计算机科学1998 Vol. 25 №. 1

建立 INTERNET 上的安全环境

Building a Security Environment on Internet

唐晓东　齐治昌

（国防科技大学计算机学院　长沙410073）

摘　要　In this paper, we analyse security risks of internet, then introduce a security architecture, finally analyse the security attributes of current Internet protocol sets.

关键词　Internet, Intranet, Kerberos, Security, Cipher, Security key, Firewall, TCP/IP

最近几年 INTERNET 飞速发展，为用户提供方便的远程计算、资源共享和电子数据传输等服务，促进了社会发展。然而，INTERNET 尚存在着一个致命缺点：缺乏安全性。在激烈竞争的社会中，用户面对着 INTERNET 拥有的巨大财富，既爱又怕，INTERNET 的安全已成为迫切需要解决的问题了。本文首先介绍一般性安全概念，然后讨论 INTERNET 存在的安全问题，并针对这些安全问题给出一个安全体系结构，最后分析现有 INTERNET 协议集的安全性。

证。它是 S/MIME、对象签名和 EDI 的安全基础。

在强安全方面，验证比密码有优越之处：鉴别身份、确保消息和内容的有效、保证隐私、授权访问、授权事务以及支持承认(non-repudiation)。

vCard　定义了个人之间电子化通讯的数据格式，即将电子、电讯手段加入 PDI(Personal Data Exchange)中，保证信息快速、准确地通讯、存储、组织和方便地定位。这种格式独立于特定的传输方法，可以是文件系统、点对点公共交换电话网、有线网或无线网。在 Internet 上，vCard 用于：

·转递电子邮件消息中的个人数据。通过使用 vCard，可自动操作 WWW 的用户在主页上填写的大量的表(form)。

·电子邮件的收件者自动记录发信者的个人信息，仅仅通过将电子邮件拖入他们的地址簿中，不需要信件头和信件尾消息。

·自动填写大量的主页表格。倘若 Web 服务器和浏览器支持 vCard，那么可加速这个应用。

签名对象(Signed Object)　是确保 Extranet、Intranet 和 Internet 上软件可靠分派，帮助用户和网络管理员决定软件资源是否可靠的一种技术。在 Extranet 上，可靠的跨平台鉴别、分派和访问控制，对于软件尤为重要。对象签名使用基于 X. 509 v3标准和一些 PKCS 规范，包括 PKCS #7签名和加密标准。数字签名可用于：

·鉴别签名者身份：确认个人、公司或其他实体的身份，他们的数字签名与一签名对象关联。

·检测变化：决定是否一签名对象未经授权而被改动。

·控制 Java/JavaScript 访问。

·自动更新软件。

Netscape 提出的 SSL 技术加密 Web 浏览器和服务器之间的通信对话。

结束语　Extranet 与其说是一种网络设计方案，不如说是一种概念。它是一个复杂的综合系统，涉及 ISP 的服务质量、通讯的可靠性以及信息的安全性。其中信息的安全性最为重要，授权和加密是两类主要的安全服务。建立 Extranet 需 Web 技术、分布式对象技术和安全认证技术的支持。在未来的二、三年里，Extranet 将成为企业的主选网络体系结构。

参考文献

[1] Georage Lawton, Extranets: Next Step for the Internet, IEEE Computer, 5, 1997

[2] The Common Object Request Broker: Architecture and Specification, OMG, July 1995

[3] Networke Working Group, RFC1777

[4] Overview of Extranet Standards Extending the Networked Enterprise, http://www.netscape.com/

[5] Security and Signed Objects, http://www.javasoft.com:80/

一、计算机安全概念

1. 计算机安全的定义

计算机安全还没有一个统一的定义。目前几个流行的定义如下：

国际标准化组织ISO的定义是："为数据处理系统建立和采取的技术的和管理的安全保护，保护计算机硬件、软件、数据不因偶然的或恶意的原因而遭受破坏、更改、显露。"这个定义虽较准确，但不够完备，它偏重于静态描述。

公安部十一局缪道期的定义是："计算机的硬件、软件、数据受到保护，不因偶然的或恶意的原因而遭到破坏、更改、显露，系统连续正常运行。"该定义注重对动态意义的描述。

计算机安全的内容可划分为物理安全和逻辑安全两类。物理安全指系统设备及相关设施受到物理保护，免受物理破坏，得以正常运行。逻辑安全包括信息保密性、信息完整性和服务可用性，其中信息保密性指信息只能由合法用户阅读，任何非法用户不能得知信息的真实内容；信息完整性指任何非法用户不能对信息进行添加、插入、删除、替换和重新排序等操作；服务可用性指合法用户请求服务时，能得到及时和正确的服务。

2. 计算机安全策略模型

在设计一个安全系统时，必须遵循软件工程开发方法，从软件需求着手。经验表明，许多计算机系统的安全控制缺陷不是因为编程错误，而是缺乏清晰的安全策略。

一个系统要获得高度安全，必须要有清晰的安全策略要求。安全策略模型的目的就是为了精确地表达那些要求。安全策略模型应具备以下几个特性：是精确的而不是歧义的；是简单而又抽象，且易于了解；它只涉及安全属性而不过分限制系统的功能和其实现；它是安全策略的明显表达。文[1]中详细介绍了各种流行的安全模型，这里简单描述如下：

状态机模型 该模型把一个系统描述为一个抽象的数字状态机，用状态变量表示机器的状态，用传送功能和操作规则描述变量如何改变。

访问矩阵模型 是状态机模型的一种。它把系统的安全状态表示成一个大型的矩阵阵列，系统中每个主体对应矩阵的一行，每个主体和客体对应矩阵的一列，在阵列中的每一位置规定每个主体对每个客体或其它主体的访问方式。

信息流模型 是访问模型的一个变种。这种模型不是检测一个主体对客体的访问，而是试图控制信息从一个客体传送到另一个客体。依据两个客体的安全属性加以限制。这种模型对寻找隐蔽通道非常有用。

非干扰模型 这种模型能限制不同域以下的主体以违反系统安全特性方式进行的相互影响。

B-L模型 是一种实用的安全模型，使计算机的操作遵循军用的多级安全策略。

二、INTERNET的安全风险

INTERNET是一个全球互联网，它包容着众多的异种网络和协议、不同的操作系统、不同类型和厂家的硬件平台，是一个非常复杂的环境，因而它的安全问题也非常复杂，主要有以下几个方面：

★身份截取 指用户的身份在通讯时被他人非法截取。

★中继攻击 指非法用户截取信息后延迟一段时间再传送。

★数据截取 指非法用户截取通讯网络中的数据。

★数据操作 指对通讯中的数据进行非法的替换、修改、插入、排序等操作。

★服务拒绝 指通讯被中止或实时操作被延迟。

★交通分析 指分析通讯线路中的信息流向、流量和流速等，从中得到有用信息。

★路由攻击 指改变信息的流动路线。

★非授权存取 指非法使用资源。

★伪装 指假冒合法用户以获取有用资源的行为。

★否认 指通讯两方有一方事后否认曾参与某次活动的行为。

面对如此多的安全缺陷，要建立INTERNET上的安全分布应用系统，该系统必须提供如下安全服务：

★维护信息的保密性和完整性。保密性指防止信息的非授权泄漏；完整性指防止数据通讯期间被非法操作(例如修改、替换、插入、删除等等)。

★提供用户和服务的认证。认证用于防止假冒的用户和服务。好的认证是存取控制得以正确实施的必要条件。不能想象连用户和服务身份真伪都无法分辨的系统的存取控制机制能有什么作用。

★提供存取控制机制。基于用户身份规定和限制用户的存取权力，尽量遵守"最小权力"原则。

★防止用户否认和服务拒绝。

安全服务由安全机制提供，下节将介绍安全机制。

三、安全机制

文[1,2]中详细讲述了各种安全机制，这里我们概述密码机制、认证机制、数据签名机制、存取控制机制和审计机制。

1. 密码机制

采用密码技术使通讯线路中的数据不被非法用户理解和伪造。它涉及两个转换算法：加密算法和解密算法。一个密码系统的强度由以下因素决定：密码空间的大小；算法是否存在后门；以及它对于密码分析的抵抗能力。目前密码机制有两种类型：对称密码机制和公开密码机制。

1)对称密码机制。该密码机制的加密算法和解密算法共用同一把密钥，加密算法和解密算法互为逆过程。该机制的主要缺点在于密钥难于管理(主要是密钥的分发和销毁管理问题)，典型的算法有DES算法。

2)公开密码机制。该密码机制的加密算法和解密算法使用各自的密钥，其中加密密钥是公开的，众所周知的，解密密钥是秘密的，只为拥有者所知道。该类算法虽没有密钥分发管理之忧，但速度慢，并且公开密钥身份的真实性需严格认证。

从上可见对称密码和公开密码机制各有优缺点，目前一般把两者结合使用，通讯双方用公开密码机制协商对称密码的会话密钥，用对称密码机制实现双方的信息通讯。

2. 认证机制

认证机制用于身份真实性的证明，它可通过指纹、口令、帐号和信用卡等来鉴别身份。认证可分为用户到主机、主机到主机和用户到用户认证。简单的认证只要提供用户帐号和口令即可，复杂的认证需有认证协议，并结合密码技术和数字签名技术。所以认证的强弱取决于协议的严格和所采用的密码系统。目前著名的认证系统有KERBEROS等。

3. 数字签名机制

该机制用于防否认，使用户无法否认自己所做的一切。它一般通过公开密码系统来实现，即发送者用自己的私有密钥解密将发送的数据以签上自己的名。由于公开密码算法速度慢，一般不对整个信息进行签名，而是对部分信息(如信息摘要，信息摘要是由不可逆的HASH算法作用于整个信息产生的)进行签名。

4. 存取控制机制

存取控制机制用于控制谁有资格存取某对象，能对对象进行何种操作，一直是主机系统的安全核心。在INTERNET上，同样存在着主机(服务器)存取控制机制，但更进一步出现了防火墙这类专门进行存取控制的设备，它们控制着内部安全网络和外部不安全网络之间的相互访问。防火墙分为报文过滤器和应用网关两类。报文过滤器一般作用于网络层和传输层，它通过检查报文头，运用过滤规则决定该报文是否可通过。报文过滤器的复杂性在于它的配置，因为很难对整个网络、通讯及应用有一个全面的了解，因而配置报文过滤器是个值得深究的问题。而应用网关一般作用于应用层，它作为应用代理控制对应用的访问，它的难点在于很难做到应用独立，即它依赖具体的应用。报文过滤器和应用网关共同的缺陷在于不防家贼和难于扩充。

5. 审计机制

审计机制是把与安全相关的事件发生记录到安全日志中，通过对安全日志的检测，来决定系统是否被入侵，现有的系统安全机制是否达到了安全防护目的，是否还需要进一步改进安全。同时，安全日志记录的信息对破案即找到系统入侵者很有帮助，这对入侵者尤其是内部入侵者是一个强有力的威慑，使他们不敢轻易作案。

从以上可以看出各种安全机制各有所长，又有缺陷，所以一个安全的系统应是针对自己的安全需求，综合且合理地运用以上机制。

四、分布系统的安全体系结构

我们不要因INTERNET众多的安全风险而犹豫不决，只要我们在连入INTERNET之前建立好自己INTRANET的安全环境，就可以把安全风险限制在有限范围内。建立安全的INTRANET环境必须做好以下几点：

★根据应用需求把INTRANET划分成两种(或更多)不同的安全域，如开放安全域和受限安全域。

★制定各安全域的安全策略，对安全要求低的安全域如开放安全域放宽安全约束，对安全要求高的安全域则严格安全约束。

★设计各安全域的安全体系结构，对开放安全域，报文过滤器和服务器操作系统就能提供足够的保护，而受限安全域的安全体系结构比较复杂，下面

将介绍。

★实现安全体系结构，并把 INTRANET 内的资源依据其安全敏感度放入相应的安全域进行保护。

建立安全体系结构就是把各种安全机制结合成一个整体，提供安全服务。一个合理的安全体系结构满足两个基本要求：①它提供一个集成的，可配置的安全功能、服务和机制集以灵活适应不同类型分布应用系统的需要。②为了隐藏实现细节，安全功能以一种通用的安全应用程序接口提供给用户和应用程序。文[4]中介绍了一种安全体系结构，在这里我们修改其存取控制机制，采用基于角色的存取控制，给出受限安全体系结构的大概框架：利用类似 KERBEROS 的服务器提供认证和基于角色的存取控制服务，通过密码模块实现保密性、完整性和防否认服务。

密码模块的构造采用分层技术和面向对象技术。在底层我们建立对称密码算法类、公开密码算法类、信息摘要生成类和随机数产生类等基本类。在高层我们直接调用或组合基本类以提供各种服务。如数字签名服务可以通过先调用信息摘要生成类生成信息摘要，然后调用公开密码算法类对信息摘要进行签名。

为什么采用基于角色的存取控制作为存取控制机制呢，从文[3]中可知，根据用户所承担的角色进行存取控制，有以下几个优点：角色及角色的层次结构使资源管理和用户管理非常方便；用户角色对应用户的职责，因而便于实施"最小权力"原则；每个角色相当于对象，因而便于采用面向对象技术。

认证服务和授权服务由三个阶段组成（如图1）。第一阶段用户获得请求授权服务的授权票证；

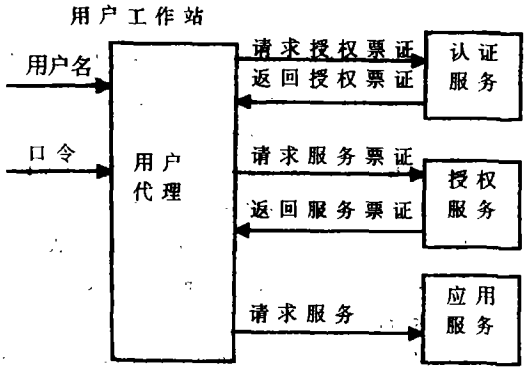

图1 认证和授权服务框架

第二阶段从授权服务处获取服务票证；第三阶段提交服务票证给应用服务器。下面将较详细地描述这三个阶段。

如同所有第三方认证系统一样，该认证服务器必须事先拥有所有用户和应用服务的私有信息，如密钥等。首先，用户被提示输入用户名。输入完毕，一个包含用户名和授权服务名的请求被发送到认证服务器。认证服务器依据用户名查找数据库看该用户是否登记。如果登记了，就产生一个用于用户和授权服务之间的随机会话密钥 K1，然后创建一个用于请求授权服务的授权票证，该票证包含用户名、授权服务名、当前时间、票证的生存期、用户的 IP 地址及刚产生的随机会话密钥 K1。认证服务器用授权服务的私有密钥加密授权票证，然后把它和会话密钥一起用用户的私有密钥加密并传送给用户。用户接收响应，用私有密钥解密，然后把会话密钥 K1和授权票证存到安全数据库中。

为了获取和使用某应用服务，客户端软件在用户登录后创建一个认证证书，该证书包含用户的名字、本机的 IP 地址和当前时间。当用户需要存取服务时，它从局部数据库取得会话 密钥 K1和授权票证。然后用 K1加密认证证书，把它和授权票证、请求的服务一起发送给授权服务器。授权服务器接收请求，用自己的私有密钥解密授权票证得到 K1，然后用 K1解密认证证书，比较认证证书和授权票证的信息以决定这次请求是否能继续下去。如果匹配，授权服务器产生用户和请求服务器之间的会话密钥 K2以及服务票证，服务票证包含用户名、用户角色、请求服务器名、当前时间、票证生存期、用户的 IP 地址和刚产生的会话密钥 K2。用请求服务器的私有密钥加密服务票证，然后用 K1加密 K2和服务票证并传送给用户。用户用 K1解密，然后用认证证书和服务票证向应用服务器请求服务。应用服务器接收请求并用自己的私有密钥解密服务票证，检查正确性，依据服务票证中的用户角色进行存取控制和提供服务。

五、INTERNET 的协议安全性

计算机网络通过协议进行通讯，不同的网络系统可能由于协议不同而不能通讯，为了互相通讯，ISO 制定了 OSI 模型，然而大家知道，INTERNET 使用 TCP/IP 协议进行互联，即 TCP/IP 模型已成

为网络互联的事实标准。下面分析 TCP/IP 模型各层协议的安全性。

1. 物理层和链路层

这两层主要涉及物理传输介质的存取和保密，在这里就不多说了。

2. 网络层(IP 层)

目前 IP 协议使用的版本为 IPv4，该协议面临着截取、信息中继、信息更改、访问拒绝、认证、非授权存取、路由攻击等危险(截取、信息更改可以通过密码机制来防止，非授权存取可通过防火墙来控制)。下面主要就认证和路由攻击来作分析。

1)认证问题。在 IP 层认证涉及的是计算机系统的认证，而非用户的认证。目前它们通过机器名即 IP 地址进行认证。上过 INTERNET 的人都知道，IP 地址是软件可配置的，这就带来了地址假冒和地址欺骗两个安全隐患。

a. 地址假冒。即当甲机器关机时，乙机器通过配置甲机器的 IP 地址来冒充甲机器。SUN 公司的 NFS(网络文件系统)是一个受此攻击的典型例子。解决的方法是避免基于地址的认证。

b. 地址欺骗。也叫 TCP 序列号攻击，它是对 TCP 三次握手协议的攻击。TCP 三次握手过程如下：

★甲发送同步请求到乙，该请求包含一个初始序列号(ISN)。

★乙收到请求后，回答一个同步号、一个 ISN 和对甲的 ISN 的确认。

★甲向乙发对乙的 ISN 的确认。

这使得第三方丙在甲关机时，伪装甲开始 TCP 三次握手过程，只不过丙必须猜出乙对甲的 ISN 值才能达到欺骗目的。解决方法也是避免基于地址的认证和使用屏蔽路由器。

2)路由攻击。路由攻击至少有两种可能：

★因为 IPv4支持源路由方式，即显示的规定信息传送的路径，这样攻击者可指定传输路线绕过障碍达到攻击目的。解决方法是取消路由软件的源路由方式。

★大多数路由协议不使用安全的认证机制，使得攻击者可以假冒路由器发送错误路由信息到其他路由器。解决方法当然是加强主机到主机的认证。

3. 传送层

传送层包括 TCP 和 UDP 两种协议，因为它们都利用 IP 报文提供的服务，因而也受到 IP 层同样的安全风险。由于 TCP 是面向连接的，而 UDP 是面向无连接的，因而 TCP 比 UDP 安全(如 UDP 更易受拒绝服务攻击)。在该层我们可以运用报文过滤器来加强安全，但要防止有缺陷的软件带来的安全漏洞。

4. 应用层

INTERNET 为用户提供了丰富的应用，而最常用的应用协议包括 SMTP(简单邮件传输协议)、Telet(终端仿真协议)、FTP(文件传输协议)。下面就介绍这些协议的安全性：

1)SMTP。它提供机器间的邮件传送服务，负责把邮件从一个 MTA(信息传送代理)传送到另一个 MTA。目前 SMTP 版本的主要缺陷在于 MTA 之间缺乏安全的认证机制，因而攻击者易发送假信欺骗和愚弄他人。

2)Telet。Telet 协议使机器仿真主机的终端，当前版本的缺陷在于：缺乏安全的用户到主机的认证；Telet 服务器接收任何用户的连接，不管是否合法，Telet 的会话信息均不保密。

3)FTP。FTP 允许用户操作服务器的文件系统，当前版本的缺陷在于：缺乏安全的用户到主机的认证；FTP 服务器接收任何用户的连接，不管是否合法；FTP 不提供信息的保密性和完整性。

从以上可见，应用协议本身的安全缺陷给安全带来了很大威胁。目前主要采取两种途径增强应用协议的安全性。一是重新修改应用协议，在协议中加入安全机制；一是在应用协议和 TCP/IP 协议之间插入一安全层，该安全层提供安全服务。

结论 从以上可以看出目前的 INTERNET 并不安全。在社会日益重视信息安全的情况下，专家们正在为建立安全的 INTERNET 而努力。我们只要充分地认识到安全问题的严重性，并严格地按照安全规则办事，就可以把安全风险限制在有限的范围内。

参考文献

[1] 殷伟，计算机安全与病毒防治，安徽科学技术出版社

[2] Actually Useful Internet Security Technology

[3] Tom Parker and Chris Sundt, Role-Based Access Control in Real Systems, Information Systems Security, Spring 1996

[4] Sead Muftic and Morris Sloman, Security architecture for distributed system, Computer Communications, 17(7)1994