EDI 系统中的数据安全防护设计

秦荪涛 王涛 （浙江财经学院信息系 310012）

摘要：文章通过数据保护、数据加密、存取控制等办法对 EDI 系统进行控制，防止各种有意或无意地对系统的破坏，以及防止系统信息不正常泄漏。

关键词：EDI 系统 数据保护 数据加密 安全防护

在 EDI 系统中，有大量涉及客户双方权益甚至国家机密的数据信息在网络的各计算机系统上输入、处理、存储，并通过有线或无线信道传输。数据信息和系统的安全，直接关系到国家经济、政治利益，若不采取有效措施，将会给国家带来极大的损失。在危及系统安全的因素中，有软硬件系统不可靠、用户误操作和难以克服的自然灾害；但更重要的是，有意破坏者采取各种手段截获数据信息或伪造信息，盗窃国家经济情报，盗窃国家资金，破坏系统的正常运行。因此，一定要设计必要安全防护措施，以保证 EDI 系统的正常运作。本文就数据保护作一些讨论。

一、数据加密

所谓数据加密，指的是通过加密算法，存储数据或传输数据时，在密钥的控制下将明码数据转化为密文数据，当取数据或接收数据时，在将加密的密文数据在相应的密钥控制下转化成明码数据。于是在数据加密中，加密算法和密钥就有着其举足轻重的地位，加密算法的设计原则应遵循“秘密寓于密钥”的原则，也就是说，既使别人对加密算法了如指掌，但无当时所用的密钥，也将无济于事。加密算法应设计得除了用穷举法将每个密钥逐一试验外，若无密钥的话将没有其他办法将密文数据还原成明码数据。

有了一个好的加密算法之后，密钥的安全就是我们要着重考虑的问题了，密钥的安全取决于包括密钥的产生、存储、分配、注入、使用、更换和销毁等所有细节。在密钥管理过程中，要配备专门人员掌管记录密钥的媒体的注入器，密钥一旦注入密码设备以后，任何人都不能将这密钥从密码设备内读出来；密钥应定期更换调整；不能在不同的密码设备中用相同的密钥；系统将通过通信网络动态地自动或手动地分配各种密码设备的密钥。每处密码设备的主密钥由专职人员进行分配，并确定使用期限。在通信时，每次通信由密码分配中心给通信双方分配一个随机密钥。由于这个密钥要在通信线路上传输，所以必须要用通信双方的主密钥分别对该次会话密钥进行加密以后再进行传输，当通信完毕，这个通信密钥马上删除。相应地，加密存储数据的密钥也与数据存储期相适应，随着存储数据的删除而删除。

下面我们再来讨论传输数据加密和存储数据加密。

二、传输数据的加密保护

传输数据的加密保护措施可从两种方面入手：一种是对线路的链路加密；一种是端－端加密。链路加密方法是通过单独保护每条通信线路传输的数据流来进行安全防护，对通过两个节点之间的数据，均进行独立地加密防护，每条通信线路都有不同的加密密钥。因此，即便是一条线路失密，并不泄露其他线路上传输的数据。这种方法只对线路上传输的数据加密，而在节点内部没有加密，如果破坏节点就完全暴露了通过该节点的数据秘密，所以采用这种方法，还应配有相应的节点物理安全保护措施。另一种端－端加密法，则是网络提供从信息源结点传送数据的加密，在这种方法下，任何线路遭破坏，都不影响数据的保密性。端－端加密的实现也比较灵活，可以从主机到主机，也可以从终端到终端等。用这种方法加密，每个用户或主服务器都可以单独进行加密，而不影响其他用户主机，这种方法很适合分组交换网络，用户可以根据需要进行加密。

三、存储数据的加密保护

为了做到既能防止文件被非法拷贝，又要保证文件可以正常运行，防止信息的泄露和破坏，需要区别不同情况进行加密保护。通常我们采用以下一些措施：

1.分散授权

根据安全性策略设置分层授权机构，逐层授于存取权力或撤销其存取权力。为了实现分散授权，我们制定一个统一的存取规则表，将每一种规则存放在同一结点上当作数据一样对待。当复制数据时，该数据的存取规则也被复制；在撤销一个存取权力时，有关其存取规则的每一个副本也都予以删除，并在全部节点间通信，保证撤销的有效性。采用这种方法可以减少不必要的数据传输量，提高处理效率。

2.重点保护机密数据

对一些机密数据设置安全标志，在分片处理某个元组时，如发现该元组包含了这类机密标志，则在调用该元组时就要按其所含的密级处理。在调用具有安全标志的元组时，如果是该元组不属于安全节点的本地关系，则一是对该元组中的机密数据加密，二是在提供整个元组的信息时，将该机密数据作空值(NULL)处理。其目的在于重点保护机密数据。

3.区分节点、重点控制

将EDI中的网络节点，区分为安全节点和普通节点两类，将安全性控制的重点放在普通节点上，对安全节点上的本地关系作本地处理，而对普通节点上的关系加强保护措施。

这里所谓安全节点是由安全操作系统支持，能够在不同的安全级别上运行各种进程。而普通节点则必须在指定方式下运行，其全部进程及数据必须处于同一安全级别上。如果要在普通节点间的不同安全级别上通信，则允许有较高安全级别的节点进程对较低安全级别上的节点进行访问，否则的话，须先发出消息，请求得到确认后，方才可以访问。

四、存取控制与数据完整性鉴别

这是数据在处理过程中的保护办法。它包括存取资格检查、存取保护、数据存取保护和防止存取信息的破坏等几个方面。

存取资格检查是对用户的存取资格和存取权限进行检查。在EDI系统中，用户终端用设备号标识。只有存取资格被主计算机检查合格的用户，才有权进入系统，执行与其身份相适应权限的操作；否则系统将报警并拒绝执行。用户的识别有三种方式：用户口令PW(PASSWORD)，用户标识号PIN(PASS IDENTIFIER NUMBER)，物理密钥标识等。用户权限控制用以确定用户使用系统的权限等级。在数据库系统中，用户定义自己的子模式和所包含的数据类有不同权限范围，用户只能在权限范围内存取数据、使用程序，越权应用则被视为非法。

存取保护分为内存保护和外存保护两种。

所谓数据完整性鉴别，是采用密码技术，通过对个人身份、传输报文和存储数据的参数进行鉴证、以保护数据免遭非法存取和蓄意的人为破坏。它包括通信双方身份验证和报文鉴别，以及在存取过程中对用户身份和主机密钥的鉴别。

五、利用操作系统进行安全控制

通过特权指令、重定位和界限寄存器、分段、分页等技术，实现对计算机资源的合理分配，并将用户的程序和数据管理起来，避免相互间的干扰和分时冲突，将一些重要的操作定义为特权操作，由特权指令而不是一般用户指令来完成，以保护系统资源免受有意或无意的破坏。

为避免一般用户闯入系统，系统的所有数据要脱离用户工作区，同时检查用户向管理程序传递参数的有效性，操作系统应提供有效的内存保护手段、防止进程之间的干扰、避免用户对系统的非法访问。

六、运用分片处理技术实施数据保护

在传统的分片技术处理中，主要是在传输代价与本地处理代价之间进行权衡，而没有将安全性作为一个主导因素考虑。其实，在有的情况下，将字段的安全性作为一个条件来考虑会改善片段处理的性能。在制定分布标准时，可以将安全级别作为一个控制考虑，在作不传送关系的选择时，可将含有安全级别最高的元组选定为不传送关系，使它在安全节点上化为本地关系处理；在分裂查询时，设法将含有机密字段的关系作为变量组合的限制条件。这样，一来减少了各种可能组合的数量，二来又可重点保护机密字段。

七、数字签名

随着计算机网络技术的迅速发展，远隔两地的用户双方，完成某项谈判或传达上级对下级的指示，必须有签了字的书面文件，以便事后查询，分清责任。而现如今，人们传统的传递手签文件的方法，已经不适应EDI系统的要求了，于是提出数字签名的方法。数字签名的要求与传统的手写签名一样，签字者事后不能否认签过名的报文；收件方也不能伪造签字方的报文。我们采用的方法是，签字方和收件方使用相同的密码算法，加密密钥双方公开，但解密密钥各自保管。当签字方向收件方发送一份签名报文时，将签字方的身份、收件方的身份附在报文上，并用自己的保密密钥进行加密运算；收件方则用签字方公开的加密密钥进行解密，达到手写签字同样的效果。

为了增强EDI信息交换系统的安全性和保密性，很多国家的一些信息交换协会都致力于研究对抗各种有意识犯罪行为的措施，采用了各种方法，如IC卡、动态口令、密钥管理中心等等。IC卡是在用户的卡上赋以某些运算功能，将原来需要在终端上进行的运算转移到卡上运行，可以大大降低PIN的泄露；而动态口令则是对用户的每次请求交易，使用不同的口令；密钥管理中心统一负责产生、分配每次交易的密钥，如美国国家标准局标准DES等，以增强系统的保安防护能力。

总之，随着EDI系统的进一步发展，人们将愈来愈重视其安全可靠性和保安防护措施。

(来稿时间：1998年2月)