数据加密技术在计算机网络安全中的应用分析

曲秀

（黑龙江省万文信息安全测评有限公司　黑龙江　哈尔滨　150000）

[摘　要]计算机的应用在人们的日常生活和企业发展中无处不在，成为人们商业办公、娱乐学习等工作和生活的无可替代的工具之一，在人类的科技发展、生产生活有着举足轻重、不可替代的低位。事有利弊，在便利生活和工作的同时，网络漏洞、病毒侵害、黑客入侵和服务器信息泄漏等安全问题也随之而来。因此，在当前网络安全技术开发中，确保数据的安全迫在眉睫。

[关键词]数据加密技术；计算机；网络信息；通信安全

【DOI】10.12252/j.issn.2096-6288.2021.05.183

1.数据加密技术发展概述

即使当前电子信息技术发展迅速，但仍存在诸多安全威胁、漏洞。因此数据加密技术应运而生。问题具体如下：首先，黑客崛起。黑客们有着不凡的计算机水平，通常以商业目的利用电脑系统存在的漏洞、后门发起进攻。如若在黑客攻击后没有及时发现并采取行动，那么他们依旧会藏匿在系统中威胁网络安全。如今，黑客们大多组成团伙，对社会运作、商业机密构成威胁，他们一旦攻击网络，危害程度极大。其次，计算机病毒。一旦受到病毒入侵，会导致整个区域内网络受到影响，甚至使区域内网络陷入瘫痪状态。例如附带型病毒、蠕虫病毒、可变病毒等等。最后，其他因素。例如计算机网络系统自身的脆弱性、社会工程学攻击、应用程序自身的设计缺陷等等，严重威胁着数据信息的安全。

2.数据加密方法

2.1对称式加密

对称加密算法指的是信息的收发两端使用同一密钥来进行加密和解析。信息的安全性取决于密钥保存的安全程度，因此，一旦密钥管理、传输的过程不安全，数据就十分容易被破解，并且难以保证数字签名功能的实现。即使如此，因为这种加密算法使用过程的便捷，还是得到广泛的应用。对称加密算法中常见的主要有以下三种算法。DES是分组加密算法的典型代表，特点就是较快速的处理速度，适用于大量数据需要加密时使用。3DES是对同一个数据分组利用不同的密钥进行3次DES算法迭代处理，提升密文安全系数。AES采用的是置换-组合架构，且AES算法相较于前二者，运算速度、资源使用效率以及安全级别都大大提升。

2.2非对称式加密

非对称加密技术在数据传输的过程中使用公钥和私钥分别进行加密和解密。公钥和私钥虽然不同，但是完全匹配，在加密过程、解析过程需要两个密钥互相配合。公钥通常被公开使用，但是私钥需要严密保管。该算法规避了因信息交流带来的数据安全威胁，从而保证数据的安全传输。非对称算法在实际运用中有着更便捷等优势，它有着两个密钥，公钥是被公开的，而私钥由专门的工作人员保管和运用。常见的非对称加密算法有RSA、ECC、D-H等。此外，本加密算法在身份认证、数字签名和证书等领域也得到广泛运用。

3.数据加密技术常见类型

3.1节点加密技术

该技术主要应用于数据的传输阶段，在数据节点进行解密-再加密。本加密技术是指在数据传输过程中，于数据节点处采用与节点机链接的安全模块，从而完成解密-再加密过程。从而规避数据解密时的安全风险，避免病毒入侵问题，从而提升数据传输安全性。

3.2链路加密技术

链路加密主要指对数据加以划分，在网络通信线路上使用加密技术对传输途径、存储区域进行反复加密解密，保证信息传输中用户信息、收发数据的安全。链路加密使用在最低协议层，加密的程度相对较弱，需要与其他加密技术相互配和提升加密效果。

3.3端到端加密技术

端到端加密技术适用于较为建议的信息传递中，对数据传输的途径、条件等均无限制，在收发两端之间采用点到点的网络安全控制。数据在发送端进行加密处理，在通信过程中已处于安全保护中，防止黑客侵犯。缺点是在传输过程中，如果信道受到干扰会影响数据的完整性，增加数据丢包的风险。本加密技术有着操作简单、节省传播流程以及利于维护的特点，因此也是常见的加密技术。

4.数据加密技术应用的应用场景

4.1在电子商务中的应用

电子商务涉及的网络安全风险多涉及经济利益和个人隐私，因此必须加大对数据安全的保护强度。电子商务平台需要加强对用户身份验证、密码保护、数据库防护、用户个人隐私保护、银行卡信息保护等措施的力度，建立多重标准保障数据安全。以淘宝举例，登陆账号需要密码或是短信验证，支付购买时需要提供支付宝的支付密码，网银用户需要银行卡密码或是U盾等安全认证设备。经过多重检验认证，消除安全隐患和漏洞威胁，对用户个人信息安全重重防护，提供优良的购物体验，保障公众经济财产安全。

4.2在局域网络中的应用

为保障企业的生产生活，大部分的企事业单位都采用构建内部的局域网络，保障内部办公需求和商业资料传输。将数据加密技术引入局域网安全保护措施中，保证数据在路由器、终端等设备之间传输的过程中由相应的安全机制进行加密和解密。保障数据传输过程中的安全性、完整性，保障企业机密不被黑客盗取、破坏，减少给企业带来不必要的经济损失。

4.3在软件加密中的应用

在人类生活中会用到形形色色的应用软件，功能也不尽相同：实时聊天、线上购物、浏览新闻以及视频观看等等。首先，利用杀毒软件扫描系统文件，及时发现病毒存在并且及时消除隐患，使得病毒失去对系统运行、数据传输进行破坏的机会，有效提高安全性。其次是数据签名技术的应用，用户需要利用口令、生物信息等正确的密码获得授权才可使用软件，配合使用登陆失败处理系统还可以提升系统防御能力。及时发现病毒入侵并处理，有效发挥杀毒软件的保护功能，减少系统安全风险，保障计算机信息安全。

5.结语

总之，在这个时代，各种技术手段为人们提供高效优质的服务的同时，也为网络安全带来种种风险。并且由于黑客频频入侵，计算机病毒和系统、软件漏洞事件频发，给互联网用户带来巨大风险。网络安全工程师们需要掌握数据加密的特点，研制对策，加强保密措施和力度、研制对策，提升网络安全系数，使得互联网能更好的服务于人类生活。

参考文献

[1]郭忠英，孙长春，崔俊，等.计算机网络通信安全中数据加密技术的应用[J].电子技术与软件工程，2017，18（04）.

[2]邹健，刘蓝田.计算机网络通信安全中数据加密技术及应用实践微探[J].网络安全技术与应用，2017，28（08）.

[3]罗潇.计算机网络通信安全中数据加密技术的应用研究[J].数码世界，2020（8）：256-257.