文章编号:1005-0523(2003)02-0078-05

实时网上交易的数据安全方案探讨

左黎明

(华东交通大学 基础科学学院,江西 南昌 330013)

摘要:提出了一种新的网上交易方法,并给出了这种方法的实现步骤,拓展了电子商务的功能.并且针对这种网上交易方法中的数据安全问题进行了深入探讨,提出了相应的解决方案,该方案便于实施而且具备高安全性和可行性,可以满足实际应用的需要.

关 键 词:实时网上交易;数据安全;加密;解密;数字签名;Deffie-Hellman协议;DES;RSA

中图分类号:TP393.08 **文献标识码**:A

0 引 言

21世纪信息时代的到来,商务网络化的趋势日渐明显,网络已逐步改变着人们生活方式和思维方法.然而电子商务的广泛展开,网络犯罪时有发生.黑客攻击、网络诈骗、网络盗窃给世界贸易每年带来了上十亿甚至上百亿美元的经济损失.没有信息安全也就没有电子商务交易的信誉,没有信誉也就不可能开展电子商务,因此信息安全是实现电子商务的最核心的部分,是网上交易的关键.传统的电子商务的形式是静态的,不管是B2B或者是B2C.如果我们能够实现动态的网上交易即实时网上交易,就将引入电子商务的一个新的激励动源.本文我们将主要探讨的是实时网上交易中的数据安全问题,并加以实现.

1 实时网上交易的过程

实时网上交易的工作流程与实际贸易的过程非常接近.贸易双方登陆网上交易平台,然后进行只涉双方的贸易洽谈,洽谈成功后买方进行网上订购(当然可以是订购货物或者是服务),卖方进行确认,一直到所定货物送货上门或所定服务完成,然后帐户上的资金转移,所有这些都是通过Internet完成的.我们把这一过程称为实时网上交易.其具体流程为:

1) 交易双方登陆网上交易平台;

2) 买方根据贸易类型和要购买的商品在网上交易平台选择交易对象;

3) 买卖双方进行实时贸易谈判;

4) 谈判成功双方确认交易;

5) 买方选择付款方式,发送给卖方一个完整的定单及要求付款的指令,定单和付款指令由买方进行数字签名,同时利用双重签名技术保证卖方看不到买方的帐号信息;

6) 卖方接受定单后,向买方的金融机构请求支付认可.通过网关到银行,再到信用卡机构确认,批准交易.然后返回确认信息给买方;

7) 卖方发送定单确认信息给买方.买方端软件可记录交易日志,以备将来查询;

8) 卖方给顾客装运货物,或完成订购的服务.

到此为止,一个网上交易过程已经结束.卖方可以立即请求银行将货款从购物者的帐号转移到商家帐号,也可以等到某一时间,请求成批划帐处理.通过上述过程,我们可以发现它是实际贸易活

收稿日期:2002-11-22

作者简介:左黎明(1981-),男,江西鹰潭人,华东交通大学助教.

动在网络上的延伸,是以往的电子商务形式的扩充,而且更具有灵活性.

2　数据安全分析与实施

针对实时交易的过程中的各个环节可能出现的问题,我们将采取有针对性的高效策略.

2.1　网络通讯的安全性

由于双方进行的是一场实时网上交易,因此实时性和保密性是很重要的.商业交易的重要信息具有很大的实时性和决策性,而其实时性和决策性是企业高层的核心机密,比如说价格,订购的数量,为此在整个实时通讯中我们将采用 Deffie - Hellman 协议并结合 DES 算法对所有通讯信息进行端到端加密.

2.1.1　Deffie - Hellman 协议

是一种密钥交换体制,其保密性是基于求解离散对数问题的复杂性.

离散对数问题:$C^d = M \bmod P$(P 为大素数)

其中 d 叫做模 P 的以 C 为底数的 M 的对数.在已知道 C 和 P 的前提下,由 d 求 M 很容易,只相当做了一次指数运算.而如果我们用 M 反过来求 d,其时间的复杂度是指数形式的.在这种方法中引用了本原元的概念.设 P 是一个很大的素数,$0 < a < P$,并且当 $K = 1,2,3,\cdots,P-1$ 时,计算 $a^k \bmod P$ 的值,使 $1,2,3,\cdots,P-1$ 中的每一个值都出现一次,则称 a 是 P 的一个本原元.a 和 P 为交易中使用该算法的所有用户共享,但每个用户 I 选择一个与 P 互素且小于 P 的整数 k_i 做为自己的私有密钥.该协议算法描述如下:

我们假定交易双方主机为 A 和 B,密钥分别为 k_1 和 k_2.在 A 与 B 通讯时,可以通过一定的步骤得到 A 与 B 公共密钥,然后再利用 DES 算法对通讯信息进行加密.

1) A 和 B 双方各自计算出:

$b_1 = a^{k_1} \bmod P (0 < b_1 < P)$

$b_2 = a^{k_2} \bmod P (0 < b_2 < P)$;

2) A 发送 b_1 给 B,B 发送 b_2 给 A;

3) A,B 各自求出公共密钥为:

$\mathrm{KEY} = b_2^{k_1} \bmod P = (a^{k_2})^{k_1} \bmod P (0 < \mathrm{KEY} < P)$

$\mathrm{KEY} = b_1^{k_2} \bmod P = (a^{k_1})^{k_2} \bmod P (0 < \mathrm{KEY} < P)$;

4) 以 KEY 作为 DES 算法的密钥对信息进行加密解密.

2.1.2　DES 算法

DES 对 64 位二进制数据加密,产生 64 位密文数据.使用的密钥为 64 位,实际密钥长度为 56 位(有 8 位用于奇偶较验).解密时的过程和加密时相似,但密钥的顺序正好相反.DES 的保密性仅取决于对密钥的保密,而算法是公开的.DES 内部的复杂结构是至今没有找到捷径破译方法的根本原因.

上述过程加密解密速度很快而且算法很可靠,但也存在一定的缺陷,那就是可能会遭受中间人攻击或者 IP 欺骗,因此仅仅加密是不够的,全面的保护还要求在加密之前进行身份认证和识别.它确保参与加密对话的对象确实是真正的买主和卖主.

我们可以依靠许多机制来实现认证和识别,例如安全卡到身份鉴别.认证能确保只有经过授权的用户才能通过个人计算机进行 Internet 网上的交互式交易;识别则提供一种方法,用它生成某种形式的口令或数字签名,交易的另一方据此来认证他的交易伙伴.用户管理的口令通常是前一种安全措施,硬件/软件解决方案则不仅逐步成为数字身份认证的手段,同时它也可以被可信第三方用来完成用户数字身份(ID)的相关确认.

2.2　身份认证和识别

认证就是指用户必须提供他是谁的证明,认证的标准方法就是身份唯一性的确定,特定用户具有什么特征,其识别的特征物信息.比如,系统中存储了他的指纹,他接入网络时,就必须在连接到网络的电子指纹机上提供他的指纹(这就防止他以假的指纹或其它电子信息欺骗系统),只有指纹相符才允许他访问系统.更普通的是通过视网膜血管分布图来识别,原理与指纹识别相同,声波纹识别也是商业系统采用的一种识别方式.网络通过用户拥有什么东西来识别的方法,一般是用智能卡或其它特殊形式的标志,这类标志可以从连接到计算机上的读出器读出来.至于说到"他知道什么",最普通的就是口令,口令具有共享秘密的属性.例如,要使服务器操作系统识别要入网的用户,那么用户必须把他的用户名和口令送服务器.服务器就将它与数据库里的用户名和口令进行比较,如果相符,就通过了认证,可以上网访问.这个口令就由服务器和用户共享.我们可以采用几种方法组合而成来获得更加保密的认证.

智能卡技术将成为用户接入和用户身份认证等安全要求的首选技术.用户将从持有认证执照的可信发行者手里取得智能卡安全设备,也可从其他

公共密钥密码安全方案发行者那里获得.这样智能卡的读取器必将成为用户接入和认证安全解决方案的一个关键部分.

2.2.1 认证的主要方法

1) 多重认证:不是采用一种证明方法,而是采用有两种形式或两种以上的证明方法,这些证明方法包含令牌、智能卡和仿生装置,如视网膜或指纹扫描器.

2) 数字证书.这是一种检验用户身份的电子文件,这种证书可以授权购买,提供更强的访问控制,并具有很高的安全性和可靠性.

3) 智能卡:一种可以持续较长的时间,并且更加灵活,存储信息更多,并具有可供选择的管理方式.

2.3 买方帐号信息的保密处理

买方的帐号信息是在交易过程中最敏感的部分,一方面很有可能一些人想通过不法手段来得到买方的这些重要信息,从某些黑客攻击的实例来看,这些部分是他们攻击目的的最终目标.另一方面,买方可能制造虚假的信息来进行商业诈骗活动.因此,在通讯保密的基础上,还有必要对买方帐号信息再进行加密和不可抵赖的数字签名.

由于对称加密体系有一个很严重的问题在于:加密解密算法均采用同一密钥,因此密钥管理存在安全问题,尤其是在网络上,黑客如果很幸运的从密钥传输过程中截获到密钥,这将是网上交易者的灾难.因此可采用非对称的公钥加密体系(RSA)或者是椭圆曲线加密(ECC).其中 ECC 被认为比 RSA 更高效并且更可靠,具体的分析有待于考证.

2.3.1 非对称的公钥加密体系

公开密钥(public key)最主要的特点就是加密和解密使用不同的密钥,每个用户保存着一对密钥.公开密钥 PKEY 和秘密密钥 SKEY,因此,这种体制被称为双非对称密钥密码体制.最有名的是 RSA.在这种体制中,PKEY 是公共信息,用作加密密钥,而 SKEY 需要由用户自己保密,用作解密密钥.加密算法 E 和解密算法 D 也都是公开的.虽然 SKEY 与 PKEY 是成对出现,但却不能根据 PKEY 计算出 SKEY.公开密钥算法的特点如下:

1) 用加密密钥 PKEY 对明文 X 加密后,再用解密密钥 SKEY 解密,即可恢复出明文,或写为:D SKEY (E PKEY (X)) = X.2) 加密密钥不能用来解密,即 D PKEY(E PKEY(X)) $\neq$ X.

3) 在计算机上可以容易地产生成对的 PKEY 和 SKEY.

4) 从已知的 PKEY 实际上不可能推导出 SKEY.

5) 加密和解密的运算可以对调,即:E PKEY (D SKEY (X)) = X.

RSA 加密解密算法如下:

1) 选取两个大质数 p 和 q;

2) 计算 $N = p * q$ 和欧拉函数 $Z = (p-1) * (q-1)$;

3) 选择一个与 Z 互质的数 d;

4) 求出 e,满足 $d * e = 1 \bmod Z$;

5) (e, N)作为公钥,将明文(买方信息)分成长度小于 $\log_2 N$ 位的明文块,欲加密的明文信息为 P $(0 \leqslant P < N)$.加密过程:$C = P^e \bmod N$;

6) (d, N)作为解密的私有密钥.解密过程为:$P = C^d \bmod N$.

由于是在通讯环境中,RSA 算法可能遭到公共模数(公共模数为 N)攻击和低加密指数攻击,因此必须对算法加以改进.主要方法是不在一组用户之间使用共同的 N,每次必须随机选取满足条件的质数 p 和 q.

2.3.2 数字签名

公钥系统的第 5 个特点可用来实现数字签名.它能保证:

1) 接收者能够核实发送者对报文的签名,证明买方的身份和信息的正确性;

2) 发送者事后不能抵赖对报文的签名,买方不能抵赖没有订购商品和服务;

3) 接收者不能伪造对报文的签名,卖方不能对买方进行商业诈骗.

签名过程如下:发送者(买方)A 用其秘密解密密钥 SKEYA 对报文 X 进行运算,将结果 D SKEYA (X)传送给接收者 B.B 用已知的 A 的公开加密密钥得出 E PKEYA (D SKEYA (X)) = X.因为除 A 外没有别人能具有 A 的解密密钥 SKEYA,所以除 A 外没有别人能产生密文 DSKEYA(X).这样,报文 X 就被签名了.

假若 A 要抵赖曾发送报文给 B.B 可将 X 及 D SKEYA (X)出示给第三者.第三者很容易用 PKEYA 去证实 A 确实发送信息 X 给 B.反之,如果是 B 将 X 伪造为 X′,则 B 不能在第三者面前出示 DSKEYA (X′).这样就证明 B 伪造了报文.可以看出,实现数字签名也同时实现了对报文来源的鉴别.

由于我们验证与交易过程是在建立在二次加

密秘密通讯的基础上,因此不用担心有人能够截获含签名的报文,因为如果有人想这样做,他必须对几重加密算法进行解密,这通常在技术上很难实现.

虽然使用RSA算法加密和签名速度有点慢,但是由于硬件技术的发展和需加密的信息量很少,因此方案是可行的.

2.3.3 网上交易系统安全体系的构成与实现

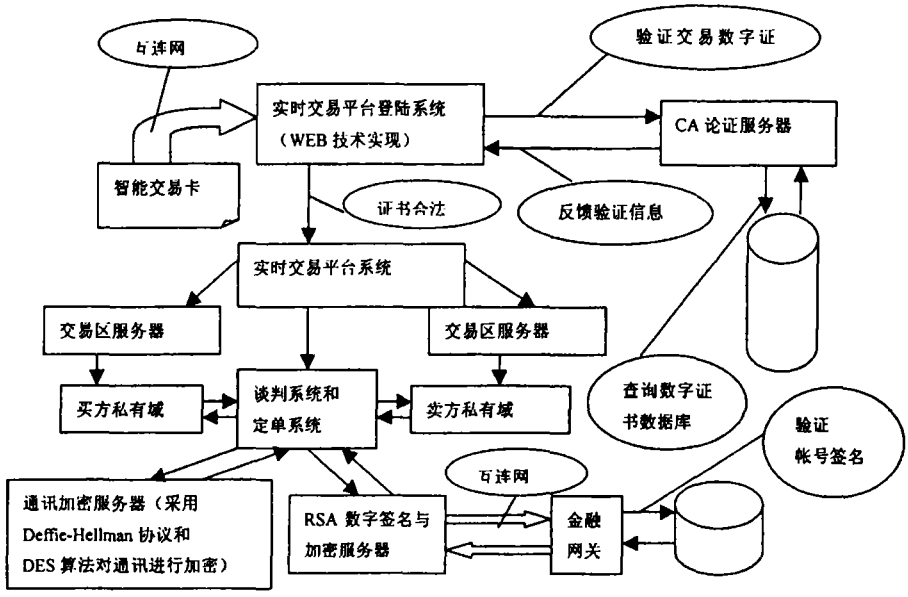

图1　网上交易系统安全体系的构成原理图

上图中,描述了具体实施实时网上交易的数据安全方案的一个简要过程.具体实现时,在通讯底层通过socket的库函数setsockopt()的选项IP_HDRINCL来自定义IP头,改变IP头中的TOS(Type of Service的优先级别和TTL(Time to Live),可以使数据包有更强的传输能力和寿命,从而提高系统性能.这种方法在Unix和LINUX很容易实现,由于Winsock2.2也全面支持setsockopt()的选项IP—HDRINCL,所以此方法在WIN2000下也顺利得以实现.

加密签名算法是该方案实现中核心的部分,以下是关键的数据结构和算法(C描述):

```
/* RSA公钥和RSA私钥数据结构为:*/
typedef struct
{
unsigned int bits; /* 模数大小 */
MP_INT e; /* 公钥指数 */
MP_INT n; /* 模数 */
} RSAPublicKey;

typedef struct
{
unsigned int bits; /* 模数大小 */
MP_INT n; /* 模数 */
MP_INT e; /* 公钥指数 */
MP_INT d; /* 私钥指数 */
MP_INT u; /* Multiplicative inverse of p mod q. */
MP_INT p; /* 质数 p */
MP_INT q; /* 质数 q */
}RSAPrivateKey;
/* 计算RSA密钥的方法及过程如下 */
/* 从质数p、q导出私钥 */
fprintf(stderr, "Computing the keys… \n");
derive_rsa_keys(&prv->n, &prv->e, &prv->d,
&prv->u, &prv->p, &prv->q, 5);
prv->bits = bits;
/* 从质数p、q导出公钥 */
pub->bits = bits;
mpz_init_set(&pub->n, &prv->n);
mpz_init_set(&pub->e, &prv->e);
/* 测试公钥和密钥是否有效 */
fprintf(stderr, "Testing the keys… \n");
rsa_random_integer(&test, state, bits);
mpz_mod(&test, &test, &pub->n); /* must be less
```

```
than n. */
    rsa_private(&aux, &test, prv);
    rsa_public(&aux, &aux, pub);
    if (mpz_cmp(&aux, &test) != 0)
    {
    fprintf(stderr,"**** private + public failed to decrypt.
\n");
    goto retry0;

    }
    rsa_public(&aux, &test, pub);
    rsa_private(&aux, &aux, prv);
    if (mpz_cmp(&aux, &test) != 0)
    {
    fprintf(stderr,"**** public + private failed to decrypt.
\n");
    goto retry0;
    }
    mpz_clear(&aux);
    mpz_clear(&test);
    fprintf(stderr, "Key generation complete. \n");
    }
```

3 评价与总结

在上述网上交易的新型形式中,针对可能出现的漏洞,我们采取的这些措施安全级别是是相当高的,针对不同的问题采用多种安全方法,不但可以适应实时的要求,而且可以抵抗例如IP欺骗,中间人攻击,以及差分攻击和公共模数攻击.本方案也易于通过软件实现,可以作为安全电子交易规范(SET)的一个补充.

参考文献:

[1] [美]Bruce Schneier,吴世忠,等译.应用密码学[M].北京:机械工业出版社,2000.

[2] 熊贵喜,王小虎,译.计算机网络[M].北京:清华大学出版社,1998.

[3] 石 峰,莫忠息.信息论基础[M].武汉:武汉大学出版社,2002.

[4] 冯登国,裴定一.密码学引论[M].北京:科技出版社,1993.

[5] Bob Toxen,前导工作室译.Linux安全-入侵防范、检测和恢复[M].北京:机械工业出版社,2000.

Discussion on Security of Data Concerning Prompt Exchange on Internet

ZUO Li-ming

(School of Natural Science, East China Jiaotong Univ., Nanchang 330013, China)

Abstract: This paper puts forward a new method of prompt exchange on the Internet as well as its procedure, which extends the functions of electronic commerce, then, have a discussion on the security of the data which are processed by the new method. Finally, it provides a solution which is so safe and feasible in practice.

Key words: prompt exchange on the internet; security of the data; encode; decode; Digital signature; Deffie-Hellman agreement; DES; RSA