开放系统互连安全体系结构

中国电子设备系统工程公司研究所 陈爱民

摘要：各个部门为了保护各自的利益，使出了各种绝招（采取了各种技术）来保护自己的财富，同时又出现了新的问题：采用不同保护措施的用户之间的信息不能互通，网与网之间不能处理相应的业务。为了解决这个问题，国际标准化组织的计算机专业委员（*ISO TC97/ SC21*）根据 *OSI* 开放系统互连参考模型（*OSI/ RM*）制定了一个安全体系结构（*ISO 7498-2*），提出了如何对网络系统的传输信息进行保密。本文介绍这个安全体系的结构模型。

一、概述

计算机网络系统是一个大型的人机系统，它应用面广，处理的信息复杂，而且一般都有一定的密级，因此，可能会受到各方面的威胁，这些威胁主要有：

1.由于电磁泄射引起的信息失密。计算机及其外部设备和电子设备一样，当它工作时会产生电磁泄射。一台计算机就像一部电台，带有信息的电磁波向外幅射，尤其视频显示装置幅射的信息量最强，用先进的电子设备，在一公里之外的地方就能接收下来。通信线路同样也有幅射。

2.搭线窃听。非法者可能在监视通信线路（包括有线、无线、卫星等线路），非法接收信息。

3.未经授权，利用电话线拨入网络系统，来窃取数据和系统资源。目前的网络系统大都采用口令来防止非法访问，一旦口令被窃，就很容易地打入网络。

4.假冒。当合法用户从网上断开时，非法用户冒充合法用户可能乘机操纵该计算机通信接口。

5.信息可能由于意外原因传到别的终端上。

6.通过电话线路有预谋地注入非法信息。如果非法者在截到所传信息后，删除原有信息，并注入非法信息再发出，这样接收者就会收到错误信息。

7.在使用加密通信时，有可能密钥被窃。由于在现代密码学中，一切秘密寓于密钥之中，当敌对者获得密钥后，就有可能得到有意义的明文。

8.假信息可能被窜入系统，而合法信息可能从系统中删除。

9.计算机病毒对计算机网络系统的威胁。病毒是一个程序，这个程序可有多种方式嵌入计算机网络，并能自行复制，然后扩散到每台计算机，轻者使系统处理能力下降，重者可使整个系统瘫痪。

为了对抗这些威胁，需要认真研究安全保密技术。由于网络安全技术是一门新型学科，它涉及到许多领域，技术复杂，而且也只是在最近十几年随着计算机网络应用的普及才趋于成熟。在这方面，国际标准化组织做了大量的工作，如在网络系统中如何既可保证网络互通，又能保证信息安全问题等。因为计算机网络技术的发展，给政府、军事、商业等部门直接处理各种信息和业务带来了很大的方便，但同时也对所处理的信息和业务带来了威胁。于是人们为了保护各自的利益，使出了各种绝招（采取了各种技术）来保护自己的财富，同时又出现了新的问题：采用不同保护措施的用户之间的信息不能互通，网与网之间不能处理相应的业务。为了解决这个问题，国际标准化组织的计算机专业委员会（ISO TC97/ SC21）根据 OSI 开放系统互连参考模型（OSI/ RM）制定了一个安全体系结构（ISO 7498-2），提出了如何对网络系统的传输信息进行保密。下面介绍这个安全体系的结构模型。

二、安全服务的一般描述

针对网络系统的威胁，OSI 安全体系结构中提出了五类安全服务。它们是：

1.鉴别(authenti cation)

鉴别包括对等实体鉴别和数据源点鉴别。

(1)对等实体鉴别服务(Peer Entity Authentication)。对等实体鉴别服务用于当两个开放系统同等层中的实体建立连接,或数据传输阶段对对方实体的合法性进行判断,以防假冒。对等实体可以是用户与用户、进程与进程等。

(2)数据源点鉴别(data origin authentication)。数据源点鉴别服务是第 N 层向第 N+1 层提供的服务,它用以确保数据是由合法的实体发出的,以防假冒。

2.访问控制服务

访问控制服务可以防止未经授权的用户非法使用系统资源。这种保护服务同时可以提供给一个用户组(通常是一个闭合的用户群)。

3.数据保密服务(Data Confidentiality)

数据保密服务的是为了保护系统之间交换的数据,防止因数据被截获而造成信息泄密。由于开放系统互连参考模型中规定数据传输可采用连接方式和无连接方式,因此,数据保密服务也提供连接方式和无连接方式两种数据保护。为了给用户提供方便,也提供可选字段的数据保护及信息流量填充服务。

4.数据完整性服务(Data Intergrity)

数据完整性服务可以防止非法实体(用户)对正常进行数据交换的数据进行修改、插入以及在数据交换过程中数据丢失等。数据完整性服务分为带恢复功能的连接方式数据完整性、不带恢复功能的连接方式数据完整性服务,以及服务数据单元(Service Data Unit)中某些字段的连接和无连接方式数据完整性服务。

5.禁止否认服务

禁止否认服务是防止数据发送方在发出数据后,又否认自己曾经发过此数据;接收方收到数据后又否认自己曾收到过此数据。

三、安全机制

为了提供上述服务,安全体系结构建议采用下述八种安全机制:

1.加密机制

加密是提供数据保护最常用的方法。前面已经讲到,按密钥的类型划分,加密算法可分为对称密钥加密算法和非对称密钥(也称公开密钥)加密算法两种;按密码体制划分,可分为序列密码和分组密码算法两种。这些算法各有各的优缺点,所以,可根据加密的层次和加密对象采用不同的算法。

2.数据签名机制

数据加密是保护数据的最基本方法。但是,这种方法只能防止第三者获得真实数据,仅解决了安全问题的一个方面;另一方面,如果在通信双方发生下列情况时,则不能解决数据的安全问题:

(1)否认。发送者事后不承认已发送过的文件;

(2)伪造。接收者伪造一份来自发送者的文件;

(3)篡改。接收者对接收到的信息进行部分篡改;

(4)冒充。网中的某一用户冒充另一用户做为发送者或接收者。

为了解决上述问题,传统的方法是在文件上手写签名。无法使用手写签名,必须采用数据安全机制—数据签名技术。

3.访问控制机制

访问控制机制是从计算机系统的处理能力方面对信息提供保护。它是信息保护的前沿屏障。访问控制机制是按照事先确定的规则决定主体对客体的访问是否合法。当一个主体试图非法使用一个未经授权使用的资源(客体)时,访问控制功能将拒绝这一企图,并可附带报告这一事件给审计跟踪系统,审计跟踪系统产生一个报警或形成部分追踪审计。

访问控制一般以下述应用为基础:

(1)访问控制数据基。该数据基存有授权访问资源的对等实体的访问权,这个信息可由安全管理中心保存,而且可能以访问控制表、矩阵、分级或分布式结构的形式存在。

(2)口令。进入网络系统所必须的凭证。

(3)安全标记。当它与实体(程序、数据等)有关时,可用来允许或拒绝与安全有关的访问。

(4)能力表。决定主体对客体访问的权利的凭证。

4.数据完整性机制

数据完整性包括两种形式:一种是数据的完整性,一种是数据单元序列的完整性。

数据完整性包括两个过程,一个过程发生在发送实体,另一个过程发生在接收实体。保证数据完整性的一般方法是:发送实体在一个数据单元上加一个标记,这个标记是数据本身的函数,如一个分组校验(类似于 CRC

校验)或密码校验函数,它本身是经过加密的;接收实体产生一个对应的标记,并将所产生的标记与接收到的标记相比较,以确定在传输过程中数据是否被修改过。

数据序列的完整性是要求数据编号的连续性和时间标记的正确性(不是过时的),以防止假冒、丢失、重发、插入或修改数据。

5.鉴别交换机制

鉴别交换是以交换信息的方式来确认实体身份的机制。用于鉴别交换的技术有:

(1)口令。由发方实体提供,收方实体检测。

(2)密码技术。将交换的数据加密,只有合法用户才能解密,得出有意义的明文。在许多情况下,这种技术与下列技术一起使用:

- 时间标记和同步时钟;
- 双方或三方"握手";
- 数字签名和公证机构。

(3)用实体的特征或所有权。这时常采用的技术是指纹识别和身份卡等。

6.业务流量填充机制

这种机制主要是抗非法者在线路上监听数据并对其进行流量和流向分析。采用的方法一般是由保密装置无信息传输时,连续地发出伪随机序列的方式,使得非法者不知哪些是有用信息、哪些是无用信息。

7.路由控制机制

在一个大型的网络中,从源节点到目的节点可能有多条线路可以到达,有些线路可能是安全的,而另一些线路是不安全的。路由控制机制可使信息发送者选择特殊的路由申请,以保证数据安全。

8.公证机制

在一个大型的网络中,由于有许多节点或端节点。在使用这个网络时,并不是所有的用户都是诚实的、可信的,同时也可能由于系统故障等原因使信息丢失、迟到等,这很可能会引起责任问题。为了解决这个问题,就需要有一个各方都信任的第三者实体—公证机构,如同一个国家设立的公证机构一样,提供公证服务,仲裁出现的问题。

一旦引入公证机制,通信双方进行数据通信时必须经过这个机构来交换,以确保公证机构能得到必要的信息,供以后仲裁。

四、安全服务和安全机制间的关系

安全服务和安全机制并不是一一对应的。有的一种服务需要多种机制来提供,而有的机制可用于多种服务。它们的关系如表1所示。

表1 安全机理与安全服务的关系

服务 \ 机制	数据加密	数据签名	访问控制	数据完整性	交换鉴别	业务流填充	路由控制	公证机构
对等实体鉴别	y	y	·	·	y	·	·	·
访问控制	·	·	y	·	·	·	·	·
连接的保密性	y	·	·	·	·	·	y	·
选择字段的保密性	y	·	·	·	·	·	·	·
业务流安全	y	·	·	·	·	y	y	·
数据的完整性	y	y	·	y	·	·	·	·
数据源点鉴别	y	y	·	·	·	·	·	·
禁止否认服务	·	y	·	y	·	·	·	y

注:Y为该机理可以提供此项安全服务,或与其它机理结合提供安全服务;·为该机理一般为提供安全服务。

实现对实体鉴别服务可以采用系统设立的一种或多种安全机制实现,如采用数据加密、数据签名、鉴别交换、公证机制等。

访问控制的实现则采用访问控制机制的方法,如最有代表性的是采用委托监控器的方法。

- 数据保密采用对数据加密的方法。
- 数据的完整性可采用加密和数据完整性机制。
- 数据源点鉴别采用加密和鉴别交换机制。
- 禁止否认采用加密和公证机制来实现。

五、安全服务机制的配置

前面只是概括介绍了网络系统所需要的安全服务和机制。但是,一种特殊的安全服务是由一特定的层有选择地提供,即安全服务是由相应层的安全机制提供的。

这些安全服务并不是在所有各层都能实现。下面介绍各层所配置的安全服务机制。

1.物理层

物理层提供的安全服务如下：

(1)保密。

(2)业务流安全。业务流安全可采用两种形式，即：

·业务流安全。它是在双向、同时、同步、点到点情况下提供这种服务。

·限制业务流安全。根据传输数据的类型提供服务。

上述服务采用数据加密和业务流填充机制来实现。

2.数据链路层

数据链路层只提供数据保密服务。用数据加密机制实现。

3.网络层

网络层的功能主要是路由选择和报文转发。因此，该层提供的安全服务有：

(1)对等实体鉴别(路由节点和路由节点的鉴别)；

(2)访问控制；

(3)数据保密；

(4)数据的完整性；

(5)数据源点鉴别；

(6)业务流填充。

安全服务采用的机制是：

对等实体的鉴别服务采用交换(用加密算法加密的)信息、受保护的口令和签名机构的方法。

访问控制服务采用如访问控制表等访问控制机制实现。在网络层，访问控制有两种用途：允许一个路由节点控制网络连接的建立并拒绝非法的网络连接；控制一个或多个子网对网络资源的使用。

数据保密服务采用加密和路由控制机实现。

数据源点鉴别服务可把加密、签名和数据完整性机制结合起来使用。

业务流安全服务是通过业务流填充，并结合该层以下的服务来实现。

4.运输层

运输层介于通信子网和资源子网之间，起呈上启下的作用。该层提供的安全服务是：

(1)对等实体鉴别；

(2)访问控制；

(3)数据保密；

(4)数据完整性；

(5)数据源点鉴别。该层安全服务采用的机制与网络层相同。

5.会话层

会话层不提供安全服务。

6.表示层

在应用层安全服务的支持下，表示层除可提供运输层所提供的安全服务外，还可提供禁止否认服务。

禁止否认服务可采用数据完整性、签名以及公证机制的结合来实现。

7.应用层

应用层作为开放系统参考模型的最高层，为OSI用户访问网络系统环境提供手段。在这一层，由于有些应用实体是系统提供给所有用户使用的；而有些应用实体是用户自己开发，供特定用户专用的。因此，这一层的安全服务一般都是专用的，而且由于应用实体不同，所要求的安全服务不同，采用的机制也不同。例如，网络虚终端功能，由于一个端用户可以注册到别的系统，使用另一系统资源，所以需要访问控制和鉴别机制来保证系统安全；而像电子公告栏系统，则一般不要求采用什么安全措施。

另外，源点和目标点禁止否认服务的功能实际上是由该层采用公证机制或签名机制实现的。所以，在该层中，用户需要什么安全服务，都由用户决定。

为了清楚起见，表2列出了安全服务和层的关系。

表2　安全服务和层的关系

	层　次						
服务	1	2	3	4	5	6	7*
对等实体鉴别	N	N	Y	Y	N	Y	Y
访问控制	N	N	Y	Y	N	Y	Y
数据保密	Y	Y	Y	Y	N	Y	Y
数据完整性	N	N	Y	Y	N	Y	Y
业务流安全	Y	N	Y	N	N	N	Y
数据源点鉴别	N	N	Y	Y	N	Y	Y
禁止否认	N	N	N	N	N	Y	Y

注：Y—是，表示该层可提供安全服务

N—不，该层一般不提供安全服务

*—原则上讲，六种安全服务都可在第七层实现。

1.安全管理的作用

在一个分布式开放系统，安全管理主要是由行政管理机构施实的，它主要包括：

(1)在通信实体上施实强制安全策略。

(2)允许实体确定与之通信的一组实体的自主安全策略。

(3)控制和分配信息到提供安全服务的各类开放系统中，报告所提供的安全服务，以及已发生与安全有关的事件。例如，在一个实体连到系统之前，分配给该实体访问权的信息就是安全管理的业务。

(4)在一个实际的开放系统中，可设想与安全有关的信息将存储在文件或表中，这些文件和表被认为是一个安全管理数据基(SMIB)。由于系统的结构不断变化，实体在不断变化，这样，安全数据基也要不断变化，因此要对它进行管理，这也是安全管理的业务。

2.安全管理的内容

(1)鉴别管理。鉴别管理包括分配描述性的信息、口令或密钥到要求实现鉴别的实体的过程。也可包括相互通信实体间采用的协议以及提供鉴别服务的其它实体。

(2)访问控制管理。该问控制管理包括分配口令和修改访问控制表、能力表，也可包括通信实体间协议的使用和提供访问控制服务的其它实体。

(3)密钥管理。在系统中只要采用加密机制，就需要有密钥管理。钥管理包括：

·定期产生相应安全等级的相应密钥；

·根据访问控制要求确定哪些实体可以接收密钥副本；

·在实际的开放系统中以秘密方式把密钥分配到各实体。

在对密钥进行管理时，可采用手工和自动相结合方式。在采用自动分配方式时，需要用加密算法来保护(如采用对称和非对称密钥加密体制)。在采用非对称密钥管理体制对密钥进行管理时应考虑下列问题：

·每个密钥都有一个基于时间、用法和其它准则的隐含或显式的“生存时间”；

·概括功能要求，应把数据加密密钥和密钥加密密钥区分开来，而且把它的应用限制在相应的功能上；

·不同的应用应采用不同的密钥管理体系结构。

在采用非对称密钥密码体制时，至少有一个密钥是保密的，而其它密钥可以是公开的。这种密钥可由可靠的第三者来保存。

(4)安全恢复的管理。在系统出现安全方面的问题时，如何尽快使系统恢复正常等。

3.安全审计跟踪

审计跟踪管理包括：远程事件收集的报告，以及允许和不允许对选择的事件进行审计跟踪。在OSI环境下，可审计的事件是妨碍系统安全的各种企图。另外还有选择记录或收集的事件，启动或解除审计跟踪的事件等。

参考文献：

1.ISO / 7498-2, 1989。

2.computers&security, 1985—1992。