计算机科学2000Vol.27№.10

计算机网络安全技术*)

Security Technologies of Computer Network

罗明宇　卢锡城　卢泽新　韩亚欣

(国防科技大学计算机学院　长沙410073)

Abstract With the development of computer network, requirements of computer network security have been more and more urgent. In this paper, goals of network security are reviewed. Several network attack methods, such as interruption, interception, modification, fabrication, are studied. Network security technologies, such as security mechanism, encryption, security detection, firewall, were discussed.

Keywords Network security, Network attack, Encryption, Security detection, Firewall

一、引言

作为一种战略资源，信息在社会生产、生活的各个领域中的作用日益显著，计算机网络的飞速发展，加强了信息的共享程度，随之而来的网络安全问题日益突出。网络如同一座不设防的城市，其应用程序、操作系统、通信协议的安全隐患比比皆是，网络安全可谓危机四伏。据权威机构统计，平均每20秒就发生一起Internet攻击事件，美国每年因计算机安全问题造成的损失高达75亿美元。

网络安全是指网络系统中各个实体进行信息存储、传输和使用等的安全。计算机网络是跨时空的，其安全问题也是跨越时空的，无论政府、公司集团还是个人在计算机网络上终究将面临网络安全的战争。

二、网络安全目标

确保网络系统极其安全是网络安全的目标。对网络系统而言，网络安全的三个中心目标是：

1. 保密性(Confidentuality)：确保数据只被授权用户访问，防止非授权用户截获并使用该数据，保证通信机密；

2. 完整性(Integrity)：确保数据在网络传输过程中不被未授权篡改；

3. 有效性(Avilability)：确保数据访问的有效性不被未授权破坏。

同时，网络安全目标还包括验证(Authentication)、认可(Nonrepudiation)和访问控制(Access Control)。验证是核实发送、接收标识一致性的过程，确保信息的真实性，证实用户是其所声称的；认可是证明信息是从发送方发出的而非来自其他地方的过程，以免用户抵赖其行为或否认曾收到信息。访问控制通过参数设置限定网络的存取访问权限。除此之外，保护硬件资源不被非法占有，软件资源免受病毒的侵害，都构成整个计算机网络的安全目标。

三、网络攻击

作为信息传输的通道，计算机网络并不提供安全的网络传输。由于网络的开放性，计算机网络面临一些独立系统碰不到的威胁。在计算机网络上，针对图1所示的信息传输服务的正常途径，大致存在四类网络攻击：

(1)中断攻击，如图2所示，这类攻击主要破坏网络服务的有效性，导致网络不可访问。主要攻击方法有中断网络线路、缓冲区溢出、死亡之Ping、单消息攻击等。

(2)窃取攻击，如图3所示，这类攻击主要破坏网络服务的保密性，导致未授权用户获取了网络信息资源。主要攻击方法有搭线窃听、口令攻击等。

(3)劫持攻击，如图4所示，这类攻击主要破坏网络服务的完整性，导致未授权用户劫持了网络会话，并假冒信源发送网络信息。主要攻击方法有数据文件修改、消息篡改等。

(4)假冒攻击，如图5所示，这类攻击主要破坏网络验证，导致未授权用户假冒信源发送网络信息。主要攻击方法有消息假冒等。

*)本文受中国博士后基金资助。罗明宇　博士后，主要研究领域：先进网络与通信技术、网络安全技术。卢锡城　工程院院士，主要研究领域：高性能计算机、先进网络技术。卢泽新　副教授，主要研究领域：计算机网络技术。韩亚欣　博士生，主要研究领域：自动化技术、系统工程。

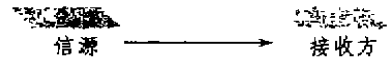

图 1 网络信息正常传输途径

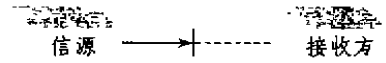

图 2 中断攻击

图 3 窃取攻击

图 4 劫持攻击

图 5 假冒攻击

四、网络安全机制

针对网络攻击，可以采用的网络安全机制包括访问控制、加密、认证交换、数字签名、业务流分析、路由控制等机制。通常，网络层的安全措施主要解决系统安全问题，包括防火墙和安全检测，防火墙是被动的，可为内部网络提供安全的边界，实现访问控制，保护系统安全；安全检测是主动的，可发现安全漏洞，防止攻击。应用层的安全措施主要解决数据安全问题，包括电子身份认证、信息传输加密、集中授权管理、审计和统计分析等。

五、网络安全技术

1. 数据加密技术

数据加密技术作为主动网络安全技术，是提高网络系统数据的保密性、防止秘密数据被外部破析所采用的主要技术手段，一般采取两种加密形式：保密密钥和公开密钥，加密算法的选择要结合具体应用环境和系统，综合考虑密钥合理分配、加密效率与系统的结合度以及投入产出分析等具体因素。

(1)保密密钥　又称私钥加密和对称密钥加密。广泛应用的数据加密标准为 DES。使用 DES 的用户和接受方采用64位密钥对报文加密和解密，在对安全性有特殊要求的情况下，应采用国际数据加密算法(IDEA)和三重 DES 等。利用密钥分发中心(KDC)可以集中管理和分发密钥，并在此基础上进行身份验证。

(2)公开密钥　在 Internet 中使用更多的是公钥系统。其加密密钥和解密密钥是不同的。用户生成一对密钥，其中一个作为公钥公开，另一个作为私钥由属主保存。常用的公钥加密算法是 RSA 算法，其加密强度高。

公钥系统结合数字签名和数据加密一起工作，发送方在发送数据前加上数字签名(用自己的私钥加密一段与发送数据相关的数据作为数字签名)，然后与发送数据一起用接收方密钥加密。接收方收到密文后，用自己的私钥将密文解密得到发送的数据和发送方的数字签名，然后用发送方公布的公钥对数字签名进行解密，若成功，则确定是由发送方发出的。数字签名与被传送的数据和时间等因素相关。

由于公开密钥系统不要求通信双方事先要建立某种信任关系或共享某种秘密，因此适合在 Internet 上使用。

(3)智能卡技术　与数据加密技术紧密相关的一项技术是智能卡技术。所谓智能卡是便携式设备，由微处理器、输入输出端口和非易失内存构成。智能卡身份验证基于用户知道的信息，用户必须持有该设备才能注册入系统。

2. 安全检测技术

作为检测外部攻击、内部攻击和授权滥用的网络安全技术，安全检测检查分析用户和系统的活动，审计系统配置的脆弱性，对非正常活动进行统计分析，识别入侵和攻击。安全检测技术是基于知识智能推理的决策分析技术，主要包括如下技术：

(1)基于模式匹配的安全检测技术　通过检查对照网络安全特征，过滤用户行为和数据，从中识别特征，发现安全漏洞。该技术的先进之处在于定义已知问题的模式，检查与模式匹配的事件和数据。入侵者的攻击往往采用一定的行为模式，如猜口令，利用行为模式可以构造具有一定特征的入侵模式，模式可以由独立事件、事件序列、事件临界值和规则表达式组成。入侵模式集的更新与新入侵的特征有关，若定义的入侵模式是通用的，新入侵实际上仅仅是入侵模式类的某个成员，那么现有模式就能检测出该入侵。

(2)基于统计异常的安全检测技术　通过检查统计量的偏差，发现入侵行为。检测前为用户、用户组、工作站、服务器、文件、网络适配器等实体定义相应的统计变量，根据历史数据和声明的期望值为每个变量建

立基值，在网络系统活动时，根据利害关系设置权函数，修改变量值，比较与期望值的偏差检测入侵行为。

(3)基于专家系统的入侵检测技术　根据安全专家对入侵行为的分析经验形成一套推理规则，进而构成专家系统自动地检测入侵行为。入侵检测专家系统的适应性较强，其实现属于知识工作问题，随着入侵经验的积累，利用自学能力扩充和修正推理规则，提高入侵检测能力。

3. 防火墙技术

作为加强网络间访问控制的网络互连设备，防火墙是在内部网与外部网之间实施安全防范的系统，它保护内部网络免受非法用户的侵入，过滤不良信息，阻止信息资源的未授权访问。

防火墙是一种基于网络边界的被动安全技术，对内部未授权访问难以有效控制，因此较适合于内部网络相对独立，且与外部网络的互连途径有限、网络服务种类相对集中的网络。防火墙的实现技术主要有：数据包过滤，应用网关和代理服务等。

(1)包过滤技术　依据系统内事先设定的过滤逻辑，检查数据流中每个数据包，根据数据包的源地址、目的地址、所用的 TCP 端口与 TCP 链路状态等实施有选择的通过。包过滤技术的实现方式有：①路由设备除完成路由选择的数据转发外，还进行包过滤，这是较常用的方式；②在工作站上使用软件进行包过滤，价格较贵；③在屏蔽路由器上启动包过滤功能。

(2)应用网关技术　基于应用层协议，利用特别的网络应用服务协议分析过滤数据包，并形成相关的报告。应用网关一般运行在专用工作站上，对易登录、控制的网络系统实施严格控制，确保网络安全。

(3)代理服务(Proxy Server)技术　防火墙网关上建立的专用代码由服务器端程序和客户端程序组成，客户端程序与代理服务连接，代理服务与将访问的外部服务器连接。与包过滤技术和应用网关技术不同，代理服务技术的内部网与外部网间不存在直接连接，实现了防火墙内外计算机系统的隔离，同时，代理服务技术可实施较强的数据流监控、过滤、日志(Log)和审计(Audit)等服务。

利用防火墙技术可以解决网络层的安全问题，但是，防火墙防外不防内，不能识别用户的身份，进行身份认证、授权管理及控制数据的存取。

结束语　互联网是庞大的信息共享系统，其网络安全问题是一个综合性课题，涉及技术、管理、使用、立法等许多方面，包括网络系统的安全问题，以及信息数据的安全问题。

在信息时代，网络安全问题越来越重要。可以预言，网络安全将是21世纪世界十大热门课题之一。

参考文献

1 Stallings W. Network and Internetwork Security Principles and Practice. IEEE Computer Society Press, 1995

2 RFC 791, Internet Protocol, 1981

3 Hare C, Siyan K. Internet Firewalls and Network Security, 1996

4 Anonymous. Maximum Security, Sams. net Publishing, 1997

5 Farley M, Stearns T. LAN Times Guide to Security and Data Integrity. McGraw-Hill Inc., 1996

6 Escamilla T. Intrusion Detection. John Wiley & Sons Inc., 1998

(上接第87页)

主要参考文献

1 Verma T, Pearl J. Equivalence and synthesis of causal models. In: Proc. of Sixth Conference on Uncertainty in AI, Boston, MA, Morgan Kaufmann, 1990. 220～227

2 Heckerman D. Learning Bayesian Network: The Conbination of Knowledge and Statistical Data. [Technical Report MSR-94-09]. 1994

3 Heckerman D. A tutorial on learning with Bayesian networks. [Technical Report, MSR-TR-95-06]. 1995

4 Heckerman D, et al. Real world applications of Bayesian networks. Communications of the ACM, 1995, 38

5 Rissanen J. Stochastic Complexity in Statistical Inquiry. World Scientific, River Edge, NJ, 1989

6 Frieman N. Learning Bayesian networks in the presence of missing values and hidden variables. In: ML'97, 1997

7 Frieman N, The Bayesian structure EM algorithm. In: Fourteenth Conf. on Uncertainty in AI, 1998