电子商务安全体系结构

Security Architecture for Electronic Commerce

张 峰 秦志光 刘锦德 张险峰

(电子科技大学计算机学院 成都610054)

Abstract Electronic commerce operates relying on the open Internet. Security architecture for e-commerce becomes the key point to its use prosperously. A finite automation of typical e-commerce model is presented in this paper. The finite automation simulates typical trade system, describes its states transition and supplies a theory basis for designing security architecture for e-commerce. Then security threats and corresponding solutions to the model are discussed. Finally, the security architecture for e-commerce is given. All of them are used as basis for further e-commerce security research.

Keywords Electronic commerce, Security threat, Trade model, Finite automation, Security architecture

1 引言

电子商务将成为21世纪人类对信息世界关注的一个焦点,也将是网络应用中极为重要的一个发展方向。但是,网络欺诈、窃听、病毒和非法入侵都在威胁着电子商务的使用。电子商务安全技术是电子商务得以推广和应用的关键,是必须考虑的核心问题。同时,由于安全技术的特殊性,以及出于别国封锁和自身安全性的考虑,安全技术必须自主研究。随着我国电子商务的发展,电子商务安全技术将会有巨大的市场需求。在研发具体的电子商务技术和产品之前,首先要解决的是电子商务的安全体系结构问题。

2 电子商务的安全威胁与安全需求

电子商务至今尚没有一个统一的定义,我们从几个方面对其加以表述。电子商务是指实现整个贸易过程中各阶段的贸易活动的电子化。从涵盖范围层面可定义为:交易各方以电子交易方式而不是通过当面交换或者直接面谈方式进行的各种商业交易;从技术层面可理解为电子商务是一个包括交换数据、获取数据、自动捕获数据等多种技术的综合体。

电子商务实现环境由企业内部网,外部网,互联网组成,每部分的安全薄弱点都可能为敌方利用、攻击,成为整个系统的潜在安全隐患。对常见的安全威胁及初步对策简述如下。

·对系统用户的攻击 网络用户的身份通过数字证书鉴别,内部用户一般是拥有数据管理权限的用户,因此对其权限的管理更为重要。内部用户的鉴别和审计现在一般采用操作系统用户加操作日志的方式。可对这种方式作一加强:对于某些特定的操作绑定到特定的控制台上进行,而且工作台的场所信息通过一个场所证书来唯一地标识。

·通过应用程序对系统的攻击 通过一些常见应用的安全漏洞对系统进行攻击。如sendmail,unix的r系列命令。解决方法是修补安全漏洞或去掉那些有潜在安全威胁的网络应用。

·针对Java平台的攻击 在开发大型企业应用方面,Sun的J2EE规范得到越来越多的支持。商家的应用服务器和交易服务器将采用Java语言开发。J2EE规范把安全代码的开发和支持都留给了应用服务器平台提供商,而EJB server的安全性归根结底依赖于Java语言的安全机制。通过Java平台的安全机制对应用系统进行攻击的的案例详见文[5]。

·CA和PKI的安全问题 有关CA和PKI的问题,涉及政策、法律、技术等多方面因素,目前还没有成型。下面仅对它所包含的安全方面的技术问题加以讨论。

如果用户的私有密钥遭泄露,敌方可以冒充该用户读取加密信息,对信息进行签名,签署合同等。这时,公开密钥库必须立即声明与特定的公钥相关的私钥已经泄露。如果是CA的私钥泄露,情况就更为严重:敌方可以任意伪造证书,还可以掌握CA所知的一些用户秘密信息。此时,所有由这个CA签发的证书都要作失效处理,并且重新为所有用户签发证书,这种开销往往是很大的。造成的破坏范围也大得多。

PKI提供的安全服务建立在私钥的保密之上。一旦用户的私钥被窃取,将发生严重后果。PKI系统中对PSE的保护,其实也是对用户私钥的保护。对私钥的保护问题,是整个公钥密码体制的薄弱点,必须在这方面有所加强,最终用户对此也应有清醒的认识。保护私有密钥可采用密码保护、内存卡保护、智能卡保护等方法。考虑到私钥的安全性,须对私钥定期替换,而且旧的私钥还要定期销毁,因为攻击者可以利用旧密钥解密以前的加密信息。对密钥彻底的销毁,涉及到销毁硬盘、内存、EPROM、临时文件、交换文件中的所有旧密钥的副本。

由于电子商务的工作特点及其重要性,必须提供一定的安全服务对电子交易加以保障,确保电子商务与传统贸易同样的安全可靠。对电子商务的安全需求分析如下:

电子商务的数据信息关系到个人、企业的经济利益,因此确保信息的有效性(Availability,即用户需要时可以立即取到)是电子商务应用的前提。需要对网络故障、系统错误、操作错误可能产生的影响进行有效的控制和防范,保证交易信息在确定的时间和地点是有效的;第二,电子商务的交易信息代表个人、企业的商业机密,需要保障在开放的互联网上传送的交易信息的数据机密性(Confidentiality),保证交易信息不被

张 峰 博士生,主研方向:网络安全主动防御技术、电子商务安全技术。秦志光 教授,博士,主研方向:网络安全、办公自动化。刘锦德 教授,博导,主研方向:开放系统与中间件、网络多媒体技术、实时分布式处理技术。张险峰 博士生,主研方向:ECC、IDS。

未授权者访问，是电子商务安全的基本要求之一；第三，交易信息在传送过程中的重发、篡改和删除造成双方交易信息不一致。因此，应保障信息在传送过程中未被篡改、删除——维护交易双方的信息完整性(Integrity)；第四，必须确定正在交易的双方是期望的交易双方，而不是冒名顶替者。因此，需要一套系统来标识交易的双方，作为身份鉴别(Authentication)的依据；第五，应使电子商务交易中的各方能进行交易系统期望的操作且不能进行未被授权的其它操作。这就需要提供一种方法对资源的读取、修改、使用加以授权，使特定的用户或应用能以特定的方式访问目标对象，也即提出了访问控制(Access-Control)的基本需求；第六，在一次交易发生之后，电子商务需要一种机制保证当事各方不能否认提交了该交易。这就是防抵赖(Non-repudiation)需求。在无纸化的电子交易中采用数字签名作为证据，来保障发送一条消息后不能否认；第七，根据数据机密性、数据完整性和不可否认性的要求，电子交易过程还需要提供审计功能(Aduit)，以对数据操作的结果进行审计，对日志进行审查。

3 典型电子商务交易的有限自动机模型

在研究电子商务安全体系结构之前，我们通过分析典型的电子商务交易过程勾划出电子商务交易环境的概貌，引出其中的安全薄弱点。为描述的简洁清楚，这里采用形式化描述方法确定型有限自动机来描述电子商务交易模型。

有限自动机是一个五元组：$M=(K,\sum,\delta,q_0,F)$，其中，M 表示有限自动机；K 是状态的有限集；$\sum$ 是有限字符集；δ 是 $K\times\sum$ 到 K 的一种映射；q_0 是初始态，$q_0\in K$；F 是终集，$F\subseteq K$。确定型有限自动机每个状态的后继状态是唯一的。

若当自动机处于状态 q，并输入字符 a 后，M 转换到状态 p，则记为 $\delta(q,a)=p$。有限自动机的工作情况可用状态转换图来表示。

对于典型电子商务交易模型用有限自动机 $M=(K,\sum,\delta,q_0,F)$ 表示之前，首先进行符号定义：

$K=\{q_0,q_1,q_2,q_3,q_4,q_5,q_6,q\}$；

其中，q_0 为初使状态，q_1 为客户与商家的交易服务器建立连接(包括认证、密钥分配、访问控制)；q_2 为用户购物并将购物信息发给商家；q_3 为支付信息发送给支付网关；q_4 为支付信息发送到收单银行(商家的帐户银行)；q_5 为收单银行向发卡银行(用户的帐户银行)校验用户的支付能力，且返回校验结果到商家；q_6 为商家发起收单行与发卡行间的划帐操作，并向客户开具电子票据；q 为划账操作成功，一次交易结束。

$\sum=\{0,1\}$，1/0表示操作成功/失败；$F=\{q\}$；

映射 δ：$K\times\sum\to K$ 为：

$\delta(q_0,0)=q$　$\delta(q_0,1)=q_1$

$\delta(q_1,0)=q_0$　$\delta(q_1,1)=q_2$

$\delta(q_2,0)=q_1$　$\delta(q_2,1)=q_3$

$\delta(q_3,0)=q_1$　$\delta(q_3,1)=q_4$

$\delta(q_4,0)=q_1$　$\delta(q_4,1)=q_5$

$\delta(q_5,0)=q_1$　$\delta(q_5,1)=q_6$

$\delta(q_6,0)=q_1$　$\delta(q_6,1)=q$

该自动机状态转换图如图1所示。

用户登录商家网站时，自动机 M 从 q_0 状态转换为 q_1 状态。用户退出系统时，M 转换为 q 状态。在 q_1 状态，进行用户和商家之间的身份认证、访问控制、密钥分配工作。若成功建立了用户与商家的连接，则接受用户请求，M 转换到 q_2 状态；若连接建立失败，则 M 转换到 q_0 状态。在 q_2 状态，若用户购物信息成功发送给商家，则 M 转换到 q_3 状态；若失败，则 M 转换到 q_1 状态。在 q_3 状态，若支付信息成功发送给支付网关，则 M 转换到 q_4 状态；若失败，则 M 转换到 q_1 状态。在 q_4 状态，支付信息发送到收单银行，若成功，则 M 转换到 q_5 状态；若失败，则 M 转换到 q_1 状态。在 q_5 状态，收单银行询问发卡银行，得到发卡银行的答复，若成功，则 M 转换到 q_6 状态；若失败，则 M 转换到 q_1 状态。在 q_6 状态，收单行与发卡行间进行清算操作，若成功，M 转换到 q 状态；若失败，M 转换到 q_1 状态。对上述模型中潜在的安全威胁分析如下：只有从状态 q_6 到状态 q，是利用现有的金融专网，不涉及过多的安全性问题，而其它的状态转换过程($q_0\leftrightarrow q_1$，$q_1\leftrightarrow q_2$，$q_2\to q_3$，$q_3\to q_1$，$q_3\to q_4$，$q_4\to q_1$，$q_4\to q_5$，$q_5\to q_1$，$q_5\to q_6$，$q_6\to q_1$)都必须经过开放的 Internet。从状态 q_3 到 q_4，和 q_4 到 q_5，包含用户信用卡号和口令的信息将经过无数没有保障的节点存储和转发，若缺乏相应的安全技术，将对其数据机密性、完整性造成威胁，而且也易遭到重放攻击。从状态 q_1 到 q_2，须完成对交易各方进行身份认证，否则无法保证交易各方不是顶替者。从状态 q_2 到 q_3，需对订货信息和支付信息进行签名，确保发方的真实身份且交易完成后发方无法抵赖。这里使用数字签名的有效性和法律效力，则由相关的签名法、电子商务安全法规提供保障。

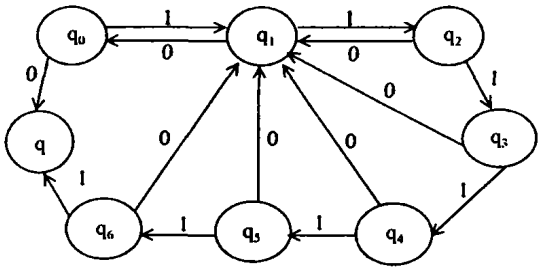

图1　典型电子商务交易模型的有限自动机 M 状态轮换图

4 电子商务安全框架

通过分析电子商务的交易模型及安全需求，在研究 OSI 安全体系结构时，我们认为电子商务安全框架是由安全基础、安全机制、安全服务、电子商务应用构成的多层次复合结构。如图2所示。

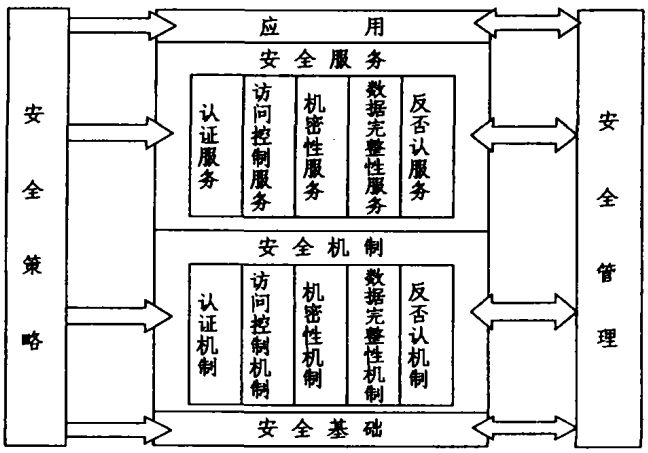

图2　电子商务安全框架

在上图中，安全基础体现为各种底层算法。如各种对称密钥算法、公开密钥算法、HASH 函数等。本层是最基本的安全技术。为安全机制层提供算法支持和其它服务。

安全机制是实现安全服务的具体软件或芯片，它为上层安全服务提供具体的实现方法。它包括了加密机制、数字签名机制、访问控制机制(访问控制表机制、基于能力和安全标签的访问控制机制)、数据完整性机制、路由控制机制、安全审记与追踪机制等。

在安全机制的基础上，形成了安全服务，体现为一系列安全协议。主要包括五种通用的安全服务。认证服务，提供对某个实体(人或系统)的身份的保证。如对等实体的的认证服务、数据起源认证服务等。认证服务是最重要的安全服务，因为其它的安全服务都在一定程度上依赖于认证服务；访问控制服务，防止对任何资源进行未授权的访问；机密性服务，保护信息不被泄露或暴露给未授权用户，如连接机密性服务、无连接机密性服务；数据完整性服务，防止对数据进行未授权的改变、删除或替换，如可恢复的连接完整性服务、不可恢复的连接完整性服务、无连接完整性服务；反否认服务，防止参与某次通信交换的一方事后否认本次交换曾经发生过。如数据起源的反否认服务、传递过程的反否认服务。一种安全服务的实现可能会需要下层的几种安全机制的支持。例如机密性服务，就包括握手协议、密钥生成、密钥交换协议，需要下层的密钥产生、密钥交换机制予以支持。

安全管理指与安全相关的基本数据的管理。如密钥和证书的生成、交换、替换等。

安全策略定义了在一个通信资源集合之上、用于所有与安全行为相关的一套规则。这套规则主要包括三方面主要内容：保护的目标，如何保护，付出的开销。安全策略的详细制定将涉及安全框架的各个层次。在应用层，我们指出针对某一特定应用进行访问控制。由于不同的安全机制及其组合提供不同级别的安全服务，因此需要综合考虑应用所带来的效益和提供安全服务的开销，共同确定采用何种安全机制甚至底层的基本算法以提供所需的安全服务。

在整个电子安全框架中，底层的安全基础提供算法支持。基本安全机制和扩展的安全机制通过使用特定的加密算法、数字签名算法、HASH 函数、随机数发生器等提供安全服务的具体实现。安全服务则表现为若干协议，电子商务具体应用通过遵循这些协议使用安全服务，从而防范电子商务交易环境中出现的各种安全威胁。安全管理则提供了对电子商务应用、安全服务、安全机制中所涉及的基本安全数据的管理和一定的人员管理。同时，为实现安全电子商务必须提供一整套安全策略明确描述对何种资源进行何种保护，这套策略覆盖到安全框架的各个部分，一般还会包括政策和制度因素在里面。上文提到的电子商务七个基本安全需求，映射到安全框架中的六种安全机制和对应的上层五种安全服务。该安全框架是实现安全电子商务的理论框架，可为设计和实现具体的电子商务安全技术提供理论指导。

目前的问题和下一步的工作 值得关注的是，我们只是提出了一个安全框架，要完全实现该框架还存在一些困难。这主要是：电子商务的复杂性，涉及交易活动的种类和需求多，相关的法规尚不健全；技术上还存在一些难点。如 Java 平台固有的安全漏洞，已知的操作系统漏洞等。另外，随着应用技术和安全技术的发展，上述安全框架也不是一成不变的，它在每一层中都留有扩展余地，应视具体情况有所调整。电子商务安全性已经引起学术界、企业界的广泛关注，并在相关的安全技术方面取得了一些成就。但是相关的安全技术还很不完善，多项研究尚处于探索阶段，我们可以在此领域有所突破。

参 考 文 献

1 Kou Weidong. Networking security and standards. Kluwer Academic Publishers

2 Schneier B. Applied Cryptography Protocols, algorithms, and source code in C(Second Edition) 应用密码学：协议、算法与 C 源程序(第二版). 机械工业出版社

3 Stallings W. Cryptography and Network Security Principles and Practice Second Edition 密码编码学与网络安全：原理与实践(第二版). 电子工业出版社

4 冯登国著. 计算机通信网络安全. 清华大学出版社

5 Li Gong 著，王运凯等译. Java2平台安全技术——结构、API 设计和实现. 机械工业出版社

6 Tang Zheng. Introduction to E-Commerce. 人民邮电出版社

7 秦志光，刘锦德. 安全系统的有限自动机. 电子科技大学学报，1996，25(1)：72～75

8 秦志光，刘锦德. 客户与服务器之间的安全交互作用. 电子科技大学学报，1996，25(1)：69～71

(上接第120页)

还是内部的证书操作员执行了非法操作。如果是内部证书操作员执行非法操作，可以删除这个证书操作员，即从系统人员表中删除这个证书操作员的身份，甚至撤销他的证书。

数据库中保存了本 CA 系统中的所有信息，其自身的安全性也需要考虑。最简单地说来，可以设置一个备份数据库。将 CA 服务器直接访问的数据库和系统管理员通过数据库前端管理程序查询管理的数据库分开，减少对数据库的有意或无意的破坏。另外，从入侵检测的角度考虑，可以对数据库中的数据计算完整性校验值。每次存入数据项时，计算并存储完整性校验值，在需要时再对数据进行完整性检查，保证数据库自身的安全性。

结论 公钥基础设施 PKI 是个功能强大、结构复杂的系统，系统中有大量的数据需要存储、发布和管理。PKI 系统中信息的发布有很多种方式，域间数据的共享和系统的安全性也有很多考虑。在证书库的构建问题上，我们综合考虑了使用的方便性和安全性，同时还考虑了系统自身的安全性。我们对于信息的发布综合采用了数据库和目录服务器的方式，对于域间数据的共享综合采用了共享数据库、复制数据库和边界数据库的方式，成功地构建了我们的 RealCert 多级 CA 认证系统。

参 考 文 献

1 Adams C, Lloyd S. Understanding Public-Key Infrastructure : Concept , Standard , and Deployment Considerations. Macmillan Technical Publishing, 1999

2 RFC2251 Lightweight Directory Access Protocol (v3) 1997

3 ITU-T Recommendation X.500 (1997)-The Directory: Overview of concepts, models and services