**山东大学继续教育学院**

**毕业综述**

题 目 网络安全问题与对策

姓 名 李安龙 学 号 18210302066054

年 级

专 业 计算机信息管理

学习中心

填表日期

****山东大学继续教育学院制****

网络安全问题与对策

 1 绪论   
　　 随着互联网的飞速发展，网络安全逐渐成为一个潜在的巨大问题。网络安全性是一个涉及面很广泛的问题，其中也会涉及到是否构成犯罪行为的问题。在其最简单的形式中，它主要关心的是确保无关人员不能读取，更不能修改传送给其他接收者的信息。此时，它关心的对象是那些无权使用，但却试图获得远程服务的人。安全性也处理合法消息被截获和重播的问题，以及发送者是否曾发送过该条消息的问题。   
　　 大多数安全性问题的出现都是由于有恶意的人试图获得某种好处或损害某些人而故意引起的。可以看出保证网络安全不仅仅是使它没有编程错误。它包括要防范那些聪明的，通常也是狡猾的、专业的，并且在时间和金钱上是很充足、富有的人。同时，必须清楚地认识到，能够制止偶然实施破坏行为的敌人的方法对那些惯于作案的老手来说，收效甚微。   
　　 网络安全性可以被粗略地分为4个相互交织的部分：保密、鉴别、反拒认以及完整性控制。保密是保护信息不被未授权者访问，这是人们提到的网络安全性时最常想到的内容。鉴别主要指在揭示敏感信息或进行事务处理之前先确认对方的身份。反拒认主要与签名有关。保密和完整性通过使用注册过的邮件和文件锁来   
　　 2 方案目标   
　　 本方案主要从网络层次考虑，将网络系统设计成一个支持各级别用户或用户群的安全网络，该网在保证系统内部网络安全的同时，还实现与Internet或国内其它网络的安全互连。本方案在保证网络安全可以满足各种用户的需求，比如：可以满足个人的通话保密性，也可以满足企业客户的计算机系统的安全保障，数据库不被非法访问和破坏，系统不被病毒侵犯，同时也可以防止诸如反动淫秽等有害信息在网上传播等。   
　　 需要明确的是，安全技术并不能杜绝所有的对网络的侵扰和破坏，它的作用仅在于最大限度地防范，以及在受到侵扰的破坏后将损失尽旦降低。具体地说，网络安全技术主要作用有以下几点：   
　　 1．采用多层防卫手段，将受到侵扰和破坏的概率降到最低；   
　　 2．提供迅速检测非法使用和非法初始进入点的手段，核查跟踪侵入者的活动；   
　　 3．提供恢复被破坏的数据和系统的手段，尽量降低损失；   
　　 4．提供查获侵入者的手段。   
　　 网络安全技术是实现安全管理的基础，近年来，网络安全技术得到了迅猛发展，已经产生了十分丰富的理论和实际内容。   
　　 3 安全需求   
　　 通过对网络系统的风险分析及需要解决的安全问题，我们需要制定合理的安全策略及安全方案来确保网络系统的机密性、完整性、可用性、可控性与可审查性。即，   
　　 可用性： 授权实体有权访问数据   
　　 机密性： 信息不暴露给未授权实体或进程   
　　 完整性： 保证数据不被未授权修改   
　　 可控性： 控制授权范围内的信息流向及操作方式   
　　 可审查性：对出现的安全问题提供依据与手段   
　　 访问控制：需要由防火墙将内部网络与外部不可信任的网络隔离，对与外部网络交换数据的内部网络及其主机、所交换的数据进行严格的访问控制。同样，对内部网络，由于不同的应用业务以及不同的安全级别，也需要使用防火墙将不同的LAN或网段进行隔离，并实现相互的访问控制。   
　　 数据加密：数据加密是在数据传输、存储过程中防止非法窃取、篡改信息的有效手段。   
　　 安全审计：是识别与防止网络攻击行为、追查网络泄密行为的重要措施之一。具体包括两方面的内容，一是采用网络监控与入侵防范系统，识别网络各种违规操作与攻击行为，即时响应（如报警）并进行阻断；二是对信息内容的审计，可以防止内部机密或敏感信息的非法泄漏   
　　 4 风险分析   
　　 网络安全是网络正常运行的前提。网络安全不单是单点的安全，而是整个信息网的安全，需要从物理、网络、系统、应用和管理方面进行立体的防护。要知道如何防护，首先需要了解安全风险来自于何处。网络安全系统必须包括技术和管理两方面，涵盖物理层、系统层、网络层、应用层和管理层各个层面上的诸多风险类。无论哪个层面上的安全措施不到位，都会存在很大的安全隐患，都有可能造成网络的中断。根据国内网络系统的网络结构和应用情况，应当从网络安全、系统安全、应用安全及管理安全等方面进行全面地分析。   
　　 风险分析是网络安全技术需要提供的一个重要功能。它要连续不断地对网络中的消息和事件进行检测，对系统受到侵扰和破坏的风险进行分析。风险分析必须包括网络中所有有关的成分。   
　　 5 解决方案   
　　 5.1 设计原则   
　　 针对网络系统实际情况，解决网络的安全保密问题是当务之急，考虑技术难度及经费等因素，设计时应遵循如下思想：   
　　 1．大幅度地提高系统的安全性和保密性；

2．保持网络原有的性能特点，即对网络的协议和传输具有很好的透明性；   
　　 3．易于操作、维护，并便于自动化管理，而不增加或少增加附加操作；   
　　 4．尽量不影响原网络拓扑结构，同时便于系统及系统功能的扩展；   
　　 5．安全保密系统具有较好的性能价格比，一次性投资，可以长期使用；   
　　 6．安全与密码产品具有合法性，及经过国家有关管理部门的认可或认证；   
　　 7．分步实施原则：分级管理 分步实施。   
　　 5.2 安全策略   
　　 针对上述分析，我们采取以下安全策略：   
　　 1．采用漏洞扫描技术，对重要网络设备进行风险评估，保证信息系统尽量在最优的状况下运行。   
　　 2．采用各种安全技术，构筑防御系统，主要有：   
　　 (1) 防火墙技术：在网络的对外接口，采用防火墙技术，在网络层进行访问控制。   
　　 (2) NAT技术：隐藏内部网络信息。   
　　 (3) VPN：虚拟专用网(VPN)是企业网在因特网等公共网络上的延伸,通过一个私有的通道在公共网络上创建一个安全的私有连接。它通过安全的数据通道将远程用户、公司分支机构、公司业务伙伴等与公司的企业网连接起来，构成一个扩展的公司企业网。在该网中的主机将不会觉察到公共网络的存在，仿佛所有的机器都处于一个网络之中。公共网络似乎只由本网络在独占使用，而事实上并非如此。   
　　 (4）网络加密技术(Ipsec) ：采用网络加密技术，对公网中传输的IP包进行加密和封装，实现数据传输的保密性、完整性。它可解决网络在公网的数据传输安全性问题，也可解决远程用户访问内网的安全问题。   
　　 (5) 认证：提供基于身份的认证，并在各种认证机制中可选择使用。   
　　 (6) 多层次多级别的企业级的防病毒系统：采用多层次多级别的企业级的防病毒系统，对病毒实现全面的防护。   
　　 (7）网络的实时监测：采用入侵检测系统，对主机和网络进行监测和预警，进一步提高网络防御外来攻击的能力。   
　　 3．实时响应与恢复：制定和完善安全管理制度，提高对网络攻击等实时响应与恢复能力。   
　　 4．建立分层管理和各级安全管理中心。   
　　 5.3 防御系统   
　　 我们采用防火墙技术、NAT技术、VPN技术、网络加密技术（Ipsec）、身份认证技术、多层次多级别的防病毒系统、入侵检测技术，构成网络安全的防御系统。   
　　 5.3.1 物理安全   
　　 物理安全是保护计算机网络设备、设施以及其它媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏过程。   
　　 为保证信息网络系统的物理安全，还要防止系统信息在空间的扩散。通常是在物理上采取一定的防护措施，来减少或干扰扩散出去的空间信号。这是政府、军队、金融机构在兴建信息中心时首要的设置的条件。   
　　 为保证网络的正常运行，在物理安全方面应采取如下措施：   
　　 1．产品保障方面：主要指产品采购、运输、安装等方面的安全措施。   
　　 2．运行安全方面：网络中的设备，特别是安全类产品在使用过程中，必须能够从生成厂家或供货单位得到迅速的技术支持服务。对一些关键设备和系统，应设置备份系统。   
　　 3．防电磁辐射方面：所有重要涉密的设备都需安装防电磁辐射产品，如辐射干扰机。   
　　 4．保安方面：主要是防盗、防火等，还包括网络系统所有网络设备、计算机、安全设备的安全防护。   
　　 5.3.2 防火墙技术   
　　 防火墙是一种网络安全保障手段,是网络通信时执行的一种访问控制尺度,其主要目标就是通过控制入、出一个网络的权限,并迫使所有的连接都经过这样的检查,防止一个需要保护的网络遭外界因素的干扰和破坏。在逻辑上，防火墙是一个分离器，一个限制器，也是一个分析器，有效地监视了内部网络和Internet之间地任何活动，保证了内部网络地安全；在物理实现上，防火墙是位于网络特殊位置地以组硬件设备――路由器、计算机或其他特制地硬件设备。防火墙可以是独立地系统，也可以在一个进行网络互连地路由器上实现防火墙。用防火墙来实现网络安全必须考虑防火墙的网络拓扑结构：  
　　 （1）屏蔽路由器：又称包过滤防火墙。   
　　 （2）双穴主机：双穴主机是包过滤网关的一种替代。   
　　 （3）主机过滤结构：这种结构实际上是包过滤和代理的结合。   
　　 （4）屏蔽子网结构：这种防火墙是双穴主机和被屏蔽主机的变形。   
　　 根据防火墙所采用的技术不同,我们可以将它分为四种基本类型:包过滤型、网络地址转换—NAT、代理型和监测型。   
　　 5.3.2.1 包过滤型   
　　 包过滤型产品是防火墙的初级产品,其技术依据是网络中的分包传输技术。网络上的数据都是以“包”为单位进行传输的,数据被分割成为一定大小的数据包,每一个数据包中都会包含一些特定信息,如数据的源地址、目标地址、TCP/UDP源端口和目标端口等。防火墙通过读取数据包中的地址信息来判断这些“包”是否来自可信任的安全站点 ,一旦发现来自危险站点的数据包,防火墙便会将这些数据拒之门外。系统管理员也可以根据实际情况灵活制订判断规则。包过滤技术的优点是简单实用,实现成本较低,在应用环境比较简单的情况下,能够以较小的代价在一定程度上保证系统的安全。但包过滤技术的缺陷也是明显的。包过滤技术是一种完全基于网络层的安全技术,只能根据数据包的来源、目标和端口等网络信息进行判断,无法识别基于应用层的恶意侵入,如恶意的Java小程序以及电子邮件中附带的病毒。有经验的黑客很容易伪造IP地址,骗过包过滤型防火墙。   
　　 5.3.2.2 网络地址转化—NAT   
　　 网络地址转换是一种用于把IP地址转换成临时的、外部的、注册的IP地址标准。它允许具有私有IP地址的内部网络访问因特网。它还意味着用户不许要为其网络中每一台机器取得注册的IP地址。在内部网络通过安全网卡访问外部网络时，将产生一个映射记录。系统将外出的源地址和源端口映射为一个伪装的地址和端口，让这个伪装的地址和端口通过非安全网卡与外部网络连接，这样对外就隐藏了真实的内部网络地址。在外部网络通过非安全网卡访问内部网络时，它并不知道内部网络的连接情况，而只是通过一个开放的IP地址和端口来请求访问。OLM防火墙根据预先定义好的映射规则来判断这个访问是否安全。当符合规则时，防火墙认为访问是安全的，可以接受访问请求，也可以将连接请求映射到不同的内部计算机中。当不符合规则时，防火墙认为该访问是不安全的，不能被接受，防火墙将屏蔽外部的连接请求。网络地址转换的过程对于用户来说是透明的，不需要用户进行设置，用户只要进行常规操作即可。   
　　 5.3.2.3 代理型   
　　 代理型防火墙也可以被称为代理服务器,它的安全性要高于包过滤型产品,并已经开始向应用层发展。代理服务器位于客户机与服务器之间,完全阻挡了二者间的数据交流。从客户机来看,代理服务器相当于一台真正的服务器;而从服务器来看,代理服务器又是一台真正的客户机。当客户机需要使用服务器上的数据时,首先将数据请求发给代理服务器,代理服务器再根据这一请求向服务器索取数据,然后再由代理服务器将数据传输给客户机。由于外部系统与内部服务器之间没有直接的数据通道,外部的恶意侵害也就很难伤害到企业内部网络系统。代理型防火墙的优点是安全性较高,可以针对应用层进行侦测和扫描,对付基于应用层的侵入和病毒都十分有效。其缺点是对系统的整体性能有较大的影响,而且代理服务器必须针对客户机可能产生的所有应用类型逐一进行设置,大大增加了系统管理的复杂性。   
　　 5.3.2.4 监测型   
　　 监测型防火墙是新一代的产品,这一技术实际已经超越了最初的防火墙定义。监测型防火墙能够对各层的数据进行主动的、实时的监测,在对这些数据加以分析的基础上,监测型防火墙能够有效地判断出各层中的非法侵入。同时,这种检测型防火墙产品一般还带有分布式探测器,这些探测器安置在各种应用服务器和其他网络的节点之中,不仅能够检测来自网络外部的攻击,同时对来自内部的恶意破坏也有极强的防范作用。据权威机构统计,在针对网络系统的攻击中,有相当比例的攻击来自网络内部。因此,监测型防火墙不仅超越了传统防火墙的定义,而且在安全性上也超越了前两代产品,虽然监测型防火墙安全性上已超越了包过滤型和代理服务器型防火墙,但由于监测型防火墙技术的实现成本较高,也不易管理,所以目前在实用中的防火墙产品仍然以第二代代理型产品为主,但在某些方面也已经开始使用监测型防火墙。基于对系统成本与安全技术成本的综合考虑,用户可以选择性地使用某些监测型技术。这样既能够保证网络系统的安全性需求,同时也能有效地控制安全系统的总拥有成本。实际上,作为当前防火墙产品的主流趋势,大多数代理服务器(也称应用网关)也集成了包过滤技术,这两种技术的混合应用显然比单独使用具有更大的优势。由于这种产品是基于应用的,应用网关能提供对协议的过滤。例如,它可以过滤掉FTP连接中的PUT命令,而且通过代理应用,应用网关能够有效地避免内部网络的信息外泄。正是由于应用网关的这些特点,使得应用过程中的矛盾主要集中在对多种网络应用协议的有效支持和对网络整体性能的影响上。   
　　 相关性：毕业论文,免费毕业论文,大学毕业论文,毕业论文模板   
　　 5.3.3 入侵检测   
　　 入侵检测是防火墙的合理补充，帮助系统对付网络攻击，扩展了系统管理员的安全管理能力（包括安全审计、监视、进攻识别和响应），提高了信息安全基础结构的完整性。它从计算机网络系统中的若干关键点收集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。入侵检测被认为   
　　 是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，从而提供对内部攻击、外部攻击和误操作的实时保护。这些都通过它执行以下任务来实现：   
　　 1．监视、分析用户及系统活动；   
　　 2．系统构造和弱点的审计；   
　　 3．识别反映已知进攻的活动模式并向相关人士报警；   
　　 4．异常行为模式的统计分析；   
　　 5．评估重要系统和数据文件的完整性；  
　　 6． 操作系统的审计跟踪管理，并识别用户违反安全策略的行为。   
　　 5.4 安全服务   
　　 网络是个动态的系统，它的变化包括网络设备的调整，网络配置的变化，各种操作系统、应用程序的变化，管理人员的变化。即使最初制定的安全策略十分可靠，但是随着网络结构和应用的不断变化，安全策略可能失效，必须及时进行相应的调整。针对以上问题和网管人员的不足，下面介绍一系列比较重要的网络服务。包括：   
　　 1．通信伙伴认证   
　　 通信伙伴认证服务的作用是通信伙伴之间相互确庥身份，防止他人插入通信过程。认证一般在通信之前进行。但在必要的时候也可以在通信过程中随时进行。认证有两种形式，一种是检查一方标识的单方认证，一种是通信双方相互检查对方标识的相互认证。   
　　 通信伙伴认证服务可以通过加密机制，数字签名机制以及认证机制实现。   
　　 2．访问控制   
　　 访问控制服务的作用是保证只有被授权的用户才能访问网络和利用资源。访问控制的基本原理是检查用户标识，口令，根据授予的权限限制其对资源的利用范围和程度。例如是否有权利用主机CPU运行程序，是否有权对数据库进行查询和修改等等。   
　　 访问控制服务通过访问控制机制实现。   
　　 3．数据保密   
　　 数据保密服务的作用是防止数据被无权者阅读。数据保密既包括存储中的数据，也包括传输中的数据。保密查以对特定文件，通信链路，甚至文件中指定的字段进行。   
　　 数据保密服务可以通过加密机制和路由控制机制实现。   
　　 4．业务流分析保护   
　　 业务流分析保护服务的作用是防止通过分析业务流，来获取业务量特征，信息长度以及信息源和目的地等信息。   
　　 业务流分析保护服务可以通过加密机制，伪装业务流机制，路由控制机制实现。   
　　 5．数据完整性保护   
　　 数据完整性保护服务的作用是保护存储和传输中的数据不被删除，更改，插入和重复，必要时该服务也可以包含一定的恢复功能。   
　　 数据完整性保护服务可以通过加密机制，数字签名机制以及数据完整性机制实现   
　　 6．签字   
　　 签字服务是用发送签字的办法来对信息的接收进行确认，以证明和承认信息是由签字者发出或接收的。这个服务的作用在于避免通信双方对信息的来源发生争议。   
　　 签字服务通过数字签名机制及公证机制实现。   
　　 5.5 安全技术的研究现状和动向   
　　 我国信息网络安全研究历经了通信保密、数据保护两个阶段，正在进入网络信息安全研究阶段，现已开发研制出防火墙、安全路由器、安全网关、黑客入侵检测、系统脆弱性扫描软件等。但因信息网络安全领域是一个综合、交叉的学科领域它综合了利用数学、物理、生化信息技术和计算机技术的诸多学科的长期积累和最新发展成果，提出系统的、完整的和协同的解决信息网络安全的方案，目前应从安全体系结构、安全协议、现代密码理论、信息分析和监控以及信息安全系统五个方面开展研究，各部分相互协同形成有机整体。国际上信息安全研究起步较早，力度大，积累多，应用广，在70年代美国的网络安全技术基础理论研究成果“计算机保密模型”（Beu& La padula模型）的基础上，指定了“   
　　 可信计算机系统安全评估准则”（TCSEC），其后又制定了关于网络系统数据库方面和系列安全解释，形成了安全信息系统体系结构的准则。  
　　 结论   
　　 随着互联网的飞速发展，网络安全逐渐成为一个潜在的巨大问题。网络安全性是一个涉及面很广泛的问题，其中也会涉及到是否构成犯罪行为的问题。在其最简单的形式中，它主要关心的是确保无关人员不能读取，更不能修改传送给其他接收者的信息。此时，它关心的对象是那些无权使用，但却试图获得远程服务的人。安全性也处理合法消息被截获和重播的问题，以及发送者是否曾发送过该条消息的问题。   
　　 本论文从多方面描述了网络安全的解决方案，目的在于为用户提供信息的保密，认证和完整性保护机制，使网络中的服务，数据以及系统免受侵扰和破坏。比如防火墙，认证，加密技术等都是当今常用的方法，本论文从这些方法入手深入研究各个方面的网络安全问题的解决，可以使读者有对网络安全技术的更深刻的了解