电子商务协议的公平性

周展飞,周典萃,王贵林,卿斯汉
(中国科学院软件所;中国科学院信息安全技术工程研究中心,北京 100080)

摘 要: 本文指出在分析电子商务协议公平性的过程中,不仅要考虑参与协议的主体被动攻击的情况,同时还要考虑参与协议的主体进行主动攻击的情况.在此基础上,本文对 Kailar 逻辑进行了改进,使之能够分析协议的可追究性和公平性.

关键词: 电子商务协议; 可追究性; 公平性; 形式化分析
中图分类号: TP309 **文献标识码**: A **文章编号**: 0372-2112 (2000) 09-0013-03

Fairness in Electronic Commerce Protocols

ZHOU Zhan-fei, ZHOU Dian-cui, WANG Gui-lin, QING Si-han
(Institute of Software, The Chinese Academy of Sciences, Beijing 100080, China; Engineering Research Center for Information Security and Technology, The Chinese Academy of Sciences, Beijing 100080, China)

Abstract: It is pointed out that it is important to consider the case with active adversaries, as well as that with passive ones. Based on this knowledge, an improvement on Kailar logic is proposed for analysis of both fairness and accountability in electronic commerce protocols.

Key words: electronic commerce protocol; accountability; fairness; formal analysis

1 引言

在电子商务这一概念出现之前,信息安全领域的研究工作主要是围绕认证、存取控制、机密性和数据完整性而展开的.电子商务的出现则将可追究性这一安全问题摆在了人们的面前.

在现实的商业交易活动中,人们常常借助于票证(如合同、发票等)来解决交易中出现的争议和纠纷.与此类似,作为电子交易规则的电子商务协议也必须具备这一机制,它必须能够为交易双方提供足够的证据,以便在产生纠纷时仲裁机构可以利用这些证据来解决纠纷,即电子商务协议的设计必须满足可追究性原则.

根据可追究性原则的要求,参与协议的任何一方主体在协议执行完毕后,必须能够提供充分的证据以解决今后可能出现的纠纷.但可追究性原则未考虑协议的每一阶段协议各主体的状态.事实证明,一个安全的电子商务协议仅仅满足可追究性原则是不够的,它还必须满足公平性原则.根据公平性原则,一个安全的电子商务协议在协议执行的任何阶段,参与协议的任何一方主体都不占优势[1].

根据公平性原则的要求,协议的发起方和响应方必须同时交换他们的证据,如何保证发起方和响应方的同步正是设计一个安全协议的关键所在.目前,解决这一问题较常用的方法是建立一个可信任的第三方,协议的发起方和响应方将相关的证据发送给第三方,第三方在收集到所有的证据后将证据发送给相应的主体.

通过对认证协议的研究[2~5]可以发现,密码协议的安全性不仅依赖于安全强度高的密码算法,它还与协议本身的结构有关.一些极细微的协议结构上的改变都可能导致严重的安全缺陷.而这些安全缺陷通常又是非形式化方法所难以察觉的.鉴于以上背景,Kailar 提出了用于分析电子商务协议可追究性的逻辑,我们称之为 Kailar 逻辑,详见文[6].

Deng[7]等人于 1995 年提出了 CMP1 和 CMP2 认证电子邮件协议,并运用 Kailar 逻辑对上述协议的可追究性进行了分析.此外,文[7]还对协议的公平性进行了非形式化的分析.但从文[7]的分析,可以发现 Kailar 逻辑实际上无法分析报文的二次签名.此外,Kailar 逻辑还缺乏对签名密文的分析机制.

2 对 Kailar 逻辑的改进

2.1 公平性

鉴于 Kailar 逻辑[6]缺乏对协议公平性的分析机制,在此文中,将对 Kailar 逻辑进行扩充,使之能够分析协议的公平性.针对 Kailar 逻辑无法分析签名的密文和再次签名的报文这一不足,也作了一些必要的改进.有关 Kailar 逻辑的缺陷,参见文[8].

在给出形式化分析方法之前,有必要重新考察公平性的

收稿日期:1999-07-09;修回日期:2000-01-04
基金项目:国家自然科学基金(No. 69673016)

含义.

在文[1]中,公平性是指在协议执行完毕后,协议的任何一方都有充分的证据以解决今后可能出现的纠纷,且在协议执行的任何阶段,参与协议的任何主体都不占优势.在通常情况下,如果协议不能保证参与协议的主体同步地提供证据,协议响应 B 方就可能在接收协议发起方 A 提供的证据之后,中止协议而不提供证据从而置 A 于不利的地位.另一方面,B 虽未接收到发起方 A 的证据却收到了 A 发送的 B 所期待的报文(如电子邮件等),B 同样可以不提供证据.以上这两种情况都会导致 B 处于有利的地位.值得注意的是上述两种情况仅考察了 B 被动攻击的情况,而未考虑到 B 作为攻击者对传输的报文进行主动截取的情况.实际上,B 为了自己的利益,完全可能截取主体 发送给第三方的报文(此报文可能由第三方转发给 B),以获取所需的信息或证据,从而处于有利地位.而文[1]中,公平性的定义并未对此作出明确的说明.在此,我们建议采用 Asokan[9] 关于公平性的定义.在文[9]中,公平性是指在协议的任何阶段,参与协议的任何诚实的主体(即正确执行协议的主体)都不处于劣势.

2.2 对 Kailar 逻辑的改进

2.2.1 语法

与 Kailar 逻辑相似,我们用 P、Q 表示参与协议的主体.K 表示密钥,如果 K 为公钥,则 K^{-1} 表示相应的私钥.X 和 Y 表示公式.本文采用了合取和蕴涵这两个命题联结词.此外,该逻辑系统还包括以下构件:

(1) P Can Prove X:对于任何主体 Q,P 能执行一系列操作使得通过这些操作以后,P 能使 Q 相信 X 而不泄漏任何秘密 $Y(Y \neq X)$ 给 Q.

(2) P Says X: P 声明公式 X 并对 X 以及 X 能推导出的公式负责.

(3) P Receives M:主体 P 接收了报文 M.

(4) $PK(K, P)$: K 为 P 的公钥,任何主体都可以用此公钥验证用相应私钥 K^{-1} 签名的报文.

(5) $SK(K, P)$: K 为 P 在协议的每个执行回合生成的会话密钥(单钥).

(6) P IsTrustedOn X: P 为可信任的第三方,其他主体都相信 P 所声明的公式 X 的真实性.

(7) P Has M: P 拥有了报文 M.

2.2.2 公理系统

公理系统包含以下推理规则和公理:

由 $|- X$ 和 $|- X \supset Y$ 可以推断 $|- Y$.

在此,将 Kailar 逻辑的推理规则改写成公理的形式,并对此进行了扩充.公理系统如下:

(1) 连接:

P Can Prove $X \wedge P$ Can Prove $Y \supset P$ Can Prove $(X \wedge Y)$

如果 P 能够证明公式 X,且 P 能够证明公式 Y,则 P 能够证明公式 $X \wedge Y$.

(2) 蕴涵:

$$P \text{ Can Prove } X \wedge (X \supset Y) \supset P \text{ Can Prove } Y$$

如果 P 能够证明公式 X,且公式 X 蕴涵公式 Y,则 P 能够证明公式 Y.

(3) 报文来源:

P Receives $\{M\}_{K_q^{-1}} \wedge P$ Can Prove $PK(K_q, Q) \supset P$ Can Prove $(Q$ Says $M)$

如果 P 接收到用 K_q^{-1} 签名的报文 M,且 P 能够证明 K_q 为 Q 的公钥,则 P 能够证明 Q 发送了报文 M.

P Can Prove $(Q$ Says $\{M\}_K) \wedge P$ Can Prove $(Q$ Says $SK(K, Q)) \supset P$ Can Prove $(Q$ Says $M)$

如果 P 能够证明 Q 发送了报文 $\{M\}_K$,且 P 能够证明 Q 承认 K 为 Q 的密钥,则 P 能够证明 Q 发送了报文 M.

(4) 信任:

P Can Prove $(Q$ Says $X) \wedge P$ Can Prove $(Q$ IsTrustedOn $X) \supset P$ Can Prove X

如果 P 能够证明 Q 声明了公式 X,且 P 能够证明 Q 是可信任的,则 P 能够证明 X 成立.

(5) 接收:在此,我们用 $\overline{K}$ 表示 K 的对偶密钥,K 可以是单钥、公钥和私钥.如果 K 表示公钥,则 $\overline{K}$ 表示相应的私钥(反之亦然);如果 K 表示单钥,则 $\overline{K} = K$.

P Receives $\{M\}_K \wedge P$ Has $\overline{K} \supset P$ Receives M

上述公理说明了如何从密文和签名中获得所需的信息.

(6) 拥有:

P Receives $M \supset P$ Has M

(7) 分解:

P Says $(X, Y) \supset P$ Says $X \wedge P$ Says Y

P Receives $(X, Y) \supset P$ Receives $X \wedge P$ Receives Y

利用上述改进的 Kailar 逻辑,我们可以对现有的电子商务协议的可追究性和公平性作出分析,我们的分析步骤如下:

(a) 列举协议要达到的目的.

(b) 对协议进行转换:在转换的协议中,将攻击者能够截取报文这一事实用主体向攻击者发送报文这一形式显式地表述出来.为了简洁起见,如果攻击者所截取的报文中仅含有提供给其他合法主体的证据,而攻击者又无法从中获得对己有利的信息,将在转换协议中略去这一步骤,因为攻击者无法利用这些提供给其他主体的证据.在上述表述形式下,如果主体向攻击者和其他诚实主体同时发送了相同的报文,总假设攻击者接收报文的优先级要高于诚实主体.在对协议的转换过程中,用 $I(P)$ 表示 P 所扮演的攻击者.例如,将文[1]中协议的报文 $A \rightarrow B: f_{EOO}, B, L, C, EOO$ 转换成 $A \rightarrow I(B), B: f_{EOO}, B, L, C, EOO$,而将报文 $A \rightarrow S: f_{SUB}, B, L, K, SUB$ 转换成 $A \rightarrow I(B): f_{SUB}, B, L, K, SUB$ 和 $A \rightarrow S: f_{SUB}, B, L, K, SUB$ 表示攻击者 $I(B)$ 截取了 A 发送给 S 的报文 f_{SUB}, B, L, K, SUB.

(c) 解释协议:在此阶段,将协议转化成逻辑能够分析的逻辑公式.

(d) 给出初始化假设:按照协议的设计思想,给出协议初始时各主体状态的描述.在此,假设协议中各主体所扮演的攻击者拥有相应主体的所有能力和资源.

(e) 运用推理规则分析协议:运用推理规则和公理系统对协议进行分析.在协议的每一阶段,除对协议进行常规的推理外,将通过比较 A 和 $I(B)$、B 和 $I(A)$ 的证明能力和他们接收

报文的情况,推断协议的公平性.

运用上述推理系统,对下面的协议(详见参考文献[1])进行分析.

①$A \rightarrow B : f_{EOO}, B, L, C, EOO$

②$B \rightarrow A : f_{EOR}, A, L, EOR$

③$A \rightarrow S : f_{SUB}, B, L, K, SUB$

④$S \rightarrow B : f_{CON}, A, B, L, K, CON$

⑤$S \rightarrow A : f_{CON}, A, B, L, K, CON$

运用上述推理系统对协议进行分析,发现由于上述协议设计未考虑参与协议的主体进行主动攻击的情况,协议不满足公平性.

3　结论

本文分析了协议公平性的定义,指出了协议公平性应考虑参与协议的主体主动攻击的情况.在此基础上,本文在 Kailar 逻辑的基础上进行了改进和扩充,提出一种新的形式化分析方法,可以同时分析电子商务协议的公平性和可追究性.

致谢:在此感谢丁一强博士、陈国龙博士,与他们的讨论给了我们许多有益的启发.

参考文献:

[1] J. Y. Zhou, Non-Repudiation, PhD Thesis. Department of Computer Science [M]. Royal Holloway, University of London, 1997.

[2] M. Burrows, M. Abadi, R. Needham. A logic of authentication [J]. ACM Trans. on Computer Science, 1990, 8(1): 18 - 36.

[3] L. Gong, R. Needham, R. Yahalom. Reasoning about belief in cryptographic protocols [A]. Proceedings of the 1990 IEEE Symposium on Reseach in Security and Privacy, Oakland, CA: IEEE Computer Society Press, 1990: 234 - 248.

[4] M. Abadi, M. Tuttle. A sementics for a logic of authentication [C]. Proceedings of the Tenth ACM Symposium on Principles of Distribued Computing, Acm Press, 1991: 201 - 216.

[5] P. Syverson, P. C. van Oorschot. On unifying some cryptographic protocol logics [A]. Proceedings of 1994 IEEE Symposium on Reseach in Security and Privacy, Oakland CA: IEEE Computer Society Press, 1994: 14 - 28.

[6] R. Kailar. Accountability in electronic commerce protocols [J]. IEEE Trans. on Software Engineeing, 1996, 22(5).

[7] R. H. Deng, L. Gong, A. A. Lazar, W. G. Wang. Practical Protocols for Certified Electronic Mail [M]. Technical Report TR95-187-0, Institute of Systems Science, National University of Singapore, 1995.

[8] 周典萃,卿斯汉,周展飞. Kailar 逻辑的缺陷 [J]. 软件学报,待发表

[9] N. Asokan. Fairness in electronic commerce [D]. PhD Thesis, Department of Mathematics, University of Waterloo, Canada, 1998.

作者简介:

周展飞　1969 年生,博士,主要研究领域为密码理论和应用数学.

周典萃　1971 年生,硕士,主要研究领域为信息安全基础理论.

(上接第 48 页)

参考文献:

[1] Patrick Couffignal, Henri Baudrand, Bernard Theron. A new rigorous for the determination of iris dimensions in dual-mode cavity filters [J]. IEEE Trans Microwave Theory Tech., July 1994, MTT-42: 1314 - 1320.

[2] Philippe Guillot, Patrick Couffignal, Henri Baudrand, Bernard Theron. Improvement in calcultaion of some surface intergals: application to junction characterization in cavity filter design [J]. IEEE Trans Microwave Theory Tech., Dec. 1993, MTT-41: 2156 - 2160.

[3] Luciano Accation, Giorgio Bertin. Design of coupling irises between circular cavities by model analysis [J]. IEEE Trans Microwave Theory Tech., July 1994, MTT-42: 1307 - 1313.

[4] J. Adams Stratton. Electronmagnetic Theory [M]. New York: McGraw-Hill, 1941: 349 - 392.

[5] M. Abramouitz, I. A. stegun. Handbook of Mathematical Functions [M]. New York: Dover, 1965: 59.

[6] N. W. Mclachlan. Theory, Application of Mathieu Function [M]. London, 1947: 168.

[7] R. H. MacPhie and Ke-Li Wu. Scattering at the junction of a rectangular and a larger circular waveguide [J]. IEEE Trans. Microwave Theory Tech., Sept. 1995, MTT-43: 2041 - 2045.