 DOI: https://doi.org/10.36956/iser.v2i1.364

Exploring the Network Security Strategy of Archives Information

Haibo Liu

Hebei University of Technology, Tianjin, 300401, China

Abstract

Network security of archival information means that the hardware, software and data in the network system are protected from damage, change and leakage due to accidental or malicious reasons, the system runs continuously and reliably, and the network service is not interrupted. File information network security is the core content and key of file information security, and also the precondition of file information construction. It includes the operation security of archival information network and the information security of archival information network. Through various computer, network, password technology and information security technology (access control, communication encryption, identification and identification, anti-virus, etc.), the confidentiality, integrity and authenticity of information transmitted, exchanged and stored in the private network and public communication network of archival information are protected, and the transmission and content of archival information are controlled.

Keywords

security management strategy; archive work; information network; network technology

探究档案信息网络安全策略

刘海波

河北工业大学，中国 · 天津 300401

摘　要

档案信息网络安全是指网络系统的硬件、软件及其系统中的数据受到保护，不受偶然的或者恶意的原因而遭到破坏、更改、泄露，系统连续可靠正常地运行，网络服务不中断。档案信息网络安全是档案信息安全的核心内容和关键，也是档案信息化建设的前提条件。它包括档案信息网络运行安全和档案信息网络上的信息安全。通过各种计算机、网络、密码技术和信息安全技术（访问控制、通信加密、识别和鉴别、防病毒等），保护在档案信息专用网络及公用通信网络中传输、交换和存储信息的机密性、完整性和真实性，并对档案信息的传播及内容具有控制能力。

关键词

安全管理策略；档案工作；信息网络；网络技术

1 访问控制技术

访问控制是网络安全防范和保护的主要策略，它的主要任务是保证网络资源不被非法使用和非常访问。它也是维护网络系统安全、保护网络资源的重要手段。各种安全策略必须相互配合才能真正起到保护作用，但访问控制可以说是保证网络安全最重要的核心策略之一。

1.1 入网访问控制

入网访问控制为网络访问提供了第一层访问控制。它控制哪些用户能够登录到服务器并获取网络资源，控制准许用户入网的时间和准许他们在哪台工作站入网。

用户的入网访问控制可分为 3 个步骤：用户名的识别与验证、用户口令的识别与验证、用户账号的缺省限制检查。三道关卡中只要任何一关未过，该用户便不能进入该网络。

对网络用户的用户名和口令进行验证是防止非法访问的第一道防线。用户注册时首先输入用户名和口令，服务器将验证所输入的用户名是否合法。如果验证合法，才继续验证用户输入的口令，否则，用户将被拒于网络之外。用户的口令是用户入网的关键所在。为保证口令的安全性，用户口令不能显示在显示屏上，口令长度应不少于 6 个字符，口令字符最好是数字、字母和其他字符的混合，用户口令必须经过加密。加密的方法很多，其中最常见的方法有：基于单向函数的口令加密，基于测试模式的口令加密，基于公钥加密方案的口令加密，基于平方剩余的口令加密，基于多项式共享

 DOI: https://doi.org/10.36956/iser.v2i1.364

的口令加密，基于数字签名方案的口令加密等。经过上述方法加密的口令，即使是系统管理员也难以得到它。用户还可采用一次性用户口令，也可用便携式验证器（如智能卡）来验证用户的身份。

网络管理员应该可以控制和限制普通用户的账号使用、访问网络的时间、方式。用户名或用户账号是所有计算机系统中最基本的安全形势。用户账号应只有系统管理员才能建立。用户口令应是每用户访问网络所必须提交的“证件”。用户可以修改自己的口令，但系统管理员应该可以控制口令的以下几个方面的限制：最小口令长度、强制修改口令的时间间隔、口令的唯一性、口令过期失效后允许入网的宽限次数。

用户名和口令验证有效之后，再进一步履行用户账号的缺省限制检查。网络应能控制用户登录入网的站点，限制用户入网的时间，限制用户入网的工作站数量。当用户对交费网络的访问“资费”用尽时，网络还应能对用户的账号加以限制，用户此时应无法进入网络访问网络资源。网络应对所有用户的访问进行审计。如果多次输入口令不正确，则认为是非法用户的入侵，应给出报警信息。

1.2 网络的权限控制

网络的权限控制是针对网络非法操作所提出的一种安全保护措施。用户和用户组被赋予一定的权限。档案信息网络控制用户和用户组可以访问哪些目录、子目参、文件和其他资源。可以指定用户对这些文件、目录、设备能够执行哪些操作。受托者指派和继承权限屏蔽（IRM）可作为其两种实现方式。受托者指派控制用户和用户组如何使用网络服务器的目录、文件和设备。继承权限屏蔽相当于一个过滤器，可以限制子目录从父目录那里继承哪些权限。我们可以根据访问权限将用户分为以下几类：①特殊用户（即系统管理员）；②一般用户，系统管理员根据他们的实际需要为他们分配操作权限；③审计用户，负责网络的安全控制与资源使用情况的审计。用户对档案信息网络资源的访问权限可以用一个访问控制表来描述。

1.3 目录级安全控制

网络应允许控制用户对目录、文件、设备的访问。用户在目录一级指定的权限对所有文件和子目录有效，用户还可进一步指定对目录下的子目录和文件的权限。对目录和文件的访问权限一般有 8 种：系统管理员权限（Supervisor）、读权限（Read）、写权限（Write）、创建权限（Create）、删除权限（Erase）、修改权限（Modify）、文件查找权限（File Scan）、存取控制权限（Access Control）。用户对文件或目标的有效权限取决于以下几个因素：用户的受托者指派、用户所在组的受托者指派、继承权限屏蔽取消的用户权限。一个网络系统管理员应当为用户指定适当的访问权限，这些访问权限控制着用户对服务器的访问。8 种访问权限的有效组合可以让用户有效地完成工作，同时又能有效地控制用户对服务器资源的访问，从而加强了网络和服务器的安全性。

1.4 属性安全控制

当用文件、目录和网络设备时，网络系统管理员应给文件、目录等指定访问属性。属性安全控制可以将给定的属性与网络服务器的文件、目录和网络设备联系起来。属性安全在权限安全的基础上提供更进一步的安全性。网络上的资源都应预先标出一组安全属性。用户对网络资源的访问权限对应一张访问控制表，用以表明用户对网络资源的访问能力。属性设置可以覆盖已经指定的任何受托者指派和有效权限。属性往往能控制以下几个方面的权限：向某个文件写数据、拷贝一个文件、删除目录或文件、查看目录和文件、执行文件、隐含文件、共享、系统属性等。网络的属性可以保护重要的目录和文件，防止用户对目录和文件的误删除、执行修改、显示等。

1.5 网络服务器安全控制

网络允许在服务器控制台上执行一系列操作。用户使用控制台可以装载和卸载模块，可以安装和删除软件等。网络服务器的安全控制包括可以设置口令锁定服务器控制台，以防止非法用户修改、删除重要信息或破坏数据；可以设定服务器登录时间限制、非法访问者检测和关闭的时间间隔。

1.6 网络监测和锁定控制

网络管理员应对网络实施监控，服务器应记录用户对网络资源的访问，对非法的网络访问，服务器应以图形或文字或声音等形式报警，以引起网络管理员的注意。如果不法之徒试图进入网络，网络服务器应会自动记录企图尝试进入网络的次数，如果非法访问的次数达到设定数值，那么该账户将被自动锁定。

1.7 网络端口和节点的安全控制

网络中服务器的端口往往使用自动回呼设备、静默调制

 DOI: https://doi.org/10.36956/iser.v2i1.364

解调器加以保护，并以加密的形式来识别节点的身份。自动回呼设备用于防止假冒合法用户，静默调制解调器用以防范黑客的自动拨号程序对计算机进行攻击。网络还常对服务器端和用户端采取控制，用户必须携带证实身份的验证器（如智能卡、磁卡、安全密码发生器）。在对用户的身份进行验证之后，才允许用户进入用户端。然后，用户端和服务器端再进行相互验证。

2 识别和鉴别

档案网络安全系统要具备识别和鉴别机制以面对网络上的各种攻击。识别就是分配给每个用户一个 ID 来代表用户和进程。鉴别是根据用户的私有信息来确定用户的真实性，防止欺骗。口令机制是最常用的鉴别方法。随着生物技术的发展，利用指纹、视网膜等可提高鉴别的强度。经常使用的还有数字签名等方法。

2.1 口令机制

口令是相互约定的代码，假定只有用户和系统知道。口令有时由用户选择，有时由系统分配。通常情况下，用户先输入某种标识信息，比如用户名或 ID 号，然后系统询问用户口令，绕口令与用户文件约定相匹配，用户即可进入访问。

作为安全防护措施，口令也有可能被攻破。攻击口令的方法主要有强力攻击，猜测一切可能的口令代码；猜测可能性较大的口令；窃取、分析系统通行字表；伪装成系统来询问用户可不可以。

对抗口令攻击通常采用加密、签名和令牌等办法。但最重要的是进行口令管理，包括选择、分发和更改等。

2.2 数字签名

在电子政务运行过程中，一个重要内容就是辨认发送者和接收者的身份并进行记录，以保证信息的真实性和不可抵赖性。

数字签名机制提供了一种鉴别方法，以解决伪造、抵赖、冒充和篡改等问题。数字签名采用一定的数据交换形式，使得双方能够满足两个条件：一是接受方能够鉴别发送方所宣称的身份；二是发送方以后不能否认它发送过数据这一事实。

在书面文件上签名是确认文件的一种手段，其作用：一是自己的签名难以否认，能够确认文件已签署的事实；二是签名不易仿冒，能够确认文件为真的事实。数字签名与书面文件签名有相同之处，采用数字签名，也能确认信息由签名者发送、信息自签发后到收到为止未被做过修改。

这样，数字签名就可以用来防止电子信息因易被修改而有人作伪，或假冒他人名义发送信息，或发出（收到）信件后又加以否认等情况发生。数字签名采用双重加密的方法来实现防伪、防抵赖，常见的数字签名主要有 3 种：RSA 算法、Rabin 算法和 DDS 算法。

2.3 数字水印

为了防止图像文件盗用，采用数字水印技术，将作者信息嵌入到图像中。数字水印的特点是即使数据的格式发生了变化，版权信息也不会丢失。例如，加入了数字水印的 JPEG 格式图像，将其转换为 BMP 格式后，数字水印的信息仍然不会丢失。这是因为版权信息并不是附加在原数据上的，而是嵌入到了原数据的当中。而且包含数字水印的数据看起来跟普通的数据完全一样，不影响图像的显示。

2.4 电子印章

对于一些须分发的文件，有时需要加盖印章，可采用自主产权的方法实现不可盗用的电子印章。印章图像的原稿事先保存到数据库中。当用印人在使用此印章时，先将须盖章的文件的检查和用印人信息、印章图像原稿制稿人信息作为水印加入印章图像原稿生成用印稿，然后将用印稿加到须盖章的文件中。使用文件时，将检查原稿制稿人、用印人信息以及文件的检查。这样，其他人即使采用图像编辑软件将印章图像取出，用在其他文件中，也无法通过印章鉴别系统的检查。

2.5 生物识别技术

生物识别技术是依靠人体的身体特征来进行身份验证的一种解决方案，由于人体特征具有不可复制的特性，这一技术的安全系统较传统意义上的身份验证机制有很大的提高。人体的生物特征包括指纹、声音、面孔、视网膜、掌纹、骨架等，而其中指纹凭借其无可比拟的唯一性、稳定性、再生性备受关注。

20 世纪 60 年代，计算机可以有效地处理图形，人们开始着手研究用计算机来处理指纹，自动指纹识别系统 AFIS 由此发展开来。AFIS 是当今数字生活中一套成功的身份鉴别系统，也是未来生物识别技术的主流之一，它通过外设来获取指纹的数字图像并存贮在计算机系统中，再运用先进的滤波、

 DOI: https://doi.org/10.36956/iser.v2i1.364

图像二值化、细化手段对数字图像提取特征，最后使用复杂的匹配算法对指纹特征进行匹配。时下，有关指纹自动识别的研究已进入了成熟的阶段。随着指纹识别产品的不断开发和生产，未来该项技术的应用将进入民用市场，服务大众。

除了指纹识别技术外，近年来视网膜识别技术和签名识别技术的研究也取得了骄人的成绩。视网膜识别技术分为两个不同的领域：虹膜识别技术和角膜识别技术。虹膜识别系统使用一台摄像机来捕捉样本，而角膜扫描的进行则是用低密度的红外线去捕捉角膜的独特特征。由于该项技术具有高度的准确性，它将被应用在未来军事安全机构和其他保密机关中。签名识别，也被称为签名力学识别（DSV：Danamic Signatuer Verification），它是建立在签名时的力度上的，分析笔的移动，例如加速度、压力、方向以及笔画的长度，而非签名的图像本身。签名力学的关键在于分出不同的签名部分，有些是习惯性的，而另一些在每次签名时都不同，DSV 系统能被控制在某种方式上去接收变量，此项技术预计在今后 10 年中会得到进一步发展和应用。

3 防火墙技术

防火墙是一种保护计算机网络安全的技术性措施，它是一个用以阻止网络中的黑客访问某个机构网络的屏障，也可称之为控制进 / 出两个方向通信的门槛。在网络边界上通过建立起来的相应网络通信监控系统来隔离内部和外部网络，以阻挡外部网络的侵入。目前的防火墙主要有以下 3 种类型：

3.1 包过滤防火墙

包过滤防火墙设置在网络层，可以在路由器上实现包过滤。首先应建立一定数量的信息过滤表，信息过滤表是以其收到的数据包头信息为基础而建成的。信息包头含有数据包源 IP 地址、目的 IP 地址、传输协议类型（TCP、UDP、ICMP 等）、协议源端口号、协议目的端口号、连接请求方向、ICMP 报文类型等。当一个数据包满足过滤表中的规则时，则允许数据包通过，否则禁止通过。这种防火墙可以用于禁止外部不合法用户对内部的访问，也可以用来禁止访问某些服务类型。但包过滤技术不能识别有危险的信息包，无法实施对应用级协议的处理，也无法处理 UDP、RPC 或动态的协议。

3.2 代理防火墙

代理防火墙又称应用层网关级防火墙，它由代理服务器和过滤路由器组成，是目前较流行的一种防火墙。它将过滤路由器和软件代理技术结合在一起。过滤路由器负责网络互联，并对数据进行严格选择，然后将筛选过的数据传送给代理服务器。代理服务器起到外部网络申请访问内部网络的中间转接作用，其功能类似于一个数据转发器，它主要控制哪些用户能访问哪些服务类型。当外部网络向内部网络申请某种网络服务时，代理服务器接受申请，然后它根据其服务类型、服务内容、被服务的对象、服务者申请的时间、申请者的域名范围等来决定是否接受此项服务，如果接受，它就向内部网络转发这项请求 o 代理防火墙无法快速支持一些新出现的业务（如多媒体）。现在较为流行的代理服务器软件是 ingate 和 Proxy Server。

3.3 双穴主机防火墙

该防火墙是用主机来执行安全控制功能。一台双穴主机配有多个网卡，分别连接不同的网络。双穴主机从一个网络收集数据，并且有选择地把它发送到另一个网络上。网络服务由双穴主机上的服务代理来提供。内部网和外部网的用户可通过双穴主机的共享数据区传递数据，从而保护了内部网络不被非法访问。

4 加密技术

信息加密的目的是保护网内的数据、文件、口令和控制信息，保护网上传输的数据。网络加密常用的方法有链路加密、端点加密和节点加密三种。链路加密的目的是保护网络节点之间的链路信息安全；端点加密的目的是对源端用户到目的端用户的数据提供保护；节点加密的目的是对源节点到目的节点之间的传输链路提供保护。用户可根据网络情况酌情选择上述加密方式。

信息加密过程是由形形色色的加密算法来具体实施的，它以很小的代价提供很大的安全保护。在多数情况下，信息加密是保证信息机密性的唯一方法。据不完全统计，到目前为止，已经公开发表的各种加密算法多达数百种。如果按照收发双方密钥是否相同来分类，可以将这些加密算法分为常规密码算法和公钥密码算法。

在常规密码中，收信方和发信方使用相同的密钥，即加密密钥和解密密钥是相同或等价的。比较著名的常规密码算法有：美国的 DES 及其各种变形，比如 Triple、DES、

 DOI: https://doi.org/10.36956/iser.v2i1.364

GDES、New DES 和 DES 的前身 Lucifer；欧洲的 IDEA；日本的 FEAL−N、LOKI−91、Skipjack，RC4、RC5 以及以代换密码和转轮密码为代表的古典密码等。在众多的常规密码中影响最大的是 DES 密码。常规密码的优点是有很强的保密强度，且经受住时间的检验和攻击，但其密钥必须通过安全的途径传送。因此，其密钥管理成为系统安全的重要因素。

在公钥密码中，收信方和发信方使用的密钥互不相同，而且几乎不可能从加密密钥推导出解密密钥。比较著名的公钥密码算法有：RSA、背包密码 AMcEliece 密码、diff−Hellman、Rabin、Ong−Fiat−Shamir、零知识证明的算法、椭圆曲线、EIGamal 算法等等。最有影响的公钥密码算法是 RSA，它能抵抗到目前为止已知的所有密码攻击。

PKI（Public Key Infrastructure，公开密钥基础设施）是一种遵循既定标准的密钥管理平台，它可以为各种网络应用透明地提供采用加密和数字签名等密码服务所必需的密钥和证书管理，从而达到保证网上传递信息的安全、真实、完整和不可抵赖的目的。PKI 可以提供会话保密、认证、完整性、访问控制、源不可否认、目的不可否认、安全通信、密钥恢复和安全时间等 9 项信息安全所需要的服务。在这个结构中，公开密钥密码算法居于中心地位，称其为 PKI0 利用 PKI，人们可以方便地建立和维护一个可信的网络计算环境，无须直接见面就能够确认彼此的身份，安全地进行信息交换。

完整的 PKI 系统有权威认证机构（CA）、数字证书库、密钥备份及恢复系统、证书撤销系统、应用接口（API）等基本构成部分。

CA 是 PKI 的核心，主要职责是颁发证书、验证用户身份的真实性。一般情况下，证书必须由一个可信任的第三方权威机构——CA 认证中心实施数字签名以后才能发布。而获得证书的用户通过对 CA 的签名进行验证，从而确定了公钥的有效性。

数字证书库是证书集中存储的地方，用户可以从此处获得其他用户可用的证书和公钥信息。数字证书库一般是基于 LDAP 或是基于 X.500 系列的，也可以基于其他平台。

密钥可能会由于一些原因而使密钥的所有者无法访问。密钥的丢失将导致那些被密钥加过密的数据无法恢复。为避免这种情况的出现，就需要 PKI 提供密钥备份与恢复的机制。

CA 签发证书来把用户的身份和密钥绑定在一起。那么，当用户的身份改变或密钥遭到破坏时，就必须存在一种机制来撤销这种认可。

一个完整的 PKI 必须提供良好的应用接口系统，以便各种应用都能够以安全、一致、可信的方式与 PKI 交互，确保所建立起来的网络环境的可信性，降低管理和维护的成本。

公钥密码的优点是可以适应网络的开放性要求，且密钥管理问题也较为简单，尤其可方便地实现数字签名和验证，但其算法复杂，加密数据的速率较低。尽管如此，随着现代电子技术和密码技术的发展，公钥密码算法将是一种很有前途的网络安全加密体制。

在实际应用中，人们通常将常规密码和公钥密码结合在一起使用，如利用 DES 或者 IDEA 来加密信息，而采用 RSA 来传递会话密钥。如果按照每次加密所处理的比特来分类，可以将加密算法分为序列密码和分组密码。前者每次只加密一个比特而后者则先将信息序列分组，每次处理一个组。

5 病毒防护技术

在网络环境下，计算机病毒有不可估量的威胁性和破坏力。档案信息网络系统中使用的操作系统一般均为 Windows 系统，比较容易感染病毒。因此计算机病毒的防范也是档案信息网络安全建设中应该考虑的重要环节之一。反病毒技术包括预防病毒、检测病毒和杀毒三种技术。

5.1 预防病毒技术

预防病毒技术通过自身常驻系统内存，优先获得系统的控制权，监视和判断系统中是否有病毒存在，进而阻止计算机病毒进入计算机系统和对系统进行破坏。这类技术有：加密可执行程序、引导区保护、系统监控与读写控制（如防病毒卡等）。

5.2 检测病毒技术

检测病毒技术是通过对计算机病毒特征（如自身校验、关键字、文件长度的变化等）进行分析，以确定病毒类型的技术。

5.3 杀毒技术

杀毒技术通过对计算机病毒代码分析，开发出具有删除病毒程序并恢复原文件的软件。反病毒技术的具体实现方法，包括对网络中服务器及工作站中的文件及电子邮件等进行频繁地扫描和检测。一旦发现与病毒代码库中相匹配的病毒代码，反病毒程序会采取相应处理措施，防止病毒进入网络进

 DOI: https://doi.org/10.36956/iser.v2i1.364

行传播扩散。

档案信息安全防范是通过安全技术、安全产品继承及安全管理来实现的，其中安全产品的继承便涉及如何选择档案信息安全产品。在进行档案信息安全产品选型时，要求档案信息安全产品能满足两方面的要求：一是安全产品必须符合国家有关安全管理的政策要求，针对相关的安全产品必须查看其是否得到相应的许可证，如密码产品满足国家密码管理委员会的要求，安全产品获得国家公安部颁发的销售许可证，安全产品获得中国信息安全产品测评认证中心的测评认证，安全产品获得原总参谋部颁发的国防通信网设备器材进网许可证，符合国家保密局有关国际联网管理规定以及涉密网审批管理规定。二是安全产品的功能与性能要求必须考虑产品功能、性能、运行稳定性以及扩展性，还必须考查安全产品自身的安全性。

参考文献

[1] 庄丽萍 . 档案信息网络安全管理策略 [J]. 科技档案 ,2006,04(4):11.

[2] 孙梅霞 . 高校档案信息网络安全与防护 [J]. 兰台世界 ,2009:46-47.

[3] 张照余 , 章丹 . 档案信息网络安全的法律保护 [J]. 广东档案 ,2002(001):34-35.

[4] 程茶 . 档案信息网络安全管理问题与对策研究 [J]. 档案天地 ,2015(S1):96-97.

[5] 张晓路 . 档案信息网络安全对策 [C]// 信息社会档案学理论与实践 .0.

[6] 罗为群 . 如何做好企业档案信息网络安全的可靠运行 [J]. 兰台世界 : 上旬 ,2010:66.