Formal analysis of a model for electronic payment systems

Chen Wang and Ni-Na Shu and Huai-Xi Wang*
Hefei Electronic Engineering Institute, 460 Huangshan Rd., Hefei, Anhui, P.R.China, 230031
E-mail: daodewang@163.com, sncyc@tom.com, paper2submit@163.com
**Corresponding author*

A model that generalizes credit-card-based electronic payment systems is analyzed by BAN logic and Kailar logic. This paper extends Kailar logic to process the analysis of ciphertext. This paper provides a new method to analyze ciphertext.

Keywords: Electronic Payment; Formal Analysis; BAN Logic; Kailar Logic.

1. Introduction

Electronic commerce is a kind of network transactions system that is used to implement the payment of e-money and encash or commitment of services. The core of the electronic commerce is the electronic payment system. Currently, many electronic payment systems have been proposed for providing different levels of security to financial transactions [1, 2, 3].

Based on these electronic payment systems, Ferreira and Dahab presented a model of credit-card-based electronic payment systems [4]. In this paper, Ferreira and Dahab utilized BAN logic [5] and Kailar logic [6] to analyze the authentication and accountability problems. Against its lack of the mechanism of ciphertext analysis, the authors extend notations, statements and postulates aspects of Kailar logic, enabling it to interpret and analyze the signed then encrypted messages, thereby expanding its range of application.

2. Model Description

The model of credit-card-based electronic payment systems generalizes the main characteristics of credit-card-based electronic payment systems. It is based on SET, IKP and CYBERCASH, three of the most important systems. The model consists of the following message exchange steps:

Msg1. M→C: Cert M, Desc, {TID, Date, H(Desc)}Km^{-1}

Msg2. C→M: Cert C, {{TID, Date, H(Desc) , CardData, amount}Kc^{-1}} Ka

{H(Desc), TID, Date}Kc^{-1}

Msg3. M→A: {{TID, Date, H(Desc), CardData, amount}Kc^{-1}} Ka

{{H(Desc), amount, IDM, TID, Date}Km^{-1}} Ka

Msg4. A→M: {Rec} Ka^{-1}

Msg5. M→C: {Rec} Ka^{-1}

Where: *C* is the customer, *M* is the merchant, and *A* is the acquirer i.e. the entity that processes credit card purchases; $Cert_X$ is X's certificate, *TID* is a transaction ID; *Date* is the current time and date; *Desc* is a description of purchased goods; *H* is a hash function; K_X and K_X^{-1} are the public and private key of X, respectively; *CardData* is the credit card number; *amount* is the amount being transferred and *Rec* is a receipt for the transaction.

3. Formal Methods Used in the Analysis

Two formal methods were used to analyze the model:

(1) Kailar logic, which deals with the accountability of the parties involved in the message exchange of a cryptographic protocol. The goal of accountability is that certain principal is required to prove to the third parties that another party is accountable for certain statement.

(2)BAN logic, which deals with the authentication aspects of a protocol.

3.1. *Kailar logic*

The goal of Kailar logic is to prove that the parties involved in a protocol exchange are able to correctly establish the origin of a message. A signed message is treated as an undeniable statement from one of the parties. As such, the proof of a statement is any sequence of operations which convinces another party that the statement is true.

Kailar Logic's Basic Framework:

1． Notation:

A, B, C…: involved principal

m: a message which is send to another principal by a principal

TTP: trusted third party

Ka: A's public key

Ka^{-1} : A's private key

Kab: the shared key between A and B.

2． Statements:

Strong Proof: "A CanProve x"

Principal A is able to strongly prove statement x to any principal B. This means that A is able to execute a sequence of operations that convinces B of statement x but not disclose any secret y($y \neq x$) to B.

Weak Proof: "A CanProve x to B"

Principal A is able to weakly prove statement x to a specific principal B. This means that A is able to execute a sequence of operations that convinces B of statement x but not disclose any secret y($y \neq x$) to B.

Global trust: "A IsTrustedOn x"

Principal A is trusted on statement x, namely A has the authority to endorse x, or is liable for making trusted statement x.

Non-global trust: "A IsTrustedOn x by B"

Principal B considers principal A is trusted on statement x, or A is able to prove to B that A is liable for statement x.

Signature Authentication: "Ka Authenticates A"

The key Ka can be used to authenticate the signature of principal A.

Message Interpretation: "x in m"

x is one or several interpretable fields in message m. Usually, interpretable fields refer to plaintext fields or encrypted fields which can be decrypted by the principals. This interpretation is protocol specific, and is expected to be defined by the protocol designers explicitly.

A Says x:

The principal A is accountable for making the statement x, and anything that x implies. Usually, the following postulate is used implicitly in the analysis:

A Says (x, y) $\Rightarrow$ A Says x

Message Receipt: "A Receives m SignedWith K^{-1}"

The principal A receives message m which is signed with K-1. Usually, the following postulate is used implicitly in the analysis:

A Receives m SignedWith K-1: x in m

A Receives x SignedWith K-1

$x \Rightarrow y$: x implies y, namely if x holds, then y holds.

$x \wedge y$: x and y.

P; Q

R:

If P and Q hold at the same time, then R holds. This also means (P; Q) can infer R.

Postulates:

K1. Conjunction Postulate:

A CanProve x; A CanProve y

A CanProve ($x \wedge y$)

K2. Inference Postulate:

A CanProve x;$x \Rightarrow y$

A CanProve y

K3. Sign Postulate:

A Receives m SignedWith K-1;x in m;A CanProve (K Authenticates B)
A CanProve (B Says x)
K4. Trust Postulate:
A CanProve (B Says x);A CanProve (B IsTrustedOn x)
A CanProve x
K5. Relationship of Strong and Weak Provabilities:
(S(presents some preconditions);C CanProve y) ⇒ (A CanProve x)
(S;C CanProve y to B) ⇒ (A CanProve x to B)
K6. Relationship of Global and Non-Global Trust:
(S(presents some preconditions);C IsTrustedOn y) ⇒ (A CanProve x)
(S;C IsTrustedOn by B) ⇒ (A CanProve x to B)
K7. Relationship to Belief:
(A Believes x) ⇔ (A CanProve x to A)
The analysis consists of the following steps:

Stating a protocol's accountability goals (in protocols for electronic commerce, this is derived from the transaction goals).

Interpreting protocol messages. While performing this step, we interpret only the signed messages and plaintexts that are related to accountability.

Articulating initial state assumptions.

Analyzing messages for accountability properties with postulates, and comparing the provability results that protocol participants obtain, with the protocol goals. Failure of a protocol to achieve its goals indicates a weakness in the protocol that can be exploited.

3.2. *BAN logic*

BAN logic is based on belief, whose goals are to prove that a principal believes certain statement. BAN logic is a kind of method which we are familiar with, so here only list some inference rules which may be used rather than detail notation and statements:

B1. Message Meaning Rule:

$$\frac{P \mid\equiv Q \leftrightarrow P,\ P \ \{ X \}\lhd K}{P \mid\equiv Q \mid\sim X}$$

B2. Nonce Verification Rule:

$$\frac{P \mid\equiv \#(X),\ P \mid\equiv Q \mid\sim X}{P \mid\equiv Q \mid\equiv X}$$

B3. Receiving Rule:

$$\frac{P(X, Y) \quad \frac{P \mid\equiv \lhd Q \leftrightarrow P,\ P \{ X \}\bowtie \lhd}{P \lhd X} \quad K}{P \lhd X}$$

$$P \mid\equiv \rightarrow P,\ P \ \{ X \}\bowtie \lhd K \qquad P \mid\equiv \rightarrow Q,\ P\bowtie \ \{ X \} K^{-1}$$

$$\frac{}{P \triangleleft X} \qquad \frac{}{P \triangleleft\!\!\triangleleft X}$$

B4. Freshness Rule:

$$\frac{P \mid\equiv \#(X)}{P \mid\equiv \#(X,Y)}$$

3.3. *Formal Analysis Model*

In order to study the security and privacy of the protocol, we build a model of formal analysis. We describe the formal analysis by Kailar logic and BAN logic.

3.4. *Using Kailar logic*

1.Protocol Goals:

（1） M CanProve (C Says H(Desc)) // C agrees with Desc.

（2） M CanProve (A Says Rec) // Transaction processed.

（3） C CanProve (M Says H(Desc)) // M agrees with Desc.

（4） C CanProve (A Says Rec) // Transaction processed.

（5） A CanProve (M Says H(Desc) ∧ M Says amount ∧ C Says H(Desc) ∧ C Says amount)

// C and M agree on H(Desc) and amount.

（6） A CanProve (M Says TID ∧ C Says TID) // C and M are talking about the same transaction.

（7） A CanProve (C Says CardData ∧ C Says amount) // C authorizes the value transfer.

2.Protocol Interpretation:

(1-1) C Receives (TID, Date, H(Desc)) SignedWith Km^{-1}

(2-1)M Receives (H (Desc), TID, Date) SignedWith Kc^{-1}

(3-1)A Receives (H (Desc), amount, IDM, TID, Date) SignedWith Km^{-1}

(3-2)A Receives (TID, Date, H(Desc), CardData, amount) SignedWith Kc^{-1}

(4-1) M Receives Rec SignedWith Ka^{-1}

(5-1) C Receives Rec SignedWith Ka^{-1}

3.Initial State Assumptions:

(I1) C, M CanProve (Ka Authecticates A)

(I2) C, A CanProve (Km Authecticates M)

(I3) A, M CanProve (Kc Authecticates C)

4.Analysis:

From statement(1-1)and assumption(I2), applying the Sign postulate can conclude:

C CanProve (M Says H(Desc)) ⇒ C CanProve (M agrees with Desc)

From statement(2-1)and assumption(I3), applying the Sign postulate can conclude:

M CanProve (C Says H(Desc)) ⇒ M CanProve (C agrees with Desc)

From statement(3-1) and assumption(I2), applying the Sign postulate can conclude:

A CanProve (M Says H(Desc)) (3-a)

A CanProve (M Says amount) (3-b)

A CanProve (M Says TID) (3-c)

From statement (3-2) and assumption(I3), applying the Sign postulate can conclude:

A CanProve (C Says H(Desc)) (3-d)

A CanProve (C Says amount) (3-e)

A CanProve (C Says TID) (3-f)

A CanProve (C Says CardData) (3-g)

From (3-a), (3-b), (3-d) and (3-e), applying the Conjunction postulate can conclude:

A CanProve (M Says H (Desc) ∧ M Says amount ∧ C Says H(Desc) ∧ C Says amount)

⇒ A CanProve (C and M agree on H (Desc) and amount)

From (3-c) and (3-f), applying the Conjunction postulate can conclude:

A CanProve (M Says TID ∧ C Says TID)

⇒ A CanProve (C and M are talking about the same transaction)

From (3-g) and (3-e), applying the Conjunction postulate can conclude:

A CanProve (C Says CardData ∧ C Says amount)

⇒ A CanProve (C authorizes the value transfer)

From statement (4-1) and assumption (I1), applying the Sign postulate can conclude:

M CanProve (A Says Rec) ⇒ M CanProve (Transaction processed)

From statement (5-1) and assumption (I1), applying the Sign postulate can conclude:

C CanProve (A Says Rec) ⇒ C CanProve (Transaction processed)

By analyzing the model with Kailar logic, we can conclude that the model meets accountability properties required.

3.5. *Using BAN logic*

The goal of this section is to show that the acquirer received the credit card number (*CardData*), the *amount*, and is able to deduce that they are fresh. We make the following assumptions:

1. All parties are able to get other parties' public keys in a secure manner (e.g. Using certificates).
2. Transaction ID and *Date* allow the parties to infer that a message is

new (fresh).

3. The credit card number is a shared secret between the customer and the acquirer.

In the analysis, we only use the first three messages of the model, since the other messages do not contribute to the logical properties of the protocol.

When C receives the first message, applying the Receiving rule can conclude:

C |≡ M |~ Desc

Applying the Nonce Verification rule then can conclude:

C |≡ M |≡ Desc

When M receives the second message, applying the Receiving rule and the Nonce Verification rule can conclude:

M |≡ C |≡ Desc

When A receives the third message, applying the Receiving rule, Nonce Verification rule and Freshness rule can conclude:

1. A |≡ M |≡ (amount, H (Desc))
2. A |≡ #H (Desc)
3. A |≡ C |≡ ⟨ amount ⟩ CardData
4. A |≡ C |≡ H (Desc)

As shown, the acquirer has no access to Desc but is able to conclude that C and M agree on it and on the value of amount. Principal A also deduces that the customer authorized a transfer of value amount from the account corresponding to CardData.

4. Conclusion

The analysis of the model with Kailar logic has shown that protocols of this type have good accountability, and the analysis with BAN logic has shown that this protocol has good authentication properties and meets their authentication goals. The use of the BAN logic has highlighted that the model uses two items to authenticate the customer: its public key and a shared secret (CardData). This allows us to infer new modes of usage for this kind of system, such as the sharing of a single credit card by many people without weakening the accountability properties of the system. Finally, we could verify that the acquirer is assured that the customer and the merchant agree on the description of the goods being sold, even if the acquirer has on access to such a description.

References

1. Donal O'Mahony, Michael Peirce, and Hitesh Tewari. Electronic Payment Systems. Artech House, 1997.

2. Aigbe P, Akpojaro J. Analysis of Security Issues in Electronic Payment Systems. International Journal of Computer Applications, 108(10): 10-14, 2014.
3. Dreier J, Kassem A, Lafourcade P, et al. Formal Analysis of E-Cash Protocols. international conference on security and cryptography, 2015.
4. Lucas de Carvalho Ferreira and Ricarko Dahab. Formal Analysis of a Model for Electronic Payment Systems.
5. Michael Burrows, Martin Abadi, and Roger Needham. A logic of authentication. ACM Transactions on Computer Systems, 8(1): pp. 18-36, February 1990.
6. Rajashekar Kailar. Accountability in electronic commerce protocols. IEEE Transactions on software engineering, 22(5), May 1996.