于非法入侵操作系统，随后盗取系统中的信息和数据，不仅会引发严重的信息和数据丢失问题，在入侵过程中也会对网络系统造成破坏，使得计算机陷入瘫痪。结合计算机数据信息管理系统来看，若不法分子进行数据的拷贝，通过抢占系统的数据库获得密钥和网关掩码，随后进行二次编程，实现对计算机网络系统的远程控制，在这个过程中，信息不会再紧密捆绑，而是大量泄漏，给用户造成巨大的损失。

3 数据加密技术在计算机网络安全中的应用分析

3.1 非对称加密算法

非对称加密算法的密钥通常为一对，一个密钥为公钥，另一个则为私钥，用户可以利用两者对数据和信息进行加密和解密，但是在后续的加密和解密过程中需要保障两者相对应，结合该算法的实际应用情况来看，私钥一般由领导进行保管，同时做好相应的安全防护，公钥则是在企业内部公开，供员工机进行正常使用，公钥可以在网络上传输信息和数据，而私钥只能对加密信息开展解密处理，该种加密模式，使得数据的传输过程实际上获得了双重防护，信息数据的安全性得到显著提升。结合该算法的实际应用情况来看，数据的发送方和接收方需要基于数据传输的安全性要求，设置相应的密钥，划分为公钥和私钥；接收

方需事前告知传输方公钥，在完成基础性的数据传输工作后，由接收方利用私钥进行解密工作，获得相应的明文（如图 1 所示）。

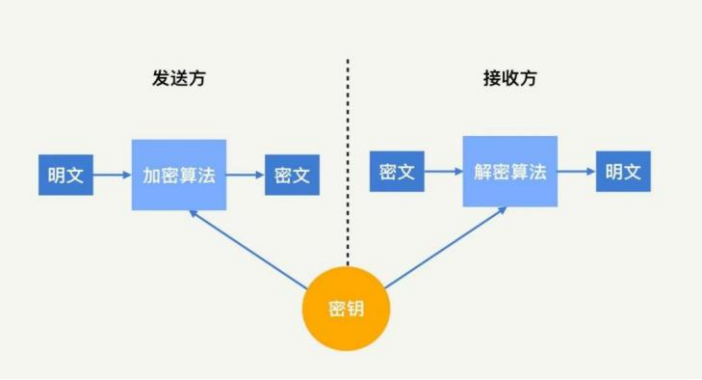

图 1 非对称加密算法原理

3.2 端到端加密技术

部分规模相对较大的企事业单位，日常的信息和数据传输量相对较大，为便于日常工作和生产，在企业内部构建了完善的局域网，这时可对端到端的加密技术进行应用，信息和数据在传输过程中借助加密算法加密信息，在数据信息未达到节电设备前并不会进行解密处理，对于提升数据信息的安全性有着较大帮助。同时，该种加密技术的应用成本相对较低，在互联网环境中也能够得到广泛的应用，可以避免在加密时的一些负面影响，得益于自身较强的适应性，是目前应用较为广泛的一类加密技术。

3.3 链路加密技术

节点是数据传输通道中的关键构成，也成为网络安全防护工作的关键技术，合理应用链路加密技术，能够对不同节点的信息数据进行加密和解密，信息数据的安全性大幅提升，便于后期信息数据的传输和处理。鉴于特殊的加密方式，该种加密技术也被称为在线加密，在加密的过程中会生成多个密钥，密钥的破译难度大幅提升，数据始终处于加密状态，为高度机密文件的传输创造了便利，整体安全系数相对比较高。但是结合该技术的实际应用情况来看，由于数据和信息长期处于加密和解密的状态，在无形中增加了网络的管理和性能负担，对于网络节点的性能来说是一项严峻的挑战。因此，如何实现加密与性能之间的权衡，成为该技术应用过程中的关键性任务。

3.4 对称加密技术

对称加密技术指的是信息数据的加密和解密过程采用的是统一密钥，具有一定的对称性，因此被称为对称加密技术，也是一种常见的数据加密方法，面对不同的应用场景，可以将对称加密技术细分为 IDEA，DES，AES 三种常用的加密算法，以 DES 为例，作为数据加密技术的一种常规算法，该算法利用 56 位密钥，可将信息划分为 64 位块大小，具有相对广泛的应用范围和应用效果，同时加密周期相对较短，面对一些较长、复杂的信息数据加密工作能够快速完成加密任务，符合加密工作的实际诉求。然而，该种加密技术也存在一定的弊端，譬如在加密过程中难以完成密钥的秘密分配，如果用户数量增加，消息确认问题难以得到有效的解决，在传输过程中容易出现密钥泄露的问题，因此，相关技术人员在后期的数据传输过程中要采取相应的防护措施。

3.5 节点加密技术

与链路加密技术的原理存在一定的相似之处，节点加密技术侧重对数据路径的加密，但节点加密技术不允许消息在网络节点以明文的形式存在，技术人员可以结合信息数据的传输器情况，在节点处设置专业的密码装置，对应的密文可在该装置中进行解密和加密，避免链路加密节点处受到攻击，进而为整个计算

机网络系统提供有效的安全防护，是该技术的一项显著特点，合理应用节点加密技术，能够在文本信息数据传输之前实现加密操作，使得信息和数据的传输成为一种密文传输的模式，同时不法分子的信息识别难度进一步提高，对于提升信息数据传输的安全性有着较大帮助。

4 IPsec VPN & SSL VPN 朋熙半导体分支互联和外出办公项目实践

4.1 项目概况

朋熙半导体公司是一家国内半导体 CIM 系统设计公司，总部设在中国上海。随着公司的业务不断扩展，需要实现总部与分支机构之间的安全互联和移动办公用户远程访问公司内部网络资源的需求。本项目涉及两个技术，分别是 IPSec 和 SSL VPN。IPSec 是一组开放的网络安全协议，为 IP 网络通信提供安全性。SSL VPN 是通过 SSL 协议实现远程安全接入的 VPN 技术。朋熙半导体公司通过使用这两种技术，实现了局域网安全互联和移动办公用户的远程访问。

4.2 技术目标

（1）IPSec 的目标是提供一种兼容 IP 协议的通用的网络安全方案，保障分支用户和总部业务数据在 Internet 中的安全传输。

（2）SSL VPN 的目标是满足企业出差员工和移动办公员工在外地远程办公的需求，并对移动办公用户进行身份认证和权限控制。

4.3 技术措施

（1）为了建立 IPSec 隧道来保护数据的安全性，需要一系列具体措施。首先，在通信的两端配置支持 IPSec 的网络设备，并确定 IPSec 策略，包括使用哪种安全协议、加密算法、认证算法和密钥长度等。其次，需要生成用于加密和认证的密钥，并配置 IPSec 隧道，包括将 IPSec 策略应用于通信的两端，并配置隧道的源 IP 地址、目标 IP 地址、隧道模式和隧道参数等。最后，在建立 IPSec 隧道之前，需要验证 IPSec 隧道的配置是否正确。AH 和 ESP 协议提供了认证和加密功能，密钥交换和用于验证及加密的算法也能够保护密钥的安全性，从而确保数据从分支到总部传输过程中不被篡改或窃取。如图 2 所示，各分支机构通过防火墙和总部建立点到多点的隧道访问总部 Server 资源。

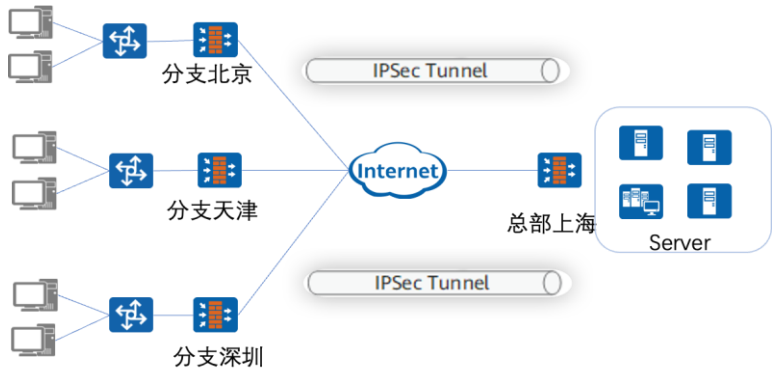

图 2 分支到总部 IPSec VPN 应用

（2）对于 SSL VPN，使用 SSL 协议实现远程安全接入，通过 SSL VPN 隧道加密访问企业内部资源。身份认证方式包括本地认证、服务器认证和证书认证。如图 3 所示，防火墙作为企业出口网关连接至 Internet，并向移动办公用户（即出差员工）提供 SSL VPN 接入服务。出差员工和移动办公用户使用终端（如笔记本、PAD 或智能手机）与防火墙建立 SSL VPN 隧道以后，就能通过 SSL VPN 隧道远程访问企业内网的 Web 服务器、文件服务器、网管服务器、KMS 服务器等资源。

图 3 移动办公 SSL VPN 应用

4.4 取得效果

通过使用 IPSec 和 SSL VPN 技术，朋熙半导体公司实现了局域网安全互联和移动办公用户的远程访问。这种组网方式有效地保障了数据传输的安全性，防止数据被篡改、泄漏或被恶意攻击。SSL VPN 的轻量级远程接入方案和精细化权限控制，提高了企业的安全性和效率，使员工能够在外地远程办公并访问内部资源。在疫情期间，SSL VPN 为保证信息安全和方便远程办公提供了有效的解决方案。它可以提高工作效率、降低成本并增强员工的协作能力。

4.5 案例意义

本案例对其他项目具有重要的借鉴意义：首先，应该将安全性放在首要位置，在设计和实施过程中采取相应的安全措施，保障敏感信息的保密性、完整性和可靠性。其次，通过多层身份认证和权限控制，可以提高系统的安全性，并根据用户的角色和需求设置相应的权限策略。此外，灵活的组网方式和移动办公支持也是值得借鉴的方面，可以根据自身需求选择合适的网络组网方式，为远程访问和移动办公提供安全、稳定的支持。综上所述，其他项目可以从本案例中借鉴并灵活应用相应的技术和措施，提升自身的网络安全性和工作效率。

5 结语

伴随经济社会的快速发展，计算机网络在人们的日常生活中发挥着日益重要的作用，为了实现对相关技术的有效利用，相关技术人员要加大对计算机网络安全的重视，针对不同的使用场景，选用合理的数据加密技术，关键在于紧跟行业和时代的发展脚步，对不同场景下的数据传输安全需求进行分析，进一步优化数据加密技术，并对以往的计算机网络安全管理经验进行总结，针对常见的计算机网络安全问题和非法攻击手段制定科学的应对策略，有效保障网络用户和计算机网络的安全，为我国经济社会的信息化建设营造良好的外部环境。

参考文献

[1] 李荣,夏天勇,张琪等. 论数据加密技术在计算机网络安全中的应用 [J]. 网络安全技术与应用, 2024, (01): 24-25.

[2] 胡冬阳. 数据挖掘技术在计算机网络安全管理中的应用研究 [J]. 软件, 2023, 44 (11): 184-186.

[3] 唐高阳. 数据加密技术在计算机网络安全中的实践探析 [J]. 软件, 2023, 44 (11): 85-87.

[4] 刘姜. 数据加密技术在计算机网络安全领域的应用分析 [J]. 电大理工, 2023, (03): 28-31.

[5] 吴凌云. 数据加密技术在计算机网络安全中的运用分析 [J]. 信息记录材料, 2023, 24 (09): 44-46.

[6] 闫军. 数据加密技术在计算机网络信息安全中的应用研究 [J]. 信息记录材料, 2023, 24 (09): 152-154.

【作者简介】

张津芳（1991-），男，汉族，上海朋熙半导体有限公司，中级，研究方向：网络应用、系统目集成；信息安全等。