文章编号 1004-924X(2000)06-0589-04

网上档案信息的安全及保密技术

杨洪波[1], 袁雅珍[1], 王洪伟[1], 吴登奎[2]
(1. 中国科学院长春光学精密机械与物理研究所, 吉林 长春 130021;
2. 吉林省档案科学技术研究所, 吉林 长春 130055)

摘要: 档案信息上网在我国已是大势所趋, 本文综述了档案信息上网所面临的一个重要课题, 即网上档案信息安全保密问题。分析了档案信息在网上传输过程中存在的安全隐患, 介绍了主要的安全防范技术措施和网上档案信息管理所要注意的问题, 重点介绍了档案信息加密通信技术手段, 提出了建立档案信息完整的档案信息网络安全体系的基本框架, 为档案信息上网工程的建设提供了一定的参考。

关 键 词: 档案; 网络信息; 网络安全
中图分类号: TP393.09 文献标识码: A

1 引 言

档案信息上网问题是我国档案界一个跨世纪的议题。近几年中, 随着我国政府办公自动化和上网工程的逐步实施、各级政府部门的政务信息网已经陆续开通。由于档案信息网络化的实现, 可使众多的用户利用互联网络直接查找档案馆的馆藏目录, 利用远程登录能直接调用档案, 档案利用服务模式也从传统的手拿介绍信, 亲自到馆内查询变为馆外网络查询、远程服务。目前全国各级各类档案部门已有各种型号微机5000多台套, 已形成的电子档案也越来越多, 这都为档案信息上网奠定了坚实的基础。因此, 档案部门上网也就被提到各级档案部门的议事日程上来。各级档案局(馆)在互连网上纷纷建立网点, 进行信息发布, 这已成为广大档案工作者的共识。据有关人员统计, 截止到1999年底, 我国能够查到的档案网站约有20个左右。其中省级档案机构上网的有北京、安徽、海南、四川、河北、天津、吉林、山东等省、市。它们从网页制作到内容结构等都各不相同。其中较有特色的有北京、安徽、海南、四川、河北, 而设有主页的只有北京市档案馆、安徽省档案馆。其余, 大多数档案部门还没有上网或没有主页。究其原因, 除了资金困难等原因外, 许多人对档案信息上网持慎重态度, 主要是担心档案信息上网可能会危及其安全保密问题。如何解决档案信息上网安全、保密措施, 已成为档案部门一个迫在眉睫的重要问题。

2 档案信息易遭到攻击的主要方面

2.1 黑客的恶意攻击

黑客利用高技术手段非法侵入远端的计算机系统, 以达到窃取政治、军事、经济机密, 或个人隐私的目的。目前, 就连保护技术最先进的美国国防部的电脑系统也曾被各地的"黑客"多次拜访。据美国FBI的调查, 美国每年因为网络安全造成的经济损失超过1700亿美元。今年我国的一些著名的网站也遭到不明身份黑客的袭击。

2.2 网络系统的缺陷

因特网的共享性和开放性使网上信息存在先天不足, 因为因特网最初设计考虑的是该网不会因局部障碍而影响信息的传输, 但它仅是信息高速公路的雏形, 在安全可靠、服务质量、带宽和方便性等方面存在着不适应性。

2.3 计算机病毒

病毒是伴随计算机及网络技术的一个顽疾。名目繁多的计算机病毒的入侵, 使广大网络用户遭受极大的损失。如大规模暴发的CIH病毒, 使我国政府、公安、财政等重要部门在大范围内造成了重大损失。

收稿日期: 2000-10-15; 修订日期: 2000-11-09

3　主要防范技术措施

3.1　采用网络接口隔离技术

目前普遍采用的是防火墙(Firewall)技术。防火墙是一种特殊的程序系统,所有经由外部网的信息在进入网络之前,都必须经它的过滤和检验。它是网络安全的第一道屏障。

防火墙技术的核心思想是在不安全的网际之间构造一个相对安全的子网环境。其主要手段有两种:一种是分组(包)过滤技术;一种是代理技术。包过滤是基于用户认证机制的服务技术。这两种技术都会降低数据传输效率,而且安全要求越严格,对效率影响越大。为防止内部的攻击,还需要设置对内的第二道防火墙,使主机对内也被隔离,效率会更低。为提高效率,有的系统采用的是动态的安全管理方法,按照数据对安全级别要求的高、低,使检测依据的安全级别自动在用户层或系统层之间动态调整。不过,如技术上处理不当,在遇到攻击时,动态安全管理模式产生的损失可能会更大。

应当注意,代理服务不能解决协议自身的问题,如果使用了不安全的协议,代理不能消除其安全漏洞。对此,通过代理服务与包过滤的结合使用可达到较高的安全性。

3.2　档案信息加密通信

采用有效的档案信息加密措施,可使攻击者不能了解、修改敏感信息,即使这些重要信息被截获,也不至于泄密,或者延缓泄密的时间。对于网络信息和电子文件具体加密的方法很多,如名称加密、内容加密、属性加密、形式加密等,但这些措施都只是加大对它们进行更改或解密的难度。在计算机技术中,加密和解密是信息存储过程中的一对矛盾,只要加密技术发展了,解密技术也一定会发展。因此,对于网络信息和电子文件的加密并不能绝对保证其内容不受更改。因此要科学设置口令,增加黑客破译的难度。缺乏必要的制度与措施,往往也是造成电子文件机密泄漏的原因之一。值得重视的是,在加强对它们自身进行保密的同时,要特别注意工作制度和管理制度的加强。以电子文件为例,其制作过程的保密、打印输出的保密,电子文件管理工作的保密等,都是必须予以注意的。与电子文件信息处理有关的加密方法主要有三种:对称型加密,非对称型和不可逆加密。

对称型加密使用单个密钥(私钥)对数据进行加密或解密,其特点是计算量小、加密效率高。此类算法在分布式系统上使用较为困难,主要是密钥管理困难,造成使用成本高,保安性能也不易保证。目前最安全的模式是使用 128 位或更多位数的密钥算法。

非对称型加密算法的特点是使用一对密钥(即公钥和私钥),只有二者搭配使用,才能完成加密和解密的全过程。典型的算法是 RSA 公钥系统模式和美国国家标准局提出的 DSA 算法(数字签名算法)。非对称加密法特别适用于分布式系统中的数据加密,但需注意如何管理和确认公共密钥的合法性。

不可逆加密算法的特征是:加密过程不需要密钥,并且经过加密的数据无法被解密,只有同样的输入数据经过同样的不可逆加密算法才能得到相同的加密数据。不可逆加密算法不存在密钥保管和分发问题,适合于分布式网络系统,但是其加密计算工作量相当可观,所以通常用于数据量有限的情形下有加密,产生“一次性的口令”。在计算机网络中应用较多的有 RSA 公司提出的 MD5 散列算法和由美国国家标准局建议的 SHS 算法(可靠哈希标准)。

以上所述的三类数据加密技术经常被单独或混合使用,广泛应用于网络数据传输、认证和应用服务中。物理层、链路层和网络层使用的加密设备一般运用对称加密技术(如 EDS);远程访问服务中使用的一次性口令技术和 Cisco 路由器的 Enable Secret 口令一般采用不可逆加密算法 MD5;基于 PKI 的认证技术和 SET 协议则综合采用了不可逆加密、非对称加密、对称加密和数字签名等多种技术,很好地将安全性和高效率结合起来,被广泛应用于电子邮件、应用服务器访问、客户认证、防火墙验证和电子支付等领域。

密码系统是加密通信的核心,该系统可以为网络上运行的电子文件提供高度的安全保护;1)机密性,通过加密技术隐藏信息从而为处理和存储数据提供隐密保护;2)完整性,向所有各方保证文件,从文件生成到被接受全过程不变;3)非否定性,用于证明文件来自某个机构或个人,而不论该机构和该人员是否承认;4)真实性,提供两种服务,一是识别文件来源,并对真实性提供保证,二是认证注册该系统的人员身份。

3.3　信息认证

认证技术被广泛应用于各种网络结构和应用系统中。网络安全服务器协议 RADIUS、

Kerberos 和 TACACS+ 被用于网络设备和远程访问用户的身份认证, 防止非授权的用户使用网络资源。常采用的认证技术有如下几种:

3.3.1 数字签名技术

数字签名是在密码技术的基础上进行的。所谓签名, 其实是对发送文件的加密。在技术术语中, 加密前的文件称 "明文", 加密后的文件称 "密文", 加密是对 "明文"信息的某种运算, 运算方法称之为加密算法, 简称 "加密密钥"; 解密则是将密文通过再次运算还原为明文, 运算方法称为 "解密运算"简称 "解密密钥"。加密密钥和解密密钥是相互配套的一对算法, 缺一不可, 但并不对称, 也就是说解密并非加密的逆运算, 由加密密钥无法推知解密密钥, 反之亦然。基于此, 发文者秘密私存一把加密密钥, 对所发文件加密, 并将密文发往收文者, 收文者则使用发文者事先公布的解密密钥将文件恢复为明文。倘若明文得以恢复, 则至少证明以下两点: 一个是该文件系拥有相应加密密钥的发文者所有; 另一个是该文件在传输过程中未被改动。理由很简单, 加密密钥是保密的, 仅被发文者私存, 他人不可能获得; 一旦密文有任何改动, 解密后得到的只能是无法识读的乱码, 而非可理解的明文。通过上述加密解密过程, 可起到维护传递过程中电子文件信息原真性的作用。

3.3.2 报文认证技术

"报文"在计算机语言中专指处于某种情况下的电子文件。报文认证即指对发送的电子文件是否被篡改, 内容是否原真的鉴别、确认。与加密一样, 报文认证亦须要对发文内容作某种运算, 其具体方法是: 发文者在向收文者发送报文(发送文件)前, 采用某种摘要算法对报文进行运算, 运算后得到一串固定长度的验证码, 通常称为 "报文摘要"。报文摘要具有以下重要性质: 改变报文中的内容, 即便只是一位代码, 所得的摘要都将发生不可预测的改变。发文者将所得摘要作为报文的一部分附在报文内容后一同发送给收文者, 收文者收文后, 利用双方事先约定的摘要算法对收到的报文内容作同样的摘要运算, 如果所得摘要同附在发送来的摘要相同, 则说明报文未作改动, 其内容具有原真性。否则, 报文已在发送途中失真。

可见, 报文认证技术是通过比较运算所得的验证码(摘要)来鉴别电子文件内容的原真性的。与数字签证技术不同的是, 发送过程中的报文是明文, 不具有保密性。报文认证的局限是, 发文者必须事先约定将使用的摘要算法, 且由于摘要算法同样存在被破解的可能, 因此, 必须及时更换, 由此而带来一系列复杂问题。

3.3.3 打水印技术

打水印技术是日本电气公司(NEC) 1997 年才投入使用的新兴技术。它是在传输的声频、视频、图象或正文等多媒体电子文件上附加一个几乎抹不去的印记。除非用特殊技术检验, 该印记在通常状态下是隐匿不见的。如果这种水印遭到破坏, 文件数据也会受到破坏。打水印技术的实现极为复杂, 本文不拟探讨。

3.4 网上病毒防治安全体系

在大型网络中, 成千上万的客户端设备和服务器均有可能在不同程度上遭受病毒的侵害, 因此建立全网络的病毒防治安全体系统是非常必要的。架设病毒防治中心服务器, 网络终端设备安装防病毒软件, 病毒防治中心服务器具有集中管理、病毒特征码分发和警告功能。它可以通过实时扫描网络终端、各种服务器、电子邮件和 HTTP、SMTP、FTP 等网络协议, 能及时查杀已知的各类病毒, 并对未知病毒进行有效的隔离。它还可以定期通过 Internet 从防病毒软件厂商的技术支持中心获得的最新的病毒特征码, 并分发给所管辖的网络终端, 以保证整个网络都能识别并杀灭世界上最新发现的病毒。

3.5 强化网络信息系统的安全机制

有关计算机专家的研究成果表明, 信息系统的安全不只是一个技术问题, 它同时也涉及到网络的规划、安装使用和维护管理各个方面。所以, 必须要对网络信息系统的安全设计进行系统分析。它主要包括网络信息分析, 网络功能分析、威协类型分析、风险分析。系统分析的目的是预测是什么人、可能从何处、用什么方法来突破安全系统, 有可能造成什么程度的损失以及万一造成灾害时, 如何作出恢复的计划。信息系统的安全手段是由网络的保密机构来提供的, 而保密机构是在网络协议的各个分层中来实现的。国际标准 ISO7498 的 OSI 安全体系结构推荐的安全保密机制包括加密机制、数字签字机制、存取控制机制、数据完整性机制、实体鉴别机制、业务填充机制、路由控制机制、公证机制等等。

根据多重保护的原则, 综合使用上面所述的多种安全措施, 建立多层次的安全防御框架, 确保即使第一道安全防线被突破, 也能延缓或阻断攻击者到达攻击目标。图 1 是一个基本的网络安全体系框架。

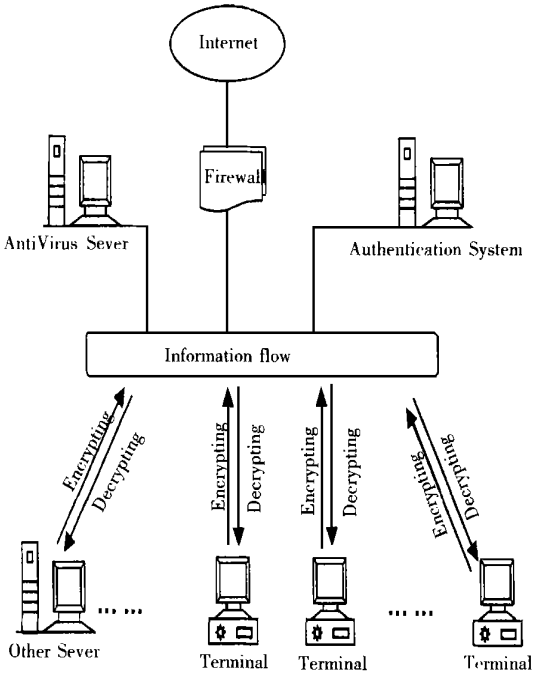

Fig.1 A basic frame of network safety system

4 结 束 语

档案信息与一般的图书情报信息相比,有许多信息涉及到一定的安全、保密、个人隐私问题。但我们也必须看到,当档案到了可以向社会开放的阶段,其知识性和文化性将逐渐凸现出来,档案馆上网并不是意味着将所有的档案信息全部上网,而是着眼于档案提供利用这一环节,可将开放的档案以适当的方式在网上向公众提供利用。本文主要是侧重那些有一定程度保密性要求的档案信息,在网上传输时一般可供选择的几种防范措施。随着计算机技术的不断完善与发展,将会有越来越多先进的防范措施涌现出来。因而我们可以根据实际情况的需要,视档案信息保密要求的不同,选择相应的技术措施,以确保档案信息在网上的安全传输。

参考文献:

[1] Farley Marc. 网络安全与数据完整性指南[M]. 北京:机械工业出版社,1997.
[2] 王育民,刘建民. 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,1996.
[3] 徐义全. 电子文件的特性与长期保管[J]. 档案研究,2000(1):53-57.
[4] 蒋斌,王在东. 20 世纪的中国档案网站:终结与开端[J]. 中国档案,2000(3):36-38.

Safety and security technology of network archives information

YANG Hong-bo[1], YUAN Ya-zhen[1], WANG Hong-wei[1], WU Deng-hui[2]

(1. *Changchun Institute of Optics, Fine Mechanics and Physics, Chinese Academy of Sciences, Changchun* 130021, *China*;
2. *Jilin Institute of Archive Science and Technology, Changchun* 130055; *China*)

Abstract: Archival information on network has become a trend today. An important problem of sofety and security faced the network archival information is discussed. Safety leaks of archives information during being transmitted on network are also analyzed. Meanwhile, the main prevention measures and cautions for network archival information are presented. Moreover, this paper focuses on encryption technology for archival information on network to supply a basic frame for establishing a complete safety system of network archival information and give a reference to networking engineering of archives information.

Key words: archives; network information; network safety

作者简介: 杨洪波(1963-),男,黑龙江齐齐哈尔人。1991 年毕业于中科院长春光机所研究生部光学仪器专业(硕士)。研究员。现在长春光学精密机械与物理研究所工作。主要从事 CAD/CAE 技术、网络技术的应用、开发工作。