网络安全与数字签名技术

摘　要

数字签名也称电子签名，digital signature，是给电子文档进行签名的一种电子方法，是对现实中手写签名的数字模拟，在电子商务的虚拟世界中，能够在电子文件中识别双方交易人的真实身份，保证交易的安全性、真实性及不可抵赖性的电子技术手段。实现电子签名的技术手段有很多种，但目前比较成熟的、许多先进国家普遍使用的电子签名技术还是数字签名技术，它力图解决互联网交易面临的几个根本问题：数据保密、数据不被篡改、交易方能互相验证身份、交易发起方对自己的数据不能否认。数字签名技术在其中起着极其重要的作用，如保证数据的完整性、私有性和不可抵赖性等方面，占据了特别重要的地位。目前群盲签名（blind signature ，group signature）方案效率不高，这样的电子现今系统离现实应用还有一段距离，因此研究高效的群签名方案，对于实现这样的系统具有重要意义。

关键词：数字签名，网络安全，blind signature，group signature

ABSTRACT

Digital signature, also known as electronic signature, is an electronic method of signing electronic documents. It is a digital simulation of handwritten signatures in reality. In the virtual world of e-commerce, it is an electronic technical means that can identify the real identities of both parties in electronic documents and ensure the security, authenticity and invincibility of transactions. There are many technical means to realize electronic signature, but the electronic signature technology that is relatively mature and widely used in many advanced countries is still the "digital signature" technology, which tries to solve several fundamental problems faced by Internet transactions: data confidentiality, data can not be tampered with, transaction parties can verify their identities with each other, and transaction initiators can not deny their own data. Digital signature technology plays an extremely important role in it, such as ensuring the integrity, privacy and non repudiation of data, and occupies a particularly important position. At present, the efficiency of blind signature (group signature) scheme is not high. Such an electronic system today is still a long way from practical application. Therefore, it is of great significance to research an efficient group signature scheme for implementing such a system.

Keywords: digital signature, network security, blind signature, group signature

目　录

第一章 引言

Internet 是世界最大的国际性计算机互联网，此外，而且也是有着技术专长的一些人比较严重肇事者目标。各种入侵者，包含员工、“网络黑客”、极端组织、以政治和军事机密为目的的其他国家政府部门、从业工业生产特工活动的世界各国公司等，给计算机和电信系统导致巨大威胁。他们千方百计地闯进技术性应用系统，盗取各种各样情报信息，打探私人信息，用于进行一定的行骗活动。

每每开通一个新 Internet 进出口、LAN 或分布式系统客户网站服务器时，便冒着为入侵者打开一道方便之门的危险性。计算机泄密已变成当今社会高新技术违法犯罪关键方式。据美国信息周刊/Ernst&Young 网络信息安全私人侦探最新发布的统计分析，在 90 年代，美国每五个公司中就有一个遭受侵入，使有关部门遭受无法估量损失。美国传媒界把数据信息遭窃揶揄地称之为“数据珍珠港”或“数据福岛核事故”。联邦政府司法机关的大臣可能，每一年美国的联机窃贼从计算机网络盗窃数据的价值在一百亿美元之上。

最大程度地降低黑客攻击的次数影响并不是不太可能，却也绝非易事。在行为上，维护数据信息决心离不开安全工作单位的安全性认同和强有力适用：从技术上，必须符合多个运维安全总体目标[1]，主要包含：

(1)务必避免违法泄露上传的信息内容；

(2)务必检验得到对发送短信的违法篡改或销毁；

(3)务必避免每一个订单量分析攻击；

(4)务必检验得到每一个服务项目赖账进攻和假关系复位进攻(Spurious association initiation attack)。

达到前三个目标唯一有效的方法是数据加密。实际上，数据库加密这是所有运维安全依靠的基础技术。

第二章 信息网的安全问题

2.1 网络的安全威胁

2.1.1 外部威胁

（1）闲游用户的好奇心闯入：因为的好奇心的迫使，闲游用户很有可能有心无意地闯入了全面的内部网络，他们也许根据相关方式获得了内部网络合理合法用户的账号及登录密码，也可能是因为网关 ip 配置不科学让她们无意中闯入内部结构网络的。在她们赢得了浏览以后，他可能会在内部网络各清单中四处乱冲，以探寻有兴趣的文件或信息，而威胁合理合法用户的正常运转及数据资料的安全与应用系统的安全性。他们也许有心无意地更改了关键性的安装文件、删掉了关键性的信息数据信息，导致了数据库的遗失，更改了一些数据库的具体内容等。

（2）信息特工的故意闯入：信息特工经常受聘于某一组织，主要从事信息的盗取工作中，具备精湛的互联网专业技能，他们通过不正当手段的方法进入你企业内部网。他们也许对你的企业查询怀着巨大的热情，或者专业来损坏你公司信息网，让你的信息网处在麻痹，进而为竞争对手燕得获得胜利的好机会。这群人很有可能根据侵入你互联网上的一台计算机或者使用信息包采样器来浏览你企业的信息、根据信息包采样器能够捕捉一切经过 Telnet 上传的数据信息，并且通过捕获 Telnet[2]。对话监听合理合法用户 ID 和动态口令而得到对你的互联网的浏览。

（3）怀着故意用户的闯入：这种用户很有可能对你的部门心存妒忌或是她们对你的公司怀着居心报仇的心态，根据不正当手段的路径闯入公司的内部网络。并故意地删掉有意义的数据库文件及安装文件，使数据信息完全损失或系统软件处在麻痹，等着你察觉时，已为时过晚仅有再次从系统备份和信息中进行修复。无意用户的故意损坏：这种用户很有可能后台运行自己并不适应的配置应用软件或网络服务器及自创程序，在无意中给你互联网导致了威胁。如 1987 年美国宾夕法尼亚大学（Cornell University）学生们 Robert T。Morris 编制蠕虫程序流程 (Internet worm)，Morris 的妄图使创建一个能静静地在 Internet 上拷贝它本身程序，便于论述电子计算机安全防范措施不合理，但是他的蠕虫程序流程拷贝地比他规划的要立即得多，并促使全部蠕虫程序流程传染的系统软件处在崩溃及冻结，促使全部美国的管理人员专注于防护该程序流程，以便它终止蔓延[3]。

2.1.2 内部威胁

（1）内部结构用户有意的安全性威胁：内部结构的安全性威胁较难提防或操纵，因为这种威胁来源于网络内部结构网络的合理合法用户。她们可能会对内部结构网络中别的用户组里的数据有兴趣或者想盗取别的用户组里有意义的数据，如高校网络里的学生及老师常共享用户的 ID 和指令，一些学生登录手机上网后，喜爱毁坏他人创建的数据，有些学生妄图浏览智能管理系统以修改他的考试成绩记录。

（2）无意用户的安全性威胁：除开内部结构用户有意盗窃数据与对数据毁坏外，另一类内部安全威胁来源于用户的应用缺乏安全意识，他们也许在不安全的安全通道中传输企业的保密信息，或把一些适宜企业安全生产的低息贷款数据储放到 Internet 的 Web 或 FTP 服务器上，或是她们无意将企业的用户账号及登录密码泄露给外界公司的用户，而给内部结构网络的安全性形成了威胁[4]。

2.2 信息网络的安全性

互联网的信息安全性经常由数据安全性和通讯安全性两个部分组成。通讯安全性是一种设备维护，规定在电信网中选用信息保密安全性、传送安全性、辐射源安全性等举措，而且规定针对通讯安全性信息采用物理学安全性对策，以回绝非授权客户在电信网中获得有意义的信息[5]。数据安全包括信息数据的完好性保密性和可用性。数据的保密性指皮内瘤信息仅仅在授权前提下流入低等其他行为主体与主体；数据的安全性指信息不被非授权客户改动及信息维持一致性等；数据的可用性指合理合法客户的正常的要求能够及时、恰当，快速地获得服务项目或回复。网络系统的安全性受影响后经常也会导致网络系统不能提供正常服务项目，或者互联网信息网络资源被变更乃至销毁，或者信息的泄露等。

2.2.1 网络的安全系统

网络的安全性系统是指应用硬件配置及系统等安全防范措施产生好几个防护层，以保障他们所围绕的计算机数据资源的安全性，外场的安全级别比较低，而里层的安全等级比较高。网络的安全防范措施与网络的灵便、方便快捷往往是彼此冲突的。从数据安全性而言尽可能对信息进行多层维护，以产生网络信息安全的双层操纵。从客户的灵巧应用而言，则期待网络的构造与技术尽可能简约，不引入额外操纵要素与资源开销。完成各种各样附带的安全配置不仅要消耗有限的资源网络资源与限定网络网络资源的应用，与此同时必须投入额外硬件配置、手

机软件及网络运行维护的附加投入，确保网络的安全性也是有代价的。

一个优秀的网络防护系统须是建立在网络的应用性能安全保障措施之间的一个最好均衡点上，使网络安全防范措施所引入的附加开销和它所产生的经济效益相当。

2.2.2 网络安全的安全点设置

信息数据信息在传输时、从哪里开始到何处完毕的解读对联安全机构制订具有一定的实际意义。网络安全性服务项目需要由 OSI 模型的绝大多数层给予。常见的安全措施也有在路由器上提升 IP filtering 作用，运用网关 ip(Appliation gateway)，客户的身份认证(Authertication)、密钥管理(Access Control)，信息的加密和解密及电子签名等。现阶段最常见两种安全措施为网络防火墙和信息数据库的加密技术。入侵检测技术较适用于相对独立性、与外界网络互连方式比较有限而且网络服务类型相对性集中化单一的网络系统软件，网络防火墙型安全性系统运维相对性非常简单，它通常只能在网络界限上有着安全防范措施作用，实际法律效力范畴相对性比较有限。而数据库加密为核心的防护系统是一种较适用于 Internet 网互联的安全技术，Interne 网是一个开放性的软件，选用数据信息加密技术大部分是一种开放型安全技术[6]。它对于网络服务产生的影响非常小，是未来网络安全防范措施的重要方式之一。

2.3 信息安全技术发展趋势

伴随着电子计算机和网络技术的迅猛发展，相关信息安全性技术愈来愈获得重视。这种安全性术主要包含以下几方面：

2.3.1 加密

数据加密应该是传送过程的信息进行维护的主要方式，也是对存放于系统中各新闻媒体中的内容进行维护的一种合理方式。信息安全性也是我们的终极目标，而数据加密是促进这一目的合理又不可缺少的技术方式，也是最重要的技术之一。

2.3.2 鉴别

鉴别技术可以解决信息交换过程的合理合法、实效性及信息真实性问题关键技术能够防止对信息开展有心伪造的主动进攻。鉴别技术的同一性是对于某些主要参数实效性开展验，亦即查验这种主要参数是否符合某类预先确定之间的关系。密码学一般可以为鉴别技术提供一种较好的安全保证，日前鉴别方式大部分都是以密码学为核心的。常见的鉴别技术主电子签名、报文格式鉴别和真实身份鉴别。

2.3.3 访问控制

访问控制技术是信息系统内要明确容许进出的消费者对什么信息网络资源具有哪种管理权限以开展哪种类型的浏览实际操作，并避免违法客户登录系统和合理合法消费者对信息网络资源非用。执行访问控制是维护保养信息系统优化，维护信息资源关键技术方式。

除了上述三个方面外，也有网络防火墙技术、防电磁感应泄漏等安全技术。而上面这些技术绝大多数跟登录密码技术的应用紧密联系。登录密码不但适用通讯的安全性，并且便捷验证身份（实体线鉴别）、确保通信信息安全性（报文格式鉴别）、容许在互联网上完成安全验证（若干名）等[7]。登录密码技术是安全性技术的关键。事实上，它这是最经济发展切实可行的方式，它促使诸多潜在性不安全的环境里确保通信的安全性。

登录密码在军队行业一直获得广泛运用，数据库加密规范（DES）和公钥密码制度的定下了近现代密码学基本促使它运用更为普遍，它成为了获得网络安全性的一种最大的方式。特别是在军工用互联网的快速发展，强制要求保证在网络上信息的安全性、数据完整性和真实有效它更奠定密码学在国防里的举足轻重的地位。电子签名及认证均是由近现代密码学衍生出的新技术与应用，早就在电商、电子邮箱、金融系统、政府部门协同办公系统等多个方面获得运用，他在信息安全生产方面所具有的重要意义逐渐得到大家的高度重视，在国防里的运用必将造成高度关注。