Security and Atomicity in Electronic Commerce: Model, Protocol and Verification*

WU Zhi-gang, FANG Bin-xing, HU Ming-zeng, SUN Peng

(Department of Computer Science and Engineering, Harbin Institute of Technology, Harbin 150001, China)

E-mail: wzg@pact518.hit.edu.cn

Received July 19, 1999; accepted March 15, 2000

Abstract: Popularization and acceptance of electronic commerce mainly depend on the following properties: security, atomicity, privacy and anonymity. There are no electronic commerce protocols appropriate for electronic transactions of physical goods in which three properties are needed: security, atomicity and privacy. An electronic commerce model is suggested in this paper. The model is named ELC which simulates L/C in international trade. Then a secure and atomic electronic commerce protocol is proposed. Finally the protocol is analyzed for its strength and correctness by proving the desired properties using BAN style logic in the presence of an intruder.

Key words: electronic commerce; security; atomicity; privacy; verification

Electronic commerce (also known as electronic shopping or Internet shopping) means exchange of money and goods through Internet. There are two kinds of goods that can be exchanged in electronic commerce: digital goods that can be digitally delivered through Internet and physical goods that must be delivered through traditional post service. Although electronic commerce has been widely accepted, it is still insecure for customers and merchants when trading through Internet, especially for valuable physical goods.

There are basicly four challenges to electronic commerce: security, atomicity, privacy and anonymity. In general, security and atomicity are required for an electronic commerce system to be feasible. Security flaws or lack of atomicity may be fatal for a principal because they may lead to loss of money or goods. Comparatively, privacy and anonymity are desired features. For transactions of physical goods in which goods must be delivered through traditional mail delivery service, anonymity will not be reasonable. Protocols like SET[1], NetBill[2] etc. have proposed many solutions to them.

1 ELC Model

Merchant fraud occurs when a customer pays for some goods but merchant doesn't deliver appointed goods (in this paper we only discuss physical goods). To solve the problem, there should be a way to monitor merchants' ac-

* This project is supported by the National Natural Science Foundation of China under Grant No. 69773040 (国家自然科学基金). **WU Zhi-gang** was born in 1972. He is a Ph. D. candidate of Department of Computer Science and Engineering, Harbin Institute of Technology. His current research areas include Internet/Web technology, electronic commerce. **FANG Bin-xing** was born in 1960. He is a professor and doctor supervisor of Department of Computer Science and Engineering, Harbin Institute of Technology. His current research areas include Internet/Web technology, network security and parallel architecture. **HU Ming-zeng** was born in 1935. He is a professor and doctor supervisor of Department of Computer Science and Engineering, Harbin Institute of Technology. His current research areas include Internet/Web technology, parallel and high-performance architecture. **SUN Peng** was born in 1974. He is a Master student of Department of Computer Science and Engineering, Harbin Institute of Technology. His current research area is electronic commerce.

tions so that there must be a goods delivery if someone has paid otherwise no payment will occur.

Nowadays electronic commerce systems are no more than a simple simulation of traditional commerce. As neither consumer nor financial institution can monitor merchant to deliver physical goods at present, merchant fraud mainly results from the limitation of the current electronic commerce protocols themselves.

In international trade a special bill of document, usually known as letter of credit (L/C), is widely used. It's possible to simulate L/C in electronic commerce to avoid merchant fraud due to L/C's successful application in international trade.

Following part of this section presents an electronic commerce model called ELC (electronic letter of credit) that provides atomicity in electronic transactions. Different from prior models, there are four principals in the model: consumer, merchant, financial institution and mail company (also post company). Consumer must send payment instruction together with a list of ordered goods to merchant. Then merchant must send it to a financial institution, for example, a bank and then send goods list to mail company for goods delivery. The bank verifies the validity of payment instruction, forms an electronic L/C and sends it to the merchant. Then the merchant delivers goods through post service. After delivering goods, post company will digitally sign a goods delivery certificate and notify the merchant that goods (with right quantity and quality) have been delivered. Now the merchant can send the L/C and the certificate to the bank to ask for payment. At last the bank verifies them and decides whether to pay the merchant. The process works like commitment and rollback operation in a database transaction. If goods delivery is certified, payment instruction will be executed to pay the merchant (transaction is committed). If there's no certificate after exceeding the deadline then merchant will never be paid and the payment instruction becomes invalid, that is, transaction rollback to its original states. Obviously such a model can resolve merchant fraud problem.

Besides above four principals, there may be an intruder in a transaction. An intruder may eavesdrop in and/or intercept messages transferred in the network. He may decrypt and store parts of a message that is encrypted with his public key or private key of another party, and introduce fake messages built from original messages whose components are visible to the intruders. Message corruption or loss is modeled as message interruption of an intruder.

2 A Secure and Atomic Electronic Commerce Protocol

We designed an electronic commerce protocol on the basis of ELC model. The protocol is named BEARCAT. BEARCAT protocol provides security, atomicity and privacy for electronic transactions.

2.1 The protocol

Public key cryptography is used to encrypt and decrypt communication messages. BERACAT is composed of four principals: consumer, merchant, financial institution and post company. Each principal has a unique key pair of public key and private key. A transaction in BREACAT protocol is shown in Fig. 1.

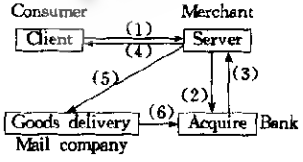

Fig. 1 BEARCAT transaction process

We have several rules in the protocol. Firstly, consumer's payment instruction must be encrypted with the bank's public key. It assures that only the desired bank can decrypt the payment instruction. Secondly, payment instruction has a period of validity. Thirdly, each principal (entity) must encrypt message with its private key and receiver's public key before the message is transmitted. Lastly, message encrypted with consumer's private key is the authorization for a bank to pay. Without it payment instruction will be considered invalid.

Let payment denote consumer's payment instruction and G denote the list of goods ordered. Sequence number SEQ is generated by the consumer and will never repeat in later transactions. Price is the amount of money con-

sumer and merchant agreed for the goods and must be consistent with that in payment instruction. DEADLINE is payment's period of validity. Once a transaction exceeds the DEADLINE, the bank will reject the payment. TID is transaction's id that's unique for the merchant and the bank and is used to identify transaction's messages.

A protocol is formally described by listing messages uttered between principals, and showing the source, destination and the message content symbolically. To describe the protocol, we use the following notations:

C denotes a consumer with public key c and private key $1/c$. M denotes a merchant with public key m and private key $1/m$. B denotes a bank with public key b and private key $1/b$. E denotes a post company with public key e and private key $1/e$. I denotes an intruder with public key i and private key $1/i$.

Protocol steps will be formally described in the following format:

$X \rightarrow Y$:[message]$1/x$ means principal X utters Y message encrypted with private key of X.

$X \rightarrow Y$:[message]y means principal X utters Y message encrypted with public key of Y.

BEARCAT protocol requires six steps that are illustrated as follows:

(1) $C \rightarrow M$: [[[SEQ, payment]b, price, G, DEADLINE]$1/c$]m;

(2) $M \rightarrow B$: [[TID,[[SEQ, payment]b, price, G, DEADLINE]$1/c$]$1/m$]b;

(3) $B \rightarrow M$: [[TID, SEQ, Tb]$1/b$]m;

(4) $M \rightarrow C$: [[[TID, SEQ, Tb]$1/b$]$1/m$]c;

(5) $M \rightarrow E$: [[TID, G, B]$1/m$]e;

(6) $E \rightarrow B$: [[[TID, G, B]$1/m$]$1/e$]b.

To simplify subsequent description and verification, let CER=[[TID, G, B]$1/m$]$1/e$.

2.2 The formal logic

Protocols, if designed improperly, may have flaws vulnerable to various security attacks. BAN logic[3] is an intuitive formal logic to verify various properties (e.g., security, privacy, and atomicity) of a protocol. Several problems or limitations of BAN logic have been reported in Refs. [3,4] and some descendents are introduced in Ref. [5]. The formal logic used in this paper is based on BAN logic and its extensions.

In analysis using BAN logic, a set of participant's final beliefs is generated from a set of initial assumptions and protocol steps. If these beliefs satisfy the goal of the protocol, then the protocol is validated. In this paper we make use of the logic to introduce an intruder who can eavesdrop, intercept messages, decrypt, and store the message components encrypted with keys available to the intruder. Besides, we also introduce the other principals in our protocol that can make various kinds of frauds.

We'll state the language (syntax) of the logic in this section. Some theorems are also introduced here. For its axioms, definitions, theorems and semantic etc., please see Refs. [3,5].

2.2.1 The language

We distinguish between the following sorts: Principal, Key, Message, and Formula. Formula is a sub-sort of Message. For Formula we have the traditional logical operators: $\rightarrow$, $\wedge$ and $\vee$. We also have the identity operator $=$. Furthermore, we have the following:

(X,Y) means a message with two parts: messages X and Y.

$P \triangleleft X$ means principal P sees message X.

$k \lessdot P$ denotes that k is public key of P, $k \gtrdot P$ denotes that k is private key of P.

$[X]k$, as in section 2.1, means X encrypted by k.

2.2.2 The model

For each principal in the environment, its local state is defined as the tuple (B_P, O_P, S_P, K_P), with the following intuitive interpretation:

· B_P: the set of formulas that P currently believes;

- O_P: the set of (sub-)messages P once said;
- S_P: the set of message that P has seen so far;
- K_P: the set of keys P possesses.

2.3 Formal analysis of the protocol

Now we formally analyze the protocol in the presence of an intruder making use of the above logic.

2.3.1 Initial state

The protocol's initial state can be described as:

$$O_C=\{\};O_M=\{\};O_B=\{\};O_E=\{\};O_I=\{\};S_C=\{\};S_M=\{\};S_B=\{\};S_E=\{\};S_I=\{\};$$

$$B_C=\{\varphi:\boldsymbol{L}\ \varphi\}\cup\{b\lhd B,m\lhd M,c\lhd C,1/c\rhd C,i\lhd I\};$$

$$B_M=\{\varphi:\boldsymbol{L}\ \varphi\}\cup\{b\lhd B,m\lhd M,c\lhd C,1/m\rhd M,i\lhd I,e\lhd E\};$$

$$B_B=\{\varphi:\boldsymbol{L}\ \varphi\}\cup\{b\lhd B,m\lhd M,c\lhd C,1/b\rhd B,i\lhd I,e\lhd E\};$$

$$B_E=\{\varphi:\boldsymbol{L}\ \varphi\}\cup\{b\lhd B,m\lhd M,1/e\rhd E,i\lhd I,e\lhd E\};$$

$$B_I=\{\varphi:\boldsymbol{L}\ \varphi\}\cup\{b\lhd B,m\lhd M,1/i\rhd I,i\lhd I,e\lhd E,c\lhd C\};$$

$$K_C=\{c,1/c,b,m,i\};KM=\{m,1/m,c,b,i,e\};KB=\{b,1/b,c,m,e,i\};$$

$$K_E=\{e,1/e,m,b,i\};$$

$$K_I=\{i,1/i,c,m,e,b\}.$$

2.3.2 Properties

The properties we want to verify are security, atomicity and privacy. They can be ogically described as:

Security: $1/c\notin S_I\wedge 1/b\notin S_I\wedge 1/m\notin S_I\wedge 1/e\notin S_I\wedge payment\notin S_I\wedge payment\notin S_M$

Privacy: $1/c\notin S_I\wedge 1/b\notin S_I\wedge 1/m\notin S_I\wedge 1/e\notin S_I$

Atomicity: $(payment\in S_B\wedge CER\in S_B)\vee CER\notin S_B$

2.3.3 Protocol verification

Let A be the set of assumptions (initial state) we start with (where all the beliefs of principals are true), P the protocol, and V the properties we want to prove. Because every step of the protocol may fail (the protocol is interrupted for some reason), we must show that V holds after each step of the protocol. In other words, if Pn is step n of our protocol, we must show $\{R[A]\}P_1;P_2;\ldots;Pn\{R[V]\}$ for every step of the protocol. Hence, we have:

Step 1. $C\rightarrow M$: [[[SEQ, payment]b,G, DEADLINE]$1/c$]m;

To simplify description, we let M_1=[[[SEQ, payment]b, price, G, DEADLINE]$1/c$]m, then

$$T(P_1)=C>M_1\wedge M\triangleleft M_1\wedge C\triangleleft M_1\wedge I\triangleleft M_1$$

We can get

(1) A is positive, $T(P_1)$ is positive, $A\triangle P_1$

From initial state A, we know that,

(2) $A\boldsymbol{L}\ 1/c\notin S_1\wedge 1/b\notin S_1\wedge 1/m\notin S_1\wedge 1/e\notin S_1\wedge$ payment $\notin S_I\wedge$ payment $\notin S_M\wedge$ payment $\notin S_B$

(3) $1/c\notin cts[M_1]\wedge 1/b\notin cts[M_1]\wedge 1/m\notin cts[M_1]\wedge 1/e\notin cts[M_1]$

From (2), (3) above, we know

(4) $A\cup T(P_1)\boldsymbol{L}\ 1/c\notin S_1\wedge 1/b\notin S_1\wedge 1/m\notin S_1\wedge 1/e\notin S_1\wedge$ payment $\notin S_I\wedge$ payment $\notin S_M$(Security)

(5) $A\cup T(P_1)\boldsymbol{L}\ 1/c\notin S_1\wedge 1/b\notin S_1\wedge 1/m\notin S_1\wedge 1/e\notin S_1$(Privacy)

(6) $A\cup T(P_1)\boldsymbol{L}\ CER\notin S_B$(Atomicity)

So we get (7) $A\cup T(P_1)\boldsymbol{L}\ V$

From (1), (7) we draw that $\{R[A]\}P_1\{R[V]\}$.

Verification for Steps 1~6 is similar. Finally, we draw conclusion that $\{R[A]\}P_1;P_2;P_3;P_4;P_5;P_6\{R[V]\}$. Then we can conclude that our protocol provides security, privacy and atomicity.

3 Summary and Future Work

In this paper we proposed a secure and atomic electronic commerce protocol for electronic trade of physical goods. Our protocol provides security, privacy and weakly certified delivery for electronic transaction. Its strength and correctness are formally verified using analysis of BAN style logic. The analysis is based on a model in which an intruder can eavesdrop, intercept, and store components of messages. The intruder can also decrypt encrypted messages if decryption keys are available to the intruder. We formally proved our protocol's security, atomicity and privacy in the presence of such an intruder.

References:

[1] Linda, J. C. Privacy & reliability in Internet commerce [Ph. D. Thesis]. Carnegie Mellon University, Pittsburgh, Pennsylvania, 1996.

[2] Sirbu, M., Tygar, J. D. NetBill: an Internet commerce system optimized for network delivered services. In: Proceedings of the IEEE COMPCON'95. Los Alamitos, CA: IEEE Computer Society Press, 1995. 20~25.

[3] Snekkenes, E. Exploring the BAN approach to protocol analysis. In: Proceedings of the IEEE Symposium on Research in Security and Privacy. Oakland, CA: IEEE Computer Society Press, 1991. 171~181.

[4] Syverson P. Adding time to a logic of authentication. In: Proceedings of the 1st ACM Conference on Computer and Communication Security. Fairfax, Virginia: ACM Press, 1993. 97~101.

[5] Michael, B., Martin, A., Roger, N. A logic of authentication. ACM Transactions on Computer Systems, 1990, 8(1): 18~36.

电子商务的安全和原子:模型、协议和验证

吴志刚, 方滨兴, 胡铭曾, 孙 鹏

(哈尔滨工业大学 计算机科学与工程系,黑龙江 哈尔滨 150001)

摘要: 电子商务的流行与接受主要取决于下述属性:安全、原子、隐私与匿名. 对于需要安全、原子和隐私等3个属性的物理商品的电子交易还没有合适的电子商务协议. 基于此,提出了一个称为ELC的电子商务模型,ELC模型模拟了国际贸易中的电子信用证. 然后提出了一个安全、原子的电子商务协议. 最后,在有一个入侵者的情况下,通过使用BAN风格的逻辑证明所期望的属性分析了协议的强度和正确性.

关键词: 电子商务;安全;原子;隐私;验证

中图法分类号: TP393 **文献标识码**: A