A Novel Logic for Analyzing Electronic Payment Protocols

Yi LIU[1, a], Xing-Tong LIU[1, b] and Chao-Jing TANG[1]

[1]*College of Electronic Science and Engineering, National University of Defence Technology, Changsha, China*
[a]*louis0121@126.com,* [b] *liuxingtong@nudt.edu.cn*

Abstract. A novel formal method which can be used to analyze security properties such as accountability, fairness and timeliness in electronic payment protocols is proposed. The novel method extends Qing-Zhou approach based on logic reasoning by adding a simple time expression and analysis method. It increases the ability to describe the event time, and extends the time characteristics of the logical inference rules. An anonymous electronic cash payment protocol is analyzed by the novel logic, and the result shows that the fairness of the protocol is not satisfied due to the timeliness problem in protocol. The novel logic method proposed in this paper has a certain theoretical and practical significance for the design and formal analysis of electronic payment protocols. At the same time, its idea has a certain guiding value for improving the security of other security protocols.

1 Introduction

Electronic payment has made unprecedented progress in recent years, and the security problems in electronic payment activities are increasingly being valued by everyone. Electronic payment protocol is the technical basis for the security of electronic commerce activities, and all kinds of security services are provided by electronic payment protocols for consumers. The analysis and research of electronic payment security protocol has become an important issue in the field of information security [1]. However, the electronic payment protocol is the same as other cryptographic protocols. Even though electronic protocols are carefully designed, there are still security vulnerabilities. Secure and reliable electronic payment protocols are important guarantees for the security of electronic payment activities. In order to ensure the correctness and security of electronic payment protocols, it is necessary to analyze protocols accurately and find out defects and vulnerabilities in protocols through formal analysis method. The results obtained can be used to guide the design of the protocol or make up for the defects of the original protocol. Therefore, it has important theoretical significance and application value to research the formal analysis method of electronic payment protocol.

Nowadays, the main formal analysis methods of electronic payment protocol are logic reasoning, model checking, and theorem proving method. The method of model checking cannot analyze some special security properties like accountability, fairness and anonymity due to lack of the ability of logical reasoning. Approach based on logic is a kind of important formal analysis method of electronic payment protocol in recent years. Kailar logic [2] can analyze the accountability in protocol, but it can't analyze the fairness; Qing-Zhou logic[3][4] can be used for the analysis of accountability and fairness in protocol. The common properties of protocols are described by the ATL logic (alternating time temporal logic) based on game theory in paper [5]. The fairness and timeliness are analyzed through the model checking tool MOCHA. However, most of the current logic methods can only be used to analyze some secure properties. Therefore, it is a hotspot and trend to improve the analysis ability of existing typical electronic payment security protocol logic methods in current formal method research.

In this paper, a novel logic is proposed for the analysis of electronic payment protocols by adding simple time expression and time analysis method. The ISI protocol is analyzed using the proposed novel logic and the analysis result shows that ISI protocol does not provide timeliness. Therefore, the novel logic has the ability to describe and analyze the timeliness of electronic payment protocols.

2 Concepts and Definitions

The definitions and symbols used in the novel logic are defined as follows:

2.1 Basic Symbol

A, *B*: Parties participate in protocol;
TTP: Trust third party;
M: Message transferred in protocol;
(M, n): Indicates that message m is combined with message n;

K_a : The public key of the party A, which is used to verify the digital signature of A. K_a^{-1} is the secret key that corresponds to K_a ;

$\tilde{K}$: Dual key of K. If K is an asymmetric key, then $\tilde{K}=K^{-1}$. If K is a symmetric key, then $\tilde{K}=K$;

$\{m\}_K$: Cipher text of message m encrypted with the secret key K;

T: Time of occurrence;

EOO (evidence-of-origin): It is non-repudiation evidence that is provided to the receiver in electronic payment protocol, which is used to prove that the sender has sent the message;

EOR (evidence-of-receipt): It is non-repudiation evidence that is provided to the sender in electronic payment protocol, which is used to prove that the receiver has received the message sent by the sender.

2.2 Time System

We describe the time when event occurs by adding a condition in the formula language of formal logic, like $A \to m$ at T. m is a message, and A is one of the parties in protocol. T is a time expression. This definition increases the description of the occurrence time of sending and receiving message.

Set $I = \{0,1,2,3,...\} \bigcup \{-1,-2,-3,...\}$, stands for integers, then the time expression defines as follows:

1. x is constant time element, while $x \in I$.

2. X is variable time element, while X is an variable element in I.

3. $X|TS$ is time binding expression, while X is an variable time element and $TS \subseteq I$.

4. $[T]$ is time expression, while T is a time binding expression.

The constant time element is represented by a lower case t with a subscript, and the variant time element is represented by a capital letters T with a subscript.

Time binding expression is a variable time element X with a certain value of constant time element as $t(t \in TS)$. Once the value of the variable time element is bound by a time binding expression, its function is the same as the time constant. It can't be bound again before the binding value is released. In logical formulas, the time expression [X|I] can be abbreviated to [X], and [X|{x}] can be abbreviated to [x], where x is a constant time element or a variable time element with bound value. The value of the variable time element is bound to the first appearance of operations in its formula.

2.3 Protocol and Environment

Protocol party set Principle={TTP,A,B,C,…,P,Q,R…}, where A,B,Q,R,…, are participants in protocol. They can either be honest or dishonest. That is, they can obey the execution of the protocol, and also can not obey the implementation of the protocol. In general, we assume that these parties are dishonest and that they may be able to interrupt the execution of the protocol at will. TTP(Third trust party) is a special party, which is regarded as a fair trusted third party by other parties participate in protocol. It can be served as the TTP role by the bank or the arbitration organization.

Another important part of the environment is the communication channel. Communication channels can be both reliable and unreliable, depending on the specific operating environment. Usually, the communication channel between general parties is unreliable, while the communication channel between the *TTP* and other parties is recoverable. That is the communication channel may not be always paralyzed, the message can be transmitted finally.

Protocol statement defines what messages should be sent and received by parties in the current round , which is described as follows :

$A \to B$: m at T : represents A sent message m to B at T.

2.4 Possession Sets in Protocol

Assuming the protocol begins to run at T_0 , A is an arbitrary party participate in protocol. At the beginning of protocol, the initial possession sets of A is $O_a(T_0)$. When protocol execution to T_x , the possession sets of A becomes $O_a(T_x)$. Besides, we defines $O_a(T_e)$ is the final possession sets of A at the end of protocol. When the protocol runs to any time, the possession sets of A contains the information that is not deleted in the possession sets before and the message which is received and sent at this time. The possession sets of A changes constantly with execution of protocol, until $O_a = O_a(T_e)$.

When the protocol runs at T_x , the possession sets of A changes from $O_a(T_y)$ to $O_a(T_x) \wedge (T_y \le T_x)$, which means T_y is the moment before T_x . It follows the following rules :

(1) If the execution of the protocol statement is $A \to B$: m at T_x . m is a new message generated by A, which means $m \notin O_a(T_y)$. Then $O_a(T_x) = O_a(T_y) \bigcup \{m\}$. If m is not a new message generated by A, we get $m \in O_a(T_y)$.

(2) If the execution of the protocol statement is $B \to A$: m at T_x , while $m \notin O_a(T_y)$, then $O_a(T_x) = O_a(T_y) \bigcup \{m\}$.

(3) Otherwise, $O_a(T_x) = O_a(T_y)$.

3 Logic Analysis Methods

3.1 Logic Component

Our method consists of the following 5 logical components :

(1) $A \succ x$: For any party B, A can make B believe in formula x by performing a series of operations without leaking any secret $y \ne x$;

(2) $A \rightarrow m$ at T : A sent message m at T. The following implication was established in the process of analysis :

$$A \rightarrow (m, n) \text{ at } T \Rightarrow A \rightarrow m \text{ at } T \qquad (1)$$

That means, if A sends messages (m, n) at T, then A sends message m at T.

(3) $A \ni m$: A possesses message m.

(4) $A \leftarrow m$ at T : A received message m at T. The following implication was established in the process of analysis :

$$A \leftarrow (m, n) \text{ at } T \Rightarrow A \leftarrow m \text{ at } T \qquad (2)$$

That means, if A received messages (m, n) at time T, then A received message m at T.

(5) $\xrightarrow{K_a} A$: K_a is the public key of A, which is used to verify the message signed by K_a^{-1}.

3.2 Axiom System

The axiom system consists of 1 inference rule and 6 axioms. Inference rule is as follows :

$$(\vdash \varphi) \wedge (\vdash (\varphi \Rightarrow \psi)) \Rightarrow \vdash \psi \qquad (3)$$

The inference rule illustrates $\vdash \psi$ can be obtained from $\vdash \varphi$ and $\vdash (\varphi \Rightarrow \psi)$. $\vdash$ is a meta language symbol. $\Gamma \vdash \psi$ represents ψ can be deduced from the formula sets Γ. $\vdash \varphi$ indicates φ is a theorem, which means φ can be deduced from axioms. Therefore, the inference rule above indicates that ψ is theorem when φ is theorem and φ contains ψ.

The 6 axioms in the axiom set are as follows :

A1. $A \succ x \wedge A \succ y \Rightarrow A \succ (x \wedge y)$

A2. $A \succ x \wedge (x \Rightarrow y) \Rightarrow A \succ y$

A3. $A \ni \{m\}_{K_b^{-1}}$ at $T_x \wedge A \succ \xrightarrow{K_b} B$ at $T_x \Rightarrow A \succ B \rightarrow m$ at $[T_Y \mid T_Y \le T_X]$

A4. $A \succ B \rightarrow \{m\}_k$ at $T_x \wedge A \succ B \rightarrow k$ at $T_Y \Rightarrow A \succ B \rightarrow m$ at $\max(T_X, T_Y)$

A5. $A \leftarrow m$ at $T \Rightarrow A \ni m$ at T

A6. $A \leftarrow \{m\}_K$ at $T \wedge A \ni \tilde{K} \Rightarrow A \leftarrow m$ at T

When the time of events is not analyzed, all time expressions in the above axioms use [X|I], and the operation at can be omitted. The steps of using the novel logic to analyze protocols are as follows :

(1) Before giving the basic assumption of the protocol, we have to give all the constant and variable time elements that are used in the process of protocol reasoning. The actual value of the constant element may not be given, but if there is a constraint relationship between the different time constant, the constraint relationship should be pointed out. It is required to describe the time dependence of the events in protocol using the formula apparently, while giving the basic assumptions and the target of the protocol.

(2) The proof procedure of protocol target is divided into two steps. The first step is called logical reasoning, which proves the first part of the protocol target. The second step is called time calculus, which proves the latter half of the protocol target. The function of this procedure is to prove that the result obtained in the logic reasoning satisfies the time constraints specified in the protocol target. The method used in this procedure is the proof approach of algebraic equation and inequality, so it is easy to grasp and use. If the formula is established at any time of the protocol, the time description at T can be omitted.

3.3 Protocol Analysis Procedure

Protocol analysis consists of the following 5 steps.

(1)List the initial possession sets of the parties in protocol.

(2)List the initial assumptions of the protocol :

(a)The basic assumptions

(b)The credible assumptions

(c) The protocol comprehension assumptions

(3)List EOO and *EOR*, and analyze whether the design of *EOO* and *EOR* meets the requirements of accountability.

(4)Analyze whether $EOO \in O_b(T_e) \wedge EOR \in O_a(T_e)$ is set up at the end of the protocol.

(5) Analyze whether the protocol is to achieve the target of fairness, which means whether the protocol meets $EOO \in O_b(T_e)$ if and only if $EOR \in O_a(T_e)$ at the end of the execution time T_e.

4 ISI Protocol Analyses

ISI protocol[6] is an anonymous electronic cash payment protocol proposed by Medvinsky and Neuman, including three participants : customer A, merchant B and the currency server CS trusted by both parties. The purpose is customer A pay the merchant B through the currency server CS, while B provides payment receipt to A. Throughout the payment process, the customer A remain anonymous, and CS play a role as TTP. Protocol steps are as follows :

(1) $A \rightarrow B : K_{ab}$ at T_0

(2) $B \rightarrow A : \{K_b\}_{K_{ab}}$ at T_r

(3) $A \rightarrow B : \{\{coins\}_{K_{cs}^{-1}}, SK_a, K\_ses, S\_id\}_{K_b}$ at T_s

(4) $B \rightarrow CS : \{\{coins\}_{K_{cs}^{-1}}, SK_b, transaction\}_{K_{cs}}$ at T_k

(5) $CS \rightarrow B : \{\{new\_coins\}_{K_{cs}^{-1}}\}_{SK_b}$ at T_c

(6) $B \rightarrow A : \{\{amount, Tid, date\}_{K_b^{-1}}\}_{SK_a}$ at T_d

In the ISI protocol, K_{ab} represents the session key between A and B. K_a and K_b respectively stand for the public key of customer A and merchant B, while K_{cs} and K_{cs}^{-1} stand for the public key and private key of currency server CS. $\{coins\}_{K_{cs}^{-1}}$ represents electronic currency of A.

All currency is issued by CS. SK_a and SK_b represent the shared key of A and B. K_ses represents the key to a service that would like to be obtained. S_id is an identifier for the service to be obtained. Transaction represents specific transaction processing.

The analysis procedure of the protocol is as follows :

(1)List the initial possession sets. At the initial time of the protocol operation, the initial state of the *A* and *B* is

$$O_a(T_0) = \{K_{cs}\}$$

$$O_b(T_0) = \{K_{cs}\}$$

$$A \succ \xrightarrow{K_{cs}} CS$$

$$B \succ \xrightarrow{K_{cs}} CS$$

(2)List the credible assumptions of the protocol are as follows :

$$\text{T1: } A \succ CS \rightarrow m_1 \Rightarrow A \succ P \rightarrow m_1'$$

Assume that the currency server is fully in accordance with the provisions of the protocol and will not do anything that is harmful to any party in the protocol. If *A* can prove that *CS* has sent message m_1 to him, then *A* can prove some other party *P* has sent the message m_1' to *CS* which made *CS* send m_1 to *A*.

(3)List the evidence of origin (*EOO*) and the evidence of receipt(*EOR*) as follows :

$$EOR=\{new\_coins\}_{K_{cs}^{-1}}$$

$$EOR=\{amount, Tid, date\}_{K_b^{-1}}$$

Assume that the equation $EOO \in O_b(T_e)$ satisfied at the end of the protocol T_e. According to axiom A3 and the credible assumption T1, we will get :

$$B \succ CS \rightarrow new\_coins \text{ at } [T_\alpha \mid T_\alpha \le T_e] \qquad (4)$$

According to the credible assumption T1, we can obtain :

$$B \succ A \rightarrow k \text{ at } [T_\alpha \mid T_\alpha \le T_e] \qquad (5)$$

Because it is a protocol for anonymous payment, *B* only needs to prove the payment of someone is effective, without the need to prove who the payer is. So the equation (5) can meet the requirement of accountability.

Assume that the equation $EOR \in O_a(T_e)$ satisfied at the end of the protocol, which means $A \ni \{amount, Tid, date\}_{K_b^{-1}}$ satisfied. Since we can't prove $A \succ \xrightarrow{K_b} B$, $A \succ B \rightarrow \{amount, Tid, date\}_{K_b^{-1}}$ can not be derived. Therefore the evidence of receipt EOR in protocol can not achieve the target of non-repudiation. It is proved by the novel logic that ISI payment protocol does not meet the accountability.

(4) After all the steps of the protocol are completed, there will be $A \ni EOR$ and $B \ni EOO$. Therefore, $EOO \in O_b(T_e) \wedge EOR \in O_a(T_e)$ is set up at the end of the protocol.

(5)Then analyze the fairness of the protocol. The fairness objective is:

$$EOO \in O_b(T_e) \text{ if and only if } EOR \in O_b(T_e) \qquad (6)$$

That is two parties obtain the evidence of each other for non-repudiation at the same time.

Because CS is completely believable, so we can obtain $CS \rightarrow B : \{new\_coins\}_{K_{cs}^{-1}}$ at T_c and $\{new\_coins\}_{K_{cs}^{-1}} \in O_b(T_c) \Rightarrow EOO \in O_b(T_c)$.

Only after the sixth step is completed, $\{amount, Tid, date\}_{K_b^{-1}} \in O_a(T_d)$ is established. According to the steps of the protocol, the relationship between T_c and T_d is $T_c < T_d$. So $EOO \in O_b(T_c) \wedge EOR \in O_b(T_e) \wedge (T_c < T_d)$, which can not achieve fairness.

The main reason is that the implementation of the protocol does not have specific constraints on the relevant event time in the process. After the completion of the third step of the protocol, B is required to perform the fourth step in certain time delay t_b . And it's also required to perform the sixth step operation within a certain time delay t_c after receipt of $\{new\_coins\}_{K_{cs}^{-1}}$.

If A did not receive $\{amount, Tid, date\}_{K_b^{-1}}$ after the certain period of time, the protocol is terminated. Due to CS is completely believable, $(T_c\text{-}T_k) \le t_s$ must be satisfied. t_s is processing delay of CS. So in order to make A received EOR at the end of the protocol, $t_b + t_s + t_c \le t_a$ must be established. It means the behavior delay of B must be constraint to satisfy $t_b + t_c \le t_a\text{-}t_s$, in order to ensure the fairness of the protocol.

5 Conclusions

In this paper, the analysis of ISI protocol specifically illustrates how the novel logic analyzes the temporal relations between events in the electronic payment protocol. The novel logic is not a simple logic method, but an integrated approach. The logic reasoning in the process of the objective proof of protocols is based on the proof method in Qin-Zhou logic approach, but the time calculus part uses the method of algebra and set theory. It is suitable for analyzing the timeliness of electronic payment protocols. Further more, this idea can be introduced to other formal methods to analyze the security of cryptographic protocols.

References

1. P. McCorry, S.F. Shahandashti, F Hao, 20th Financial Cryptography and Data Security, (2016)
2. Kailar R, IEEE Trans. on Software Engineering, 22, 313-328,(1996)
3. DC Zhou, SH Qing, ZF Zhou, Journal of Software, 12, 1318-1328(200l)
4. SH Qing, Journal of Software, 16, 1758-1765(2005)
5. Kremer S, Universit'e Libre de Bruxelles Facult'e des Sciences(2003-2004)
6. G. Medvinsky, C. Neuman, Proc of the 1st ACM Conference on Computer and ComAnications Security, 102-106(1993)