网络通信中的基本安全技术

戴　磊
北京云集智造科技有限公司　北京　100102

摘　要：如今网络已经成为当今全球数据通信的有效工具，它的迅猛发展对全球经济和社会生活都产生了巨大影响，网络安全技术的应用也非常广泛，促进了其发展。本篇文章介绍了网络安全的基本内容，详细分析了DES、RSA、数字签名、数字信封、密钥管理和CA认证体系等基本的安全技术。

关键词：网络通信；信息安全；安全技术

Basic security technology in network communication

Lei Dai
Beijing Yunji Zhizao Technology Co., Ltd. Beijing 100102

Abstract: Nowadays, network has become an effective tool for global data communication. Its rapid development has had a great impact on the global economy and social life. The application of network security technology is also very extensive, which promotes its development. This article introduces the basic contents of network security, and analyzes in detail the basic security technologies such as DES, RSA, digital signature, digital envelope, key management and CA authentication system.

Keywords: network communication; Information security; Safety technology

前言：

随着社会不断发展，互联网时代逐步进入大众视野，这使得用户在计算机中的信息和数据不断增多，对于网络安全的需求也不断提升。网络防火墙技术为内外网络建立实时的防护系统，对于网络安全技术而言，现如今已成为炙手可热专业技术，网络安全技术也促进了市场的我发展，其安全技术产品在市场中也占据的种重要地位，对于大部分应用网关而言，包含了过滤技术这种技术与网络安全技术相融合，体现出的应用价值远远大于单独使用。因此，在防火墙布置方面也需要进行相应的分析工作，安装防火墙时应将位置定位在公司内的网络和公司外的互联网接口上，阻止除企业外的人员利用网络对企业网络系统的入侵。随着企业规模的逐渐增大，对于网络安全系统也越发严格，设置好虚拟网络（局域网）并在自身企业的局域网中设置好防火墙进行应对外来入侵。企业的网络分为总网和支网，在总网络与分网络之间建立相互联系的防火墙系统。

作者简介：戴磊，1995，男，汉，技术经理，研究方向：软件工程管理。

1　加密技术

如今，网络已经普及到了千家万户，对于计算机安全也得到了高度重视，网络数据加密技术就是其中之一，由于加密算法涉及广泛，在强度方面也大不相同，现有的两种加密系统分为共享钥匙加密（对称钥匙加密）和非共享加密两种形式。

1.1 对称密钥加密

共享钥匙加密可以理解为私人共享要是加密，利用相同的钥匙进行对对称加密的解密。为此，对于数据和信息的收集者和发送者而言都应有一把同样的钥匙，在私人共享加密钥匙的系统中，相对于有一定权威的加密算法，是一种使用密钥匙的快算法（DES）。此加密算法是由国际商业机器公司（IBM）开发出来的，利用64比特钥匙和相应数据针对算法进行解密与加密。对于DES（一种使用密码钥匙的快速算法）进行多样化的操作模式，平时普遍使用的两种操作模式：分组密码的最基本操作模式简称（ECB）和加拿大广播网络（CBC）：电子密码本模型又可称为电子密码本型其原理是：将明文按分组密码的分组规模分成若干个分组，并将明文分组按照一定的顺序编号，每一个明文分组直接作为分组密码

算法（ECB）的输入。对于相同种的密码钥匙而言，在其控制下加密的到相应的密文组。所以很容易遭到“在破译密码时，逐一尝试用户自定义词典中的可能密码（单词或短语）的攻击方式简称字典攻击。出现解密错误或时其他问题时单纯影响目前的加密算法，并不能产生大范围的影响。对于西班牙（ES）语而言，它在加密技术的发展中起到了重要的作用。现如今，对于网络的安全更加严格，各加密技术专业人员对于安全性也进行了严格的分析，在细节方面缺少一定细致，随着一种使用密钥的快速算法开发出来，推动了快速算法的发展其功能在算法方面。

2 信息安全

随着网络行业的逐步发展，信息安全逐步进入大众视野，对于这方面的研究也在不断进行，对于信息安全而言从根本上讲是对重要的数据进行防护和加密，保护重要资料和数据不被泄露。从计算机问世到如今，互联网一直处于飞速发展阶段，如今计算机从局域网发展到可以连接千家万户的网络，对于计算机的使用也逐步大众化，信息安全技术是当今信息化时代的重要保障，随着网络遍布全球各地，这使得对于网络信息安全的概念逐步加深，对于数据安全来讲加密性和整合程度，完整性都是数据安全的相关概念，而对于使用者来说身份识别，各项授权和访问权限隐私问题等等，二者相结合才能体现出信息安全的本质，还需依赖认证技术，权限，修复功能，清理病毒，对黑客进行防护等等一些安全隐患的防护措施并进行解决处理。对于网络信息安全技术而言，我们熟知的网络防火墙技术就是其中之一和网络加密技术等等一些对于个人数据进行防护的，我们都称之为安全技术。对于网络安全技术可理解为保障网络系统硬件、软件、数据以及服务器安全进行采集的信息安全技术。随着网络时代的到来，在网络中网络安全技术对于用户的个人信息和个人隐私的保护具有很大程度上的保障，其中加密技术是网络安全技术不可而缺少的一部分。

3 身份认证技术

3.1 数字签名

对于数字签名而言，可以简单的理解为附加在数据单元上的一些数据，或是对数据单元所做的密码变换，也是信息运输过程中保证其完整性的关键信息安全技术，还可以进行信息发送者身份信息的认证这也是现如今网络的一种安全技术。

其优点是对于接收者而言可以更加方便的看见发送者的身份信息，保障了其数据的完整，在安全上数字签名具有一定的独特性，增强网络安全的发展。对于互联网而言，数字签名是电子商务重要的技术，其特点是防止他人对传输的文件进行破坏，以及确定发信人的身份。非对称密钥加密是数字签名的核心技术，这项加密算法包括两个加密数据的加密算法分别是：数字签名数据加密密钥另外的是保密加密算法，可以认定为使用单个私钥来加密和解密数据，还有一个是验证加密算法其具有一定的公开性。对于公开数据加密算法而言运算缓慢，需要利用SH进行对相应信息的处理，降低非对称密钥的运算。还可以利用函数算法进行加密，例如：散列算法它可以做到无法逆转的加密，在速度上更加理想，使网络安全得到保障。

3.2 数字证书和身份认证技术

现如今，在网络安全技术不断发展的同时另一个组织，也是我们熟知的“黑客”也逐渐诞生，这就使得不得不加强网络的密钥管理，对于这种参数而言，如果保护措施做的不够，就会遭到黑客的攻击造成不可估量的损失。所以对于这方面的保护是保障网络安全的重要措施。密钥管理是指管理加密密钥的密码系统，其中也包含一系列的流程。对于密钥这种参数而言，是现今为止在密钥管理方面，很容易出现问题，在这方面也是网络安全需要重视的安全问题。要想处理好这方面的问题，需要建立一个密钥管理系统，针对密钥这种参数，利用人工的方法给予每个用户传输一次密钥的方式，使用不同的通路加密密钥或是解密密钥进行对加密密钥的密码系统的管理[1]。用户在网络上使用一些软件时会弹出安全协议，其协议内容包含了用户的数据信息等，进行对用户的数据安全和对数据单元所作的密码变换的保存。CA指的是一串能够表明网络用户身份信息的数字，也是一种网络上验证用户身份的一种方式，对于这种验证方式的数字签名来所，外界因素并不能对其造成巨大威胁也不能进行伪造和更改，CA还可以进行对私钥的更新。

4 防火墙技术

随着网络时代的普及，计算机网络也遍布千家万户，用户对于防火墙的应用也逐渐产生依赖性，防火墙技术是一种综合性强，保护能力强的一种网络安全技术，防火墙技术也是网络安全技术的核心内容。防火墙也是一个由计算机的硬件系统和软件系统相互结合成的一种安全系统，安装在网络外部进行对网络的保障工作，还能对进出系统的各项重要数据进行时时保护，防止外来攻击等一些恶意入侵，从而起到保障网络安全的作用。随

着互联网安全指标的确立，也提供了相应的安全支持。防火墙技术作为网络技术和信息安全技术的基础，在网络的内外部（例如：因特网）相连接的边界上设立防火墙，因为在这里能够起到外来入侵的抵御作用。过滤作用也是防火墙的最大特征，起作用是对具有威胁的外来攻击的有效过滤。防火墙技术也包含四大类：1.包过滤性防火墙；2.应用级网关、电路网关与规则检查防火墙。防火墙技术在网络之间也是执行控制的一个系统，其保护的网络是可信任的网络，对于外界来说相对于内部，外部是具有一定威胁的，这也是防火墙过滤的本质所在，其用途是保障自身数据信息防止不被外界网络所使用和进行一定的恶意攻击。

4.1 状态检测技术

状态检测技术是计算机网络防火墙中来防止未经授权访问的一种技术，其原理在于通过连接的同一检测机制归纳成一个整体，进行连接状态的统计；利用每个人进入或离开的数据包和规则表格的互相协助，针对表格中出现的问题引述进行相应的辨别，对于网络安全系统而言，在形成网络保护时就会涉及到相应的成本问题，存有的资产不能高于最大损失的成本。例如：在系统中的数据信息的价值固定，那么其总的成本就不能高于这个固定值任何损失都包含在内。假如进行相应成本的估计，那么在网络安全的防火墙方面花费的成本应低于网络安全系统所花费的总成本。对于防火墙来说其自身就是一个保护屏障，但防火墙也是属于网络安全系统的一部分，所以它也应进行网络的时时防护，为网络安全系统带来相应保障让网络安全变的无懈可击。网络安全系统虽然看起来无懈可击，但是对于一些网络技术比较专业的人士来说，完全可以利用手段绕开防护系统，随后进行攻击[2]。所以对于防火墙一定要有严格的要求，但其自身的设计会导致一些普通使用者并不能对其造成威胁，只能依靠比较专业的相关部门和相关技术人员进行检测才能得到定论，在相关技术人员上也应进行培训，让其熟练掌握这项专业知识，以免在配置防火墙的过程中，导致网络系统漏洞百出。

5 安全技术的研究现状和动向

从计算机问世到如今的遍布全球，在网络信息安全方面启动早，涉及范围广，应用性强。现如今我们应用的软件，在使用前都会进行安全协议的同意事项，为保障用户的信息安全，该形式早在80年代就展露头角，现今为止虽然经过不断探索研究和分析出三类分析方法，但是仍无法达到预期效果仍然存在一定的缺陷，在这方面的研究仍然位于发展状态，还没有先进水平。近些年在国际上进行了不少网络安全技术方面的学术会议。在会议上各国先后提出了相应的研究意见，对于不同的加密密钥和解密密钥制度，在网络安全种的密钥的安全管理方面也得到了极大的改善，也解决了网络安全研究方面的重要问题。

随着社会经济的逐步发，现如今的社会已经离不开网络安全技术，对于商务类更是在企业发展中的核心技术，电子商务就是依赖网络安全技术发展的对象，随着信息化时代逐步覆盖，这方面的安全性也得到了更多人的重视。在这方面我们仍处在发展阶段，但是这方面的发展促进了密钥的安全管理方面的发展，随着计算的逐步加快，就不得不进行新密码制度的研究，现如今人们对这种新型密码仍处在不断摸索研究当中，随着网络发展的不断更新换代，对于网络安全技术这方面的发展也得到了高度重视，随着信息时代的更新交替，对于网络安全方面的需求越来越大，在步入信息化之后，对于这方面更应得到重视和研究，才能促进我国在这个领域的发展，现如今我国仍然处于发展水平还无法达到先进阶段，对于这方面的工作还需要我们进行不断地探索不断的研究，才能跟上时代进度，在网络安全技术发展中建立新的里程碑，这样才能促进经济的稳定快速发展[3]。

6 网络空间安全防御相关概念

想要让整个网络安全技术工程中更好的融入人们的生活，将整个工作更直观的展现在大众眼光中，那么就需要我们对整个工程的具体含义进行详细的阐述。

6.1 网络空间

网络原指用一个巨大的虚拟画面，把所有东西连接起来，也可以作为动词使用。在计算机领域中，网络就是用物理链路将各个孤立的工作站或主机相连在一起，组成数据链路，从而达到资源共享和通信的目的。凡将地理位置不同，并具有独立功能的多个计算机系统通过通信设备和线路而连接起来，且以功能完善的网络软件（网络协议、信息交换方式及网络操作系统等）实现网络资源共享的系统，可称为计算机网络空间[4]。

6.2 进攻性网络作战

所谓进攻性网络作战就是一种黑客行为，它通过破坏对方的计算机网络和系统，刺探机密信息达到自身的政治目的。现如今时代飞速发展，各国的相互联系也由网络而相联系，而现如今出现了一些破坏网络安全的系统，这种系统具有十分强大的侵略性，一旦设定好目标对象，那么第一时间就会让其系统瘫痪，这就是当代的

一种战争形式。

6.3 网络防御

网络安全防御是一种网络安全技术，指致力于解决诸如如何有效进行介入控制，以及如何保证数据传输的安全性的技术手段，主要包括物理安全分析技术，网络结构安全分析技术，系统安全分析技术，管理安全分析技术，及其它的安全服务和安全机制策略。

6.4 网络态势感知

态势感知是一种基于环境的、动态、整体地洞悉安全风险的能力，是以安全大数据为基础，从全局视角提升对安全威胁的发现识别、理解分析、响应处置能力的一种方式，最终是为了更好的方便决策与行动，是安全能力的落地。

7 发展趋势与展望

现如今网络发展速度在日益变快，各种维持网络安全的防火墙也在逐渐更替。因此想要更好的维护整个网络的安全进行，就需要我们每一个工作人员的共同努力，这样才可以才众多网络发达的领域里崭露头角。想要使网络安全管理系统变得更加完善，就要选择新的接入途径，进行储存网络信息管理档案的应用和把每一个档案进行重新排序，从而进一步的把人们的各类要求逐个完成。怎样让自己对人工智能有个正确的认知是我们现如今存在的大问题，一部分教授觉得把帮助人们学习和思考方面的效果放大，这样不仅仅有利于人们的科技进步，还可以提升学习的效率和利用率，在当今社会时代的发展速度下要利用最基础的档案将总体全部改变，包括档案的检测，档案的利用和每一份档案应具有的作用都应该发生新的改变[5]。由于时代的发展网络安全技术在当今社会的利用也越来越广泛了起来，每一位员工利用自身对网络安全的技术还是研究整体的管理方面的新方案都可以让自身的技能熟能生巧。

8 结束语

随着网络时代的到来，网络安全问题也逐步得到重视，防止外来入侵、保障用户的信息安全等等都是我们现如今应考虑的问题，随着防火墙技术和各项加密技术的不断发展，网络安全安全技术定会突飞猛进，伴随着人们对于这个领域的不断探索不断研究，定会完善网络安全技术，从而推动网络安全技术的飞速发展。

参考文献：

[1]蔡双进.网络通信中的基本安全技术[J].网络技术安全与应用，2019（02）：19-20.

[2]张耀东，张娴静.网络通信安全中的基本安全技术[J].网络技术安全与应用，网络技术安全与应用，2020（06）：42-43.

[3]刘斌.网络通信中的基本安全技术[J].网络技术安全与应用，2020（08）：33-36.

[4]宋韧.网络通信中的基本安全技术[J].网络安全技术与应用，2019（08）：28-28.

[5]李红超，田有朋.网络通信中的基本安全技术[J].数字技术与应用，2019（6）：188-188.