# 密码学在网络信息安全中的应用

张 靖[1],薛 冰[2]
(1. 河南工业大学 河南郑州 450052 2. 平顶山工学院计算机系 河南平顶山 467000)

【摘 要】:现代计算机网络面临着信息泄露、黑客攻击、病毒感染等多种威胁,使用密码学可以保障信息的机密性和完整性,防止信息被篡改、伪造。本文概括介绍了密码学在现代网络信息安全体系建设中的地位,同时对如何合理的利用密码学技术来保障网络信息安全进行了分析。

【关键词】:密码学;信息安全;数字签名

## 1. 引言

信息网络国际化、社会化、开放化和个人化的特点,决定了它在给人们提供高效率、高效益、高质量的"信息共享"的同时,也投下了不安全的阴影。随着政府和人民对网络环境和网络资源依赖程度的不断加深,信息泄露、黑客入侵、计算机病毒传播甚至于威胁国家安全的问题会出现得越来越多。

密码技术作为保障信息安全的核心技术,在古代就已经得到应用但仅限于外交和军事等重要领域。目前随着现代计算机技术的飞速发展,密码技术正在不断向更多其他领域渗透。密码技术不仅能够保证机密性信息的加密,而且完成数字签名、身份验证、系统安全等功能。所以使用密码技术不仅可以保证信息的机密性而且可以保证信息的完整性,还可以防止信息被篡改、伪造和假冒。

## 2. 网络信息安全问题

网络与信息安全是一个综合、交叉的学科领域,要涉及到安全体系结构、安全协议、密码理论、信息分析、安全监控、应急处理等各个方面,还要利用数学、电子、信息、通信、计算机等诸多学科的长期知识积累和最新发展成果。信息安全要综合利用数学、物理、通信和计算机诸多学科的长期知识积累和最新发展成果,进行自主创新研究,加强顶层设计,提出系统的、完整的,协同的解决方案。

网络信息安全面临的威胁是多方面的,具有无边界性、突发性、蔓延性和隐蔽性等新的特点。网络模糊了地理、空间上的边疆概念,使得网上的冲突和对抗更具隐蔽性。对计算机网络的攻击往往是在没有任何先兆的情况下突然发生的,而且会沿着网络迅速蔓延。对网络信息安全防御的困难还在于,一个攻击者仅需要发起一个成功的攻击,而防御者则需要考虑所有可能的攻击;而且这种攻击是在动态变化的。因此,仅从技术上解决网络信息安全是有一定风险的。

国际标准化组织(ISO)将"信息安全"定义为:为数据处理系统建立和采取的技术和管理的安全保护,保护计算机硬件、软件数据不因偶然和恶意的原因而遭到破坏、更改和泄露。简单说,信息安全的基本属性有可靠性、保密性、完整性、可用性和可控性。

信息保密性是指信息不被泄漏给非授权的个人和实体,或供其使用的特性。信息的保密性包括文件的保密性、传输过程中的保密性等两个方面。

信息的完整性是指信息在存储或传输时不被修改、不被破坏,不被插入、不延迟、不乱序和不丢失的特性。

信息可用性是指信息可被合法用户访问并能按要求顺序使用的特性。

信息可控性是指授权机关可以随时控制信息的机密性。每一个用户只能访问自己被授权可以访问的信息。同时对系统中可利用的信息及资源也要进行相应的分级,确保信息的可控性。

信息的可靠性是指以用户认可的质量连续服务于用户的特性。这不仅是要保护信息的安全可用,还和信息系统本身的可靠性有关。

实际上不论是局域网还是广域网,都是一种系统,所以系统安全问题的解决,必然是一项系统工程,必须采用系统工程学的方法、运用系统工程学的原理来设计网络信息安全体系。解决网络信息安全的基本策略是技术、管理和法制并举。技术是核心,要通过关键技术的突破,构筑起国家信息安全技术防范体系。管理是关键,根据"木桶原理",信息安全链条中任何一个环节的脆弱都有可能导致安全防护体系的失效,必须要加强各管理部门和有关人员间的密切合作。法制是保障,通过建立信息安全法规体系,规范信息化社会中各类主体的行为,以维持信息化社会的正常运作秩序。

## 3. 密码是解决网络信息安全的关键技术

网络环境下信息的保密性、完整性、可用性和抗抵赖性,都需要采用密码技术来解决。密码技术是信息安全技术的核心,它主要由密码编码技术和密码分析技术两个分支组成。密码编码技术的主要任务是寻求产生安全性高的有效密码算法和协议,以满足对消息进行加密或认证的要求。密码分析技术的主要任务是破译密码或伪造认证信息,实现窃取机密信息或进行诈骗破坏活动。这两个分支既相互对立又相互依存,正是由于这种对立统一关系,才推动了密码学自身的发展。目前人们将密码理论与技术分成两大类,一类是基于数学的密码理论与技术,包括公钥密码、分组密码、序列密码、认证码、数字签名、Hash函数、身份识别、密钥管理、PKI技术、VPN技术等;另一类是非数学的密码理论与技术,包括信息隐藏、量子密码、基于生物特征的识别理论与技术等。

网络信息安全体系的构建要求我们必须合理的使用多种密码技术,这样才能保证信息的可靠性、保密性、完整性、可用性和可控性。

### 3.1 使用信息隐藏和公钥密码、分组密码等密码技术保证信息的保密性。

信息隐藏对于在网络中保护信息不受破坏起到重要作用,信息隐藏是把机密信息隐藏在大量信息中不让对手发觉的一种方法。主要侧重于隐写术、数字水印、潜信道、隐匿协议、可视密码等方面的理论与技术的研究。

### 3.2 使用HASH函数保证信息的完整性。

Hash函数(也称杂凑函数或杂凑算法)就是把任息长的输入消息串变化成固定长的输出串的一种函数。Hash函数主要用于完整性校验和提高数字签名的有效性,目前已有很多方案。这些算法都是伪随机函数,任何杂凑值都是等可能的。输出并不以可辨别的方式依赖于输入。

### 3.3 使用数字签名和各种身份验证技术保证信息的可控性。

数字签名是对电子形式的消息签名的一种方法。基于公钥密码体制和私钥密码体制都可以获得数字签名,特别是公钥密码体制的诞生为数字签名的研究和应用开辟了一条广阔的道路。关于数字签名技术的研究,目前主要集中在基于公钥密码体制的数字签名技术的研究。数字签名的研究内容非常丰富,主要有RSA数字签名算法、ElGamal数字签名算法、椭圆曲线数字签名算法和有限自动机数字签名算法等。数字签(下转第66页)

分布在世界各地计算机的计算能力。

3. P2P技术的发展

P2P技术经过多年的发展和演进，其蕴含的巨大的创造力和应用前景已经逐步展现，正吸引越来越多的企业投入到这方面的研究和应用中。但P2P技术还不十分成熟，还有亟待完善的问题，如标准不统一、管理困难、安全和信用存在隐患等，这些问题制约了P2P技术的发展空间和应用范围。如果将这些问题进行划分又可以划分为技术方面的问题和非技术方面的问题。其中非技术方面的问题的解决比技术方面的问题的解决难度更大些。

㈠ 网络安全问题

"网络安全"是P2P技术应用所面临的一个重要的技术性问题。P2P模式弱化了服务器的功能，对资源共享的管理相对较弱，传统的安全防范措施不能起到应有的作用，使得P2P网络的安全性变差。大多P2P软件在进行节点之间的访问时需要打开特定的端口来实现，该操作往往能够绕过防火墙，进而使防火墙产生漏洞；P2P网络通信往往可以避开网络周边安全防御设备，实现点对点的直接通信，同时使得防病毒网关无法发挥作用。P2P网络上的节点从其他节点上下载的文件绕过了防火墙、防病毒网关的监控，使得下载文件的安全性大大降低。安全漏洞使本来可以为客户提供便捷、大范围的资源共享的方式也同样可以给病毒及其他不安全信息的传播开辟新的路径。对于这类问题的解决核心在于对于开放端口的审核及对信息的检验。

㈡ 网络管理问题

在"网络管理"问题上，P2P技术最主要体现在对不良内容的传播控制和数字版权两个方面。对不良内容的传播控制除了使用屏蔽等技术加以防范外，更多的需要规范个人上网行为，但这种非技术的控制会更为复杂。在版权管理方面，数字版权管理(Digital Rights Management, DRM)是一种较可行的手段。DRM可以对数字产品在分发、传输和使用等各个环节进行控制，使得数字产品在分发、传输和使用等各个环节进行控制，使得数字产品只能被授权使用的人按照授权的方式在授权使用的期限内使用。但技术并不能解决所有问题，相关法律手段的加强也是十分必要的。法国议会通过的一项名为《信息社会著作权法及相关条例》的法案，规范了个人从互联网上下载的权限，并明确禁止非法出售下载的受版权保护的产品。[3]

㈢ 标准问题

P2P技术涉及到的标准问题有开发平台规范标准化和P2P业务标准化。不同的P2P系统具有不同的应用背景和应用类别，由于这些P2P系统都是在不同的平台上开发出来的，所以相互之间不能通信。现在在P2P平台开发中，由Sun推出的JXTA是最为看好的，有望成为P2P系统开发的标准平台。P2P业务标准化是由于P2P技术的应用使得网络宽带数据流量增加，而运营商却不增收的基础上提出来的。按照流量统计数据，目前P2P应用占带宽流量的50%~60%(白天)到90%(晚上)。数据流量的增加和入网用户的增加，而运营商的收入却没有在此基础上得到相应的增加。有的运营商想采用封锁BT下载等手段来改善现状，但并没有取得预想的效果。网络电话Skype也遭到中国电信的软件屏蔽，被视为"非法业务"。我国于2005年10月在北京成立了中国互联网协会宽带P2P应用推进联盟，旨在针对宽带"点对点"文件传输技术及其应用进行研究、跟踪、探讨、推广等工作，为P2P技术今后的统一规划与良性发展构建基础平台。

4. P2P技术前景

尽管P2P技术的发展还面临诸多的问题，其不断扩大的用户量仍表明它的远大前景。基于P2P技术的网络电视、网络电话也正在互联网上迅速发展。P2P技术的应用领域也在不断得到扩展，今年我国的P2P联盟将在教育、音乐等领域进行试点，以试探与传统产业相融合的机会。随着日后各种标准的出台和完善，P2P技术的应用范围将进一步扩大，发展前景也会越来越好。

**参考文献：**

1. 王大锋，刘在强，冯登国.P2P即时通讯软件监控系统的研究与实现[A].计算机工程与应用,2005.10,129-144
2. 李阳明，王丽芬，郭慧.P2P对等网络的关键技术.现代计算机,2005.8(217),50-52
3. 杨骏.法国通过新法案规范个人网上下载行为.新华网.2006-3-22
4. 王艳丽，鲜继清，白洁.基于P2P的流媒体技术[A].计算机应用,2005.6(25),1267-1270
5. 何卓如,P2P技术及其在信息检索中的应用[A].广东广播电视大学学报.2005.2(14),20-26

(上接第75页)

名的应用已经涉及到法律问题，美国联邦政府的部分州已制定了数字签名法，一些国家如法国和德国也已经制定了数字签名法，我国的电子签名法也在2004年颁布。

3.4 使用PKI和VPN保证信息的可靠性及可用性。

简单的说，PKI技术就是利用公钥理论和技术建立的提供信息安全服务的基础设施。PKI是解决信任和加密问题的基本解决方案，本质就是实现了大规模网络中的公钥分发问题，建立了大规模网络中的信任基础。PKI是创建、管理、存储、分发和撤消基于公钥加密的公钥证书所需要的一套硬件、软件、策略和过程的集合。PKI为开放的Internet环境提供了四个基本的安全服务：

(1) 认证，确认发送者和接收者的真实身份；

(2) 数据完整性，确保数据在传输过程中不能被有意或无意地修改；

(3) 不可抵赖性，通过验证，确保发送方不能否认其发送消息；

(4) 机密性，确保数据不能被非授权的第三方访问。

另外，PKI还提供了其他的安全服务，主要包括以下两个：

(1) 授权，确保发送者和接收者被授予访问数据、系统或应用程序的权力；

(2) 可用性，确保合法用户能正确访问信息和资源。

VPN是利用接入服务器(Access Server)，广域网上的路由器或VPN专用设备在公用的WAN上实现虚拟专网的技术。也就是说，用户觉察不到他在利用公用WAN获得专用网的服务。如果强调其安全性，可以认为VPN是综合利用了认证和加密技术，在公共网络(比如Internet)上搭建一个只属于自己的虚拟专用安全传输网络，为关键应用的通信提供认证和数据加密等安全服务。如果将VPN的概念推广一步，我们可以认为凡是在公共网络中实现了安全通信（主要包括通信实体的身份识别和通信数据的机密性处理)的协议都可以称之为VPN协议。到目前为止，VPN已经在网络协议的多个层次上实现，从数据链路层、网络层、传输层一直到应用层。特别是IPSec标准的制定，对实施VPN奠定了坚实的基础。

4. 结束语

我们必须正确理解密码学在网络和信息安全中的地位。密码技术仅仅是解决信息和信息系统安全的关键技术之一，单靠密码技术不能彻底解决信息和信息系统的安全问题，安全问题涉及到人、技术、管理和操作等多方面的因素。安全系统的防御等级遵循"木桶"原理，取决于其最薄弱的环节。总而言之，在解决信息和信息系统安全这个问题上，密码技术不是万能的，但离开密码技术是万万不能的。

**参考文献：**

1. 杨明，谢希仁，等.密码编码学与网络安全:原理与实践(第二版)[M].北京:电子工业出版社,2001.
2. JessGarms,DanielSummerfield.ProfessionalJavaSecurity[M].北京:电子工业出版社,2002.
3. STEVE B, STEPHEN B.Cryptography [M].New York:McGraw-Hill, 2001.
4. 冯登国.密码分析学[M].北京:清华大学出版社,2000.
5. 王育民，刘建伟.通信网的安全-理论与技术[M].西安:西安电子科技大学出版社,1999.
6. 孟博，熊丽，陈浩然.基于PKI的电子商务安全研究[J].计算机工程与应用,2002,38(11):152-155.