数据存取安全性 计算机网络 网络安全 (14)

计算机科学2000Vol. 27№. 10

基于网络的数据存取安全性探讨

The Researches on the Security of Data Access Based on Network Enviroment

55-58 TP 309.2 TP393.08

徐洁磐

（南京大学软件新技术国家重点实验室 南京210093）

（南京大学计算机科学与技术系 南京210093）

Abstract This paper mainly discusses the security of data storage and access based on network environment. The basic concepts, standards of data security are discussed in this paper, and the system implementation of data security is also introduced.

Keywords Network, Data security, Data security model

1 引言

计算机网络以及 Internet、Intranet 的出现与发展引发了计算机领域新的应用高潮，诸如电子商务、远程教育、远程医疗、数字图书馆。网络计算以及层出不穷的网络服务和网站使得计算机网络由少数专门人员使用成为成千上万广大用户工作与生活不可缺少的助手。但是随之而来的网络黑客、病毒以及网上的恶意攻击、诈骗、犯罪甚至利用网络盗窃国家机密，破坏军事情报等，致使网络安全已成为当前网络发展极其重要内容。

网络安全主要研究的问题是保护网上数据不受破坏及防止非法访问。对此我们可以作如下的解释：

1）网络安全所主要保护的对象是网上的数据，网络安全始终围绕着网上数据这个中心。

2）网络安全的主要内容是：数据在网上受到两方面的保护，一是数据自身不会因外界的暴力而受到破坏；二是网上数据上的访问必须受到严格的控制和管理，使得非法访问成为不可能，而合法访问则应受到保护。

基于上述两点理由可知，网络安全主要可以理解为网上数据的安全。网上数据安全性目前可以分为两个部分：网上数据传递的安全性与网上数据存储和存取的安全性，它可以解释如下：

1）网上数据传递的安全性 此类安全性主要用于保护数据在网上传递时的正确性与防止传递中的非法盗窃，对此种安全性目前可通过多种网络安全设施，如防火墙、安全路由器以及实行于网上的密码系统等方式解决。

2）网上数据的存储与存取安全性 此类安全性主要用于保护存储于网上物理及逻辑介质上的数据的安全性，以及对这些数据存取的保护，它又可简称为网上数据存取安全性，对此种安全性目前主要通过操作系统及数据库管理系统的安全性解决。

在当前网络安全性的研究中对第一种安全性已有足够的讨论与重视，而对第二种安全性——网上数据存储与存取安全性则尚未引起足够的重视，特别是对数据库管理系统安全性。本文主要探讨第二种安全性，探讨其一般性原理，特别是概念、理论、方法、标准化、系统实现等有关问题，对数据存取安全性作较为全面的研究与探讨，具体探讨四个问题：

1）数据安全基本概念；2）数据安全标准化研究与制定；3）安全数据管理系统的研究；4）安全操作系统研究。下面我们对这四个问题逐一讨论之。

2 数据安全的基本概念与内容

在传统单机方式下的数据安全与网络方式下的数据安全有着截然不同的区别，这主要表现在：

1）在网络环境下数据具有更广泛的共享性，网上用户不管是善意的或恶意的都有访问网上数据的权利，因此针对不同用户的不同数据应该制订更为严厉的共享策略并且在网络范围内执行。

2）由于网络环境下数据访问途径的复杂性，因此极易引发隐蔽通道，这对数据安全访问带来极大的影响，因此发现并堵塞隐蔽通道是网络环境下数据安全的重要问题。

3）由于在网络环境下数据安全的要求与策略的多样性与复杂性，因此建立一个理论层次上的抽象模型——即抽象的数据安全模型极为重要。这种抽象的模型可以有效地把握所提出的安全要求并填补安全上的

漏洞。为表述上的严格起见，这种模型有时可用形式化描述，它可以实现对模型形式的验证与安全漏洞的发现。

基于上面三点，网络环境下数据安全的基本概念与内容远比单机方式下要丰富和复杂，它们包括下面几个方面：

a. 可信计算基（Trusted Computing Base，又称TCB） 为实现系统安全保护策略的各种安全保护机制的集合，它是数据安全的基本概念，在下面我们将多次引用这个概念。

b. 主体、客体与主客体分离 在讨论数据安全时我们将网络上与数据安全有关的实体抽象成客体与主体两部分。所谓客体即是数据及其载体。它包括如数据表、数据视图、数据文件、磁盘区域、内存区域以及存储过程等。所谓主体即是数据的访问者，它包括如用户、应用程序、进程以及线程等。在数据安全模型中与数据安全有关的实体是独立的并且只能被标识成一种体（即或为客体、或为主体）。因此，可以将整个实体集分解成两个独立的互不相关的子集：客体（子）集与主体（子）集，这两个子集间存在着单向（由主体向客体）访问关系，它们可用图1表示之。主体、客体及主客体分离概念是数据安全的基础。

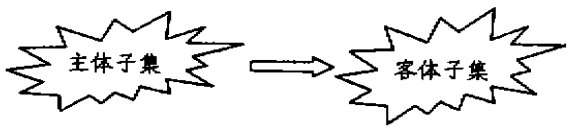

图1 主/客体关系图

c. 身份鉴别 主体访问客体前，首先要求主体用一定标志标识自己身份，可信计算基使用这些标志以鉴别用户身份，并阻止非法主体的访问。

身份鉴别用的方法很多，简单的如口令、过程等，近期常用的是密码学中的身份鉴别技术。身份鉴别是数据安全的基本内容。

d. 自主访问控制 可信计算基定义和控制系统中命名主体对命名客体的访问，实施机制（如访问控制表）允许主体规定与控制对客体的共享，并阻止非授权主体访问客体。

自主访问控制适合于在单机方式下的访问控制并允许主体规定对客体的共享控制，并且这种控制可通过主体授权形式任意改变主体访问权限。

e. 数据完整性 数据完整性即是保护数据的修改并保持其一致性，通过完整性策略阻止非授权主体修改或破坏数据，在网络环境使用完整性敏感标记以确保数据在传送中不受破坏。

f. 审计 为防止非法主体对客体的访问，需设置审计功能以记录可疑主体访问客体轨迹。记录内容包括：访问时间、用户、操作类型、是否成功等。为提高审计功能，必要时还需设置审计安全事件发生积累机制，当超过一定阈值时，能立刻发出报警，以提示应采取措施。

g. 标记与强制访问控制 在网络环境下主体访问客体时控制权应由一个统一的强制的机构管理以保证其网络下的共享性，这就叫强制访问控制，为实现强制访问控制，首先需对主体与客体作标记，标记是一个数字或一个字母集合，它分为两种，一种是安全级别（Security Level）标记，另一种是安全范围（Security Category）标记。安全级别标记是一个数字，它规定了主客体的安全级别，在访问时，只有主体级别高于客体级别时，访问才能允许；范围标记是一个字母集，它规定了主体的访问范围，在访问时只有主体的标记包含或相等于客体的标记时访问才能允许，综上所述可以看出，强制访问控制的具体操作方式如下：

·对每个主、客体打上两个标记：安全级别标记与安全范围标记；

·主体在访问客体时由TCB检查标记，只有主/客体的两种标记都符合允许访问条件时访问才能运行。

强制访问控制与自主访问控制是两种完全不同的访问控制手段，它是网络环境下实现数据安全的有效方式。

h. 数据安全模型的形式化 由于数据安全模型其内在安全关系的复杂性与多样性，因此需要建立一个有效的形式化体系，用以把握所提出的安全要求并填补安全漏洞，此种形式化系统可以实现对模型形式化验证与安全漏洞发现，还可以有效发现隐蔽通道，并且可为数据安全提供进一步研究的理论基础。因此，数据安全形式化是数据安全的重要内容。

i. 访问监控器 上述安全功能需要有一个独立的抗篡改的复杂度足够小的系统实体，以实现数据安全，这就是访问监控器，访问监控器在功能上仲裁主体对客体的全部访问。具有扩充的审计功能，提供系统恢复机制，它是一个独立的物理机构，由一定的硬件与软件联合组成。

3 数据安全标准

在网络环境中不同系统对数据安全要求是不同的，因此有必要划分成不同的安全级别，目前国际上最有名的划分标准是美国政府于1985年所颁布的TCSEC（Trustad computer system Evaluation Criteria）中所划分的四类七级标准。我国政府于1999年末颁布了信息系统安全评估标准，它将信息安全划分成五级标准，现介绍如下：

1)美国标准D级(我国标准无此级):为无安全保护的系统;

2)美国标准C_级(我国标准为.第一级——用户自主保护级),满足该级别的系统必须具有:①主体、客体及主/客体分离;②身份鉴别;③数据完整性;④自主访问控制等四项功能,其核心是:自主访问控制。C_1级适合于单机工作方式系统,目前国内使用的系统大都符合此种标准;

3)美国标准C_2级(我国标准为:第二级——系统审计保护级),满足该级别的系统必须具有:①满足C_1级全部功能;②审计功能。C_2级的核心是审计,C_2级适合于单机方式同时适合于网络方式,目前国内使用的系统大部分符合此种标准。

4)美国标准B_1级(我国标准为:第三级——安全标记保护级)。满足该级别的系统必须具有:①满足C_2级全部功能;②标记及强制访问控制。B_1级的核心是强制访问控制,它适合于网络工作方式,目前国际上有部分系统符合此标准,国内基本上尚无符合此类标准的系统,满足此类标准的系统可命名为可信系统或安全系统。

5)美国标准B_2级(我国标准为:第四级——结构化保护级),满足该级别的系统必须具有:①满足B_1全部功能;②形式化安全模型与隐蔽通道。B_2级的安全核心是形式化安全模型,它适合于网络工作方式,目前国内外均尚无符合此类标准的系统出现。

6)美国标准B_3级(我国标准为:第五级——访问验证保护级)。满足该级别的系统必须具有:①满足B_2全部功能;②访问监控器,B_3级的安全核心是:访问监控器,它适合于网络工作方式,目前国际及国内外均尚无符合此类标准的系统出现。

7)美国标准A级(我国标准无此级)。更高的形式化要求。

4 安全数据库管理系统

数据库管理系统是管理数据的软件系统,它是网络环境下数据存取安全性的主要软件,从标准的角度看,数据库管理系统的标准最著名的是美国国家计算机安全中心NCSC于1991年所发布的TDI(Trusted Database Management System Interpretation of the Trusted Computer Evaluation Criteria),它将TCSEC扩展到数据库领域,其所定义的四类七级标准与TCSEC中的四类七级标准一致,但是其基本概念的语义与具体处理方面均有所不同,它们是:

1)主体:数据库系统的主体主要指的是数据库管理系统的用户。

2)客体:数据库系统的客体主要指的是数据库管理系统的数据逻辑结构及相应数据,其具体化为表与视图,并更进一步可具体化为存储过程。

数据库系统中的数据安全模型主要框架可以用图2表示之。数据库管理系统中的自主访问控制与强制访问控制中的主、客体均以图2所示框架为准。

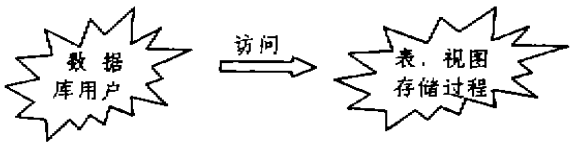

图2

3)审计:数据库管理系统的审计对象为数据库用户,审计事件为与数据库用户操作有关的事件。

在上述语义下,凡满足下列六条的数据库管理系统(即符合B_1安全级的系统称为可信数据库管理系统(TrustedDBMS):①主体、客体及主客体分离;②身份鉴别;③数据完整性;④自主访问控制;⑤审计;⑥强制访问控制。

可信数据库管理系统的六个条件中前三个是基本的条件,第四、五个条件给出了传统单机数据库管理系统(单用户/多用户)的安全性,而第五、六两个条件则给出了网络下的安全性要求。

5 安全操作系统

操作系统管理数据的物理区域,因此,有关物理区域中的数据安全性由安全操作系统负责,安全操作系统的数据安全标准基本遵从TCSEC标准,但在基本概念语义与处理上均有所不同,它们是:

1)主体:操作系统的主体主要指的是操作系统用户以及进程,近年来还包括线程。

2)客体:操作系统的客体主要指的是受操作系统管理的数据结构及数据体,它包括文件、磁盘区以及内存区等。

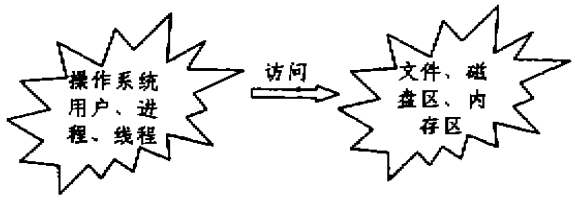

图3

3)操作系统中的数据安全模型主要框架可以用图3表示之。操作系统中的自主访问控制强制访问控制中的主、客体均以图3所示框架为准。

4)审计:操作系统的审计对象为操作系统用户,其审计事件为与操作系统用户操作有关的事件。

在上述语义下凡满足下列六个条件的操作系统

(即符合B1安全级的系统)称为可信(或安全)操作系统(Trusted OS):①主体、客体及主客体分离;②身份鉴别;③数据完整性;④自主访问控制;⑤审计;⑥强制访问控制。

可信操作系统的六个条件中前三个是基本的条件,第四、五个条件给出了传统操作系统(单用户/多用户)的安全性,而第五、六两个条件则给出了网络下的安全性要求。

6 实用的安全数据库管理系统与安全操作系统

目前国内外流行的数据库管理系统如Oracle、Sybase、Informix、SQL server等均仅符合C_1级或C_2级标准,流行的操作系统如Windows系列(包括Win 97,Win98、WinNT等)、UNIX系列(如SUN的Solaris, IBM的Aix、SGI的IRIX等)也均仅符合C_1级或C_2级标准。目前仅有少量的系统如Oracle、WinNT有符合B_1级的军用版本或安全版本,但在我国很少见到。符合B_2、B_1标准的实用系统在国内外均未见有报导。

我国正在开展数据库管理系统与操作系统的安全版本(符合B_1级)的开发与研究,如基于Linux的安全操作系统的研究,如我国自主开发的DBMS上的安全版本有DM2、Cobase以及由南京大学开发研制的SOFTBASE安全版等。

由南京大学研制开发的SOFTBASE是一个具有B_1级安全的DBMS,它不仅具有身份鉴别自主访问控制等C_1级安全的能力,还有审计及强制访问控制能力,同时SOFTBASE(SECURE)建立在南京大学研制开发的安全Linux上,这两者的结合构成了一个完整的信息安全体系,同时SOFTBASE(SECURE)有了安全的Linux支撑,其安全性能及非法通道防止能力都有了极大的提高,有关SOFTBASE(SECURE)的详细介绍及建立在安全Linux上的SOFTBASE(SECURE)的介绍可参考文献[5,6]。

小结 本文主要介绍网络环境下的数据安全问题,特别是数据存取安全,重点介绍:数据安全理论、标准与实现。且对网络环境下数据存储存取的安全性作了全面的探讨与研究,它可为我国开展计算机安全研究提供帮助。

参考文献

1 Bell-La padula L. Secure computer system: Mathematical Foundations and Model. M74－244, Bodfrod, Mass: The MITRE Corp, 1973

2 Lmpson B W. A Note on the confinament problem. Cammunication of the ACM, 1973, 16, 613～615

3 Department of Defense, Trusted computer system Evaluation Critaria. 1985

4 Sandhu R S. Role－Based Access Control Models. IEEE Computer, 1996, 29

5 Smith K. Entity Modeling in the MLS Relational Model. In: Proc of VLDB'92, 1992

6 刘启源,等.数据库与信息系统的安全.科学出版社,1999

7 徐洁磐,等. Softbase(Secure)数据安全子系统的设计与实现.南京大学学报《自然科学》,1999(4)

8 徐洁磐,等.基于安全Linux的Softbase(Secure)的设计方案探讨,南京大学学报《自然科学》,1999(4)

(上接第98页)

④在某一时刻T3,$Agent_i$与$Agent_r$进行接受回复通信:

$Communication_{T3}$(accept) | = Capability ($Agent_r$(method)) ∧ Accept($Agent_r$) =)reply($Agent_i$ ∧ $Agent_r$(method))

结论 本文提出了适用于多Agent系统进行通信的BICC结构体系,这种体系是基于最新的通信理论和多Agent意向系统理论得出的,具有广泛的使用价值,尤其是在当今运用广泛的大型数据库的更新、维护方面(比如:数据库的同步更新,预防过多冗余等)更显示了巨大的先进性。

参考文献

1 Konolige K, Pollack M E. A representationalist theory of intention. In: Bajcsy R, ed. Proc of the 13th Intl. Joint Conf. on Artificial Intelligence. California: Morgan Kaufman Publishers, 1999. 390～395

2 Bratman M E. Intenions, Plans and Practical Reason. Cambridge MA: Harvard University Press, 1987

3 Haddadi A S. Communication and Cooperation in Agent Systems Berlin: Springer, 1996

4 Rao A S, Georgeff M P. Modeling rational agents within a BDI-architecture. In: Proc KR-91, San Mateo, CA: Morgan Kaufman Publishers, 1991. 473～484

5 Rao A S, Georgeff M P. The semantics of intention maintenace for rational agent. In: Mellish C S, ed. Proc of the 14th Intl. Joint Conf. on Artificial Intelligence. California: Morgan Kaufman Publishers, 1995. 704～710