British Journal of Mathematics & Computer Science
22(1): 1-14, 2017, Article no.BJMCS.32744
ISSN: 2231-0851

SCIENCEDOMAIN *international*
www.sciencedomain.org

Formal Analysis of MCAP Protocol Against Replay Attack

Shadi Nashwan[1] **and Bandar M. Alshammari**[1*]

[1] *Department of Computer Science, Aljouf University, Saudi Arabia.*

Authors' contributions

This work was carried out in collaboration between both authors. Both authors read and approved the final manuscript.

Article Information

DOI: 10.9734/BJMCS/2017/32744
Editor(s):
(1) Doina Bein, Applied Research Laboratory, The Pennsylvania State University, USA.
(2) Vitor Carvalho, Polytechnic Institute of Cávado and Ave, Portuguese Catholic University and Lusiada University, Portugal.
(3) Dariusz Jacek Jakóbczak, Chair of Computer Science and Management in this Department, Technical University of Koszalin, Poland.
Reviewers:
(1) G. Y. Sheu, Chang-Jung Christian University, Tainan, Taiwan.
(2) Rui Guo, Xi'an University of Posts and Telecommunications, PR China.
(3) Zahid Akhtar, University of Quebec, Canada.
Complete Peer review History: http://www.sciencedomain.org/review-history/19003

Original Research Article

Received: 14th March 2017
Accepted: 2nd May 2017
Published: 10th May 2017

Abstract

Replay attack is considered a common attacking technique that is used by adversaries to gain access to confidential information. Several approaches have been proposed to prevent replay attack in security-critical systems such as Automated Teller Machines (ATM) systems. Among those approaches is a recent one called the Mutual Chain Authentication Protocol for the Saudi Payments Network transactions (MCAP). This protocol aims to allow Saudi banking systems to overcome existing weaknesses in the currently used Two-Factor Authentication (2FA) protocols. In this paper, we analyze and verify the recent MCAP authentication protocol against replay attacks. Therefore, we examine the mutual authentication between the ATM Terminal, Sponsoring Banks (SBAT), Saudi Payments Network (SPAN) and the Issuing of Financial Bank (CIFI). The paper also provides a formal analysis of the MCAP to conduct formal proofs of the MCAP protocols against replay attacks.

Keywords: ATM Systems; SPAN Networks; Mutual Chain Authentication Protocol (MCAP); replay attack.

**Corresponding author: E-mail: bmshammeri@ju.edu.sa;*
Email: shadi$_n$*ashwan@ju.edu.sa*;

2010 Mathematics Subject Classification: 53C25, 83C05, 57N16.

1 Introduction

Protecting critical data in financial systems from being exploited by unauthorized parties is a major concern. As the number of payment networks increases, the services they provide increase rapidly. Providing these services to customers in a secure way is the main challenge. In many cases, attackers can easily gain access to information during transmissions across the Automated Teller Machine (ATM) networks. This can allow them to gain unauthorized access to the sponsoring banks or the issuing of financial bank to whom they are not allowed to access.

MCAP protocol [1] was proposed to be used for SPAN transactions in Saudi Arabia banking systems in order to solve existing vulnerabilities in the current two-factor-authentication (2FA) protocol [2] [3]. MCAP is defined as an Authentication and Key Agreement protocol (AKA) which uses pre-loaded shared keys between authentication entities [4] [5]. Moreover, MCAP meets all the security requirements of ATM systems specified by Singh et al. [6]. Therefore, there are no input authentication variables are transported as plain texts by the authentication messages between the ATM system components. Furthermore, the mutual authentication between all the ATM system components is achieved. This means that ATM card holders must prove themselves to the system in order for the system to prove itself to the network. In general, the MCAP protocol is resistant against the known attacks such as Replay attack, and hence this paper aims to prove such hypothesis using a formal verification approach.

Technically, replay attacks aim to maliciously or fraudulently repeat transmission of valid data through the originator or an adversary who can capture the data and redirect it to unauthorized sides [7] [8] [9] [10]. If messages are exchanged in such an authentication protocol that does not carry appropriate freshness identifiers, then an adversary can easily get authenticated by replaying messages copied from a legitimate authentication session between authentication entities [7] [8] [9] [10] [11] [12].

The main purpose of this paper is to perform an evaluation of the MCAP objectives and analyze it against replay attack using a formal verification approach. Formal verification is the use of mathematical techniques to ensure that a certain design conforms to some precisely expressed notion of functional correctness. The absence of formal methods for verification of security protocols could lead to security errors remaining undetected [13]. Moreover, formal verification techniques can provide a systematic way of discovering protocol flaws [14] [15] [16] [17] [18] [19] [20]. This allows us to check if there are any inconsistencies might exist in the MCAP. Then, we use a formal verification approach called the BAN logic formal methods on the MCAP protocol to prove that no threats or vulnerabilities can be exploited in MCAP as a result of replay attack methods [21] [22] [23]. Unfortunately, we are not able to compare our protocol with others since this protocol has been recently proposed and there is no similar protocol which is specifically defined for the case of banking systems in Saudi Arabia.

The rest of the paper is organized as follows. Section 2 provides an overview of the MCAP authentication protocol. Section 3 illustrates a security analysis of the MCAP protocol against replay attacks. Then, we formally verify the security of the MCAP authentication protocol against replay attack using the BAN logic formal method in Section 4. Finally, Section 5 concludes the salient results of the paper.

2 Overview of MCAP Protocol

According to the specifications of MCAP [1], the mutual chain in the authentication session consists of four pairs of initiator-responder messages. These pairs are divided into two classes (direct and indirect) [1]. In direct class, the mutual authentications between (ATM terminals and Sponsoring banks (SBAT)), (SBAT and SPAN), and (SPAN and CIFI) depend on the values of (old and new) transaction numbers as freshness values. On the

other hand, the mutual authentications between (ATM terminal and Issuing of Financial Bank (CIFI)) in indirect class depend on the value of (RAND) that is created by the ATM terminal and ATM Card Identity (ACI).

2.1 Direct class of mutual authentication

Direct mutual authentication during the authentication session between the authentication entities is shown in Fig. 1. The initiator (I) begins authorization by sending a challenge expected value that represents the authentication request message. In Fig. 1.a, the ATM terminal sends XRES2 value to SBAT. It is an encrypted value generated from a new transaction number SQNATMS + 1 (i.e., the Sequence number of ATM terminal and SBAT) exclusive-or (XOR) with the identity number of the ATM terminal (AMID) based on the pre-loaded shard key (K2) between the ATM terminal and SBAT. In Fig. 1.b, the SBAT sends XRES3 value to SPAN. XRES3 is an encrypted value of a new transaction number SQNSS + 1 (i.e., the Sequence number of SBAT and SPAN) of SBAT exclusive-or (XOR) with AMID based on the pre-loaded shard key (K3) between the SBAT and SPAN. In Fig. 1.c, the SPAN sends XRES4 value to CIFI which is an encrypted value of AMID based on the pre-loaded shard key (K4) between the SPAN and CIFI.

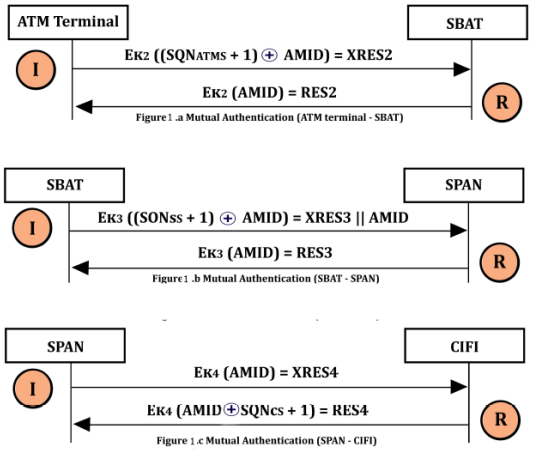

Fig. 1. Direct Mutual Authentication (ATM terminal, SBAT, SAPN, CIFI)

In the opposite direction, the responder (R) sends back the expected response value which represents the authentication response message. In fig. 1.c, the CIFI sends back RES4 value to the SPAN. RES4 is an encrypted value of a new transaction number SQNCS + 1 (i.e., next Sequence transaction number between CIFI and SPAN) exclusive-or (XOR) with the (AMID) based on (K4). In Fig. 1.b, the SPAN sends back RES3 value to SBAT. RES3 is an encrypted value of AMID based on (K3). In Fig. 1.a, the SBAT sends backs RES2 value to the ATM terminal. RES2 is an encrypted value of AMID based on (K2).

2.2 Indirect class of mutual authentication

Fig. 2 shows the indirect mutual authentication during the authentication session between the ATM terminal and the CIFI authentication entities. The initiator ($I \rightarrow ATM\ Terminal$) begins authorization by sending a challenge expected value (ISID || XACI || XRES1) to CIFI through SBAT and SPAN entities. XRES1 is an encrypted value of (RAND) based on the pre-loaded shard key (K1) between the ATM terminal and CIFI. XACI is an encrypted value of the ATM card identity (ACI) exclusive-or (XOR) with the identity number of the ATM terminal (AMID) based on (K1). In the opposite direction, the responder ($R \rightarrow CIFI$) sends back the expected response value (RES1) to the ATM terminal through the same direction and authentication entities of the challenge message, which is an encrypted value of (RAND +1).

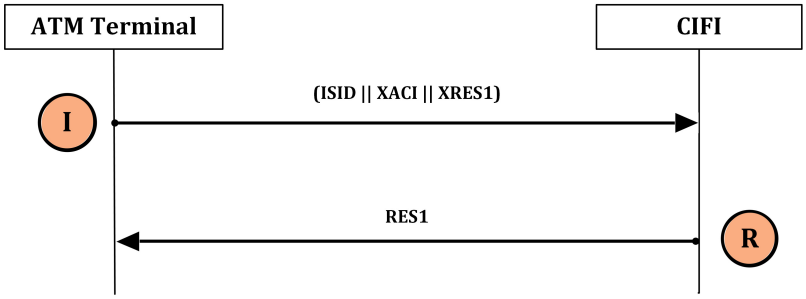

Fig. 2. Indirect Mutual Authentication (ATM Terminal - CIFI)

3 Security Analysis of MCAP Against Replay Attacks

Security protocols are often used to ensure secure communications in a hostile environment. Authenti-cation protocols are always vulnerable to a variety of attacks such as message replay, data interception and manipulation, repudiation, and impersonation. Therefore, it is necessary for systems' designers to have some degree of assurance before enforcing any authentication protocol [14].

Attacking authentication protocols using replay attacks approach can be done using the authentication request message (challenge message of initiator), authentication response message (response message of responder) or may be based on both messages [14]. If messages in any authentication protocol are exchanged without appropriate freshness identifiers, then an adversary can easily get themselves authenticated by replaying messages copied from a legitimate authentication session. In MCAP, the freshness identifiers are used in both direct and indirect class mutual authentication [1].

Results of MCAP authentication processes for all authentication events are completely ciphered based on the ciphered keys (EK1, EK2, EK3 and EK4) [1]. All authentication streams whether they are initiator or responder messages must contain ciphered variables [1]. These processes use the pre-loaded ciphered keys without transferring the value of the cipher keys between the entities of ATM systems [1].

In the direct class, authentication processes between all entities are represented by a mutual of Challenge and Response ciphered messages [(XRES2/RES2), (XRES3/RE3) and (XRES4/RES4)], which are computed based on the cipher keys (EK2, EK3 and EK4) consequently [1]. These mutual cipher messages depend on the freshness parameters (SQN) that are included in the system entities databases. They also depend on the AMID parameter that is attached to the authentication request message by the SBAT entity. When the initiator sends a challenge message as a cipher stream to the next system entity, the authentication entity evaluates the freshness of the SQN value by two values to check whether these values are equal or not. One of these values is the SQNnew which is extracted from the output of the decryption process (XRES value), while the other is the SQNold which is included in the database of the system entity. In case both values (SQNnew and SQNold) are in range, then the authentication entity sends an authentication request to the next system entity. On the other hand, a mismatch message is transmitted to the initiator. At the opposite side, the AMID value is validated by the authentication entity through comparing the AMID that is fetched from the decryption value of RES with the value that is attached to the authentication request message. In case they are not in rang, then a mismatch authentication message is returned.

In indirect class, authentication processes are performed between ATM Terminal and CIFI based on the XRES1, XACI and RES1 values. The ATM Terminal performs authentication processes by calculating XRES1 and XACI values depending on the pre-loaded shred key (EK1) so it can authenticate itself to the CIFI. In each

authentication session, the ATM terminal computes a new RAND value which is used to modify the XRES1 and XACI values. At the opposite side, CIFI performs an authentication process to find RES1 value which depends on the same cipher key (i.e., EK1). This process is conducted in order for CIFI to authenticate itself to the ATM terminal. RES1 value can be also changed based on the incremental value of (RAND + 1).

The freshness values of RAND, AMID, and SQNS of transactions (SQNATMS, SQNSS, and SQNCS) generate different challenge and response messages for each authentication session. If the same ATM card holder uses the same ATM Terminal, the previous challenge message cannot be used again. Moreover, the attacker can neither play the role of an intruder entity, access the provided services, nor impersonate legal users between legal authentication entities.

4 Formal Analysis of MCAP Protocol

BAN logic represents a powerful tool to describe and validate authentication protocols [19]. It provides a formal method for reasoning about the beliefs of principals in authentication protocols [19] [24] [25]. Its main objective is to believe that a message is authentic if it is encrypted with a relevant key and fresh in each authentication session of the authentication protocol [15] [26] [27] [28] [29] [30].

In this section, we use BAN logic approach to formalize and prove that MCAP [1] protocol is resistant against replay attacks. In order to achieve this goal, we have to address two principles. The first one is related to proving that if an initiator sends a challenge request message (whether in indirect or direct class) to a responder for the first time and it receives that message back from the responder which depends on the freshness value of RAND and SQN, then the initiator ought to believe that the responder's message is fresher than its message. The second principle is related to proving that if the initiator believes that only the responder knows the pre-loaded shared key, then the initiator ought to believe that any encrypted message has been received from a legal responder.

In the following sections, we provide an illustration for BAN notations and deduction rules which are of interest to our case. We also show how to formally prove that MCAP is resistant against replay attacks using BAN logic rules. This followed by a section that summarizes our findings and results.

4.1 BAN logic notations

The definition of BAN logic notations and their implications are presented in Fig. 3 (assuming P and Q are network agents, X is a message, and K is an encryption key).

4.2 BAN logic deduction rules

The deduction rules that are used in the analysis of the proposed scheme are described below [15] [19]. Each rule has the form:

$$\frac{hypotheses}{conclusion} \quad \text{[name]}$$

where the judgment appearing as the conclusion is considered valid if the hypotheses are all true.

$P \mid \equiv X$	Denotes that P believes X.	• P may act as though X is true.
$P \triangleleft X$	Denotes that P sees X.	• Someone has sent P a message containing X. • P can read X and can repeat it in other messages.
$P \mid X$	Denotes that P said X at one time	• P transmitted (and believed) message X. • Although P might no longer believe X.
$P \mid \Rightarrow X$	Denotes that P control X	• P has jurisdiction over X. • P is a trusted authority on the truth of X.
$\#(X)$	Denotes that X is fresh	• X has not been sent in a message at any time before the current run of the protocol.
$P < K > Q$	Denotes that K is a good shared key for communication between P and Q	• K will never be discovered by any principal except for P or Q.
$P = X = Q$	Denote X is a secret known only to P and Q	• Only P and Q may use X to prove their identities to one another.
$\{X\}K$	Denotes that X encrypted with the key K	• Indicates that if the decryption value of X is true then K is secret.
$< X > Y$	X is combined with Y	• Intent is that Y is a secret. • Y proves the origin of X.

Fig. 3. BAN Logic Notations Used in Contexts

4.2.1 The message meaning rule

This rule concerns the interpretation of messages and helps to explain the origin of the messages for a shared key.

$$\frac{P \mid \equiv P < K > Q, P \triangleleft \{X\}K}{P \mid \equiv Q \mid X} \quad \text{[Message Meaning Rule]}$$

This rule indicates that if P believes that K is a good key for P and Q, and P sees that X is encrypted with K, then P believes that Q once said X.

4.2.2 The nonce verification rule

This rule ensures that decryption of a message only says that it was uttered at some point (possibly in the past). It reflects the essence of Challenge/Response protocols (fresh statement is a challenge) and any message contains that challenge is also fresh.

$$\frac{P| \equiv \{X\}, P| \equiv Q \mid X}{P| \equiv Q \mid \equiv X} \quad \text{[Nonce Verification Rule]}$$

This rule indicates that if P believes that X was said recently, and that Q said X, then P believes that Q believes X.

4.2.3 The jurisdiction rule

This rule states what it means for a principle to be the trusted authority on the truth of X.

$$\frac{P| \equiv Q \Rightarrow X, P| \equiv Q \mid \equiv X}{P| \equiv X} \quad \text{[Jurisdiction Rule]}$$

This rule indicated that if P believes that Q has jurisdiction over X, then P trusts Q on the truth of X.

4.2.4 The seeing rule

This rule says that a principle sees all the components of every message it sees, providing that the principle knows the necessary key.

$$\frac{P \triangleleft (X,Y)}{P \triangleleft (X)} \quad \text{[Seeing Rule (1)]}$$

$$\frac{P| \equiv P < K > Q, P \triangleleft \{X\}K}{P \triangleleft X} \quad \text{[Seeing Rule (2)]}$$

If a principle sees a formula, then it can see its components (provided keys are known).

$$\frac{P \mid \equiv \#(X)}{P \mid \equiv \#(X,Y)} \quad \text{[Seeing Rule (3)]}$$

If part of a formula is known to be fresh, then the entire formula is fresh.

4.2.5 The belief rule

This rule states that a principle believes a collection of statements, if and only if it believes each statement individually.

$$\frac{P \mid \equiv (X,Y)}{P \mid \equiv X} \quad \text{[Belief Rule]}$$

In this rule, P believes a set of statements if and only if P believes each individual statement.

4.3 Security proof

The prevention of MCAP protocol against the replay attack can be proved through the following four steps:

1. Transforming the MCAP protocol into an idealized form.
2. Identifying the initial assumptions using BAN logic.
3. Deducing new predicates using the BAN logic rules.
4. Showing that the goals of MCAP protocol have been met.

The first step relates to idealizing the MCAP protocol. The original version of the MCAP protocol without idealization form is shown below.

- Message (1) : $ATM\ terminal \rightarrow SBAT : ISID \ || \{XACI \ || XRES1\}K1 \ || \{XRES2\}K2$.
- Message (2) : $SBAT \rightarrow SPAN : ISID \ || \{XACI \ || XRES1\}K1 \ || \{XRES3\}K3$.
- Message (3) : $SPAN \rightarrow CIFI : ISID \ || \{XACI \ || XRES1\}K1 \ || \{XRES4\}K4$.
- Message (4) : $CIFI \rightarrow SPAN : \ \{RES1\}K1 \ || \{RES4\}K4$.
- Message (5) : $SPAN \rightarrow SBAT : \ \{RES1\}K1 \ || \{RES3\}K3$.
- Message (6) : $SBAT \rightarrow ATM\ Terminal : \ \{RES1, RES2\}K1$.

We idealize the MCAP protocol through replacing the challenge and response messages with idealized messages. Each authentication entity sees the following messages.

- Idealized Message (1) : $CIFI \triangleleft (ISID, XACI, XRES, XRES4)$
- Idealized Message (2) : $SPAN \triangleleft (ISID, XACI, XRES, XRES3)$
- Idealized Message (3) : $SPAN \triangleleft (RES1, RES4)$
- Idealized Message (4) : $SBAT \triangleleft (ISID, XACI, XRES1, XRES3)$
- Idealized Message (5) : $SBAT \triangleleft (RES1, RES3)$
- Idealized Message (6) : $ATM\ Terminal \triangleleft (RES1, RES2)$

The second step of proving that our MCAP protocol is resistant against replay attacks is to identify a set of assumptions using BAN logic. The initial suppositions of the MCAP indicate that all the authentication entities can use a shared key to communicate whether in challenge or response messages as follows.

- Supposition (1) : $CIFI < K1 > ATM\ Terminal$ [For Indirect Class]
- Supposition (2) : $SBAT < K2 > ATM\ Terminal$ [For Direct Class]
- Supposition (3) : $SBAT < K3 > SPAN$ [For Direct Class]
- Supposition (4) : $CIFI < K4 > SPAN$ [For Direct Class]

The third and fourth step of proving that our MCAP protocol is resistant against replay attacks is to deduce new predicates using the BAN logic rules and show that the objectives of MCAP are met. We conduct these two last steps on the direct class communications and then on the indirect class communications as follows.

4.3.1 Direct class security proof

In this part, we show how to prove that our MCAP protocol is secured against the replay attacks in direct class communications (i.e., SBAT and ATM Terminal, SPAN and SBAT, and CIFI and SPAN).

A) SBAT and ATM Terminal:

The first part of this proof is to show that SBAT believes that the per-loaded shared key with an ATM terminal, and that ATM terminal believes that the per-loaded shared key with the SBAT. Hence, the SBAT believes that the value of $XRES2$ is fresh and the ATM terminal believes that the value of $RES2$ is fresh. The set of principles which we aim to prove here are as follows.

$$SBAT \mid \equiv SBAT < K2 > ATM\ Terminal \tag{GA1}$$

$$SBAT \mid \equiv \#(XRES2) \tag{GA2}$$

$$ATM\ Terminal \mid \equiv ATM\ Terminal < K2 > SBAT \tag{GA3}$$

$$ATM\ Terminal \mid \equiv \#(RES2) \tag{GA4}$$

By applying the Message Meaning rule and according to Supposition 2 of the MCAP protocol, we get the following. $SBAT \mid \equiv SBAT < K2 > ATM\ Terminal, SBAT \triangleleft \{XRES2\}K2/SBAT \mid \equiv ATM\ Terminal \mid (XRES2)$ and $SBAT \mid \equiv ATM\ Terminal \mid (XRES2)$. If we say that $(ATM\ SQN_{new} == ATM\ SQN_{old} + 1)$, then we can prove the following.

$$SBAT \mid \equiv SBAT < K2 > ATM\ Terminal \tag{GA1}$$

By applying the Nonce Verification rule and according to the fact that $(SQN_{new} == ATM\ SQN_{old} + 1)$, then the value of $XRES2$ is fresh. If we know that $(SBAT \mid \equiv \#(XRES2), SBAT \mid \equiv ATM\ Terminal \mid (XRES2)/SBAT \mid \equiv ATM\ Terminal \mid \equiv (XRES2))$, then this leads to $(SBAT \mid \equiv ATM\ Terminal \mid \equiv (XRES2))$.

By applying the Jurisdiction rule, we can prove that $(SBAT \mid \equiv ATM\ Terminal \mid \Rightarrow (XRES2), SBAT \mid \equiv ATM\ Terminal \mid \equiv (XRES2)/SBAT \mid \equiv ATM\ Terminal)$, and this leads to deduce the following, $SBAT \mid \equiv (XRES2)$, and therefore we prove the following.

$$SBAT \mid \equiv \#(XRES2) \tag{GA2}$$

By applying the Message Meaning rule and according to Supposition 2 in the MCAP protocol, it can be shown that $(ATM\ Terminal \mid \equiv ATM\ Terminal < K2 > SBAT, ATM\ Terminal \triangleleft \{RES2\}K2/ATM\ Terminal \mid \equiv SBAT \mid (RES2))$ and $(ATM\ Terminal \mid \equiv SBAT \mid (RES2))$. If we can say that $(AMID == AMID)$, then we can deduce the following.

$$ATM\ Terminal \mid \equiv ATM\ Terminal < K2 > SBAT \tag{GA3}$$

By applying the Nonce Verification rule and according to the fact that $(AMID == AMID)$, then the value of $(RES2)$ is fresh. If we say that $(ATM\ Terminal \mid \equiv \#(RES2), ATM\ Terminal \mid \equiv SBAT \mid (RES2)/ATM\ Terminal \mid \equiv SBAT \mid \equiv (RES2))$. This leads to the following, $(ATM\ Terminal \mid \equiv SBAT \mid \equiv (RES2)$ and $ATM\ Terminal \mid \equiv SBAT \mid \equiv \#(RES2))$.

By applying the Jurisdiction rule, we get $(SBAT \mid \equiv ATM\ Terminal \mid \Rightarrow (RES2), SBAT \mid \equiv ATM\ Terminal \mid \equiv (RES2)/SBAT \mid \equiv ATM\ Terminal)$, which leads to deducing that $(ATM\ Terminal \mid \equiv (RES2))$, and hence proving the following.

$$ATM\ Terminal \mid \equiv \#(RES2) \tag{GA4}$$

B) SPAN and SBAT:

The second set of goals is to prove that SPAN believes that the per-loaded shared key with SBAT, and to prove that SBAT believes that the per-loaded shared key with SPAN. An additional goal is to prove that SPAN and

SBAT believe that the value of $(XRES3)$ is fresh. The set of principles which we aim to prove in this part are as follows.

$$SPAN \mid \equiv SPAN < K3 > SBAT \tag{GB1}$$

$$SPAN \mid \equiv \#(XRES3) \tag{GB2}$$

$$SBAT \mid \equiv SBAT < K3 > SPAN \tag{GB3}$$

$$SBAT \mid \equiv \#(RES3) \tag{GB4}$$

By applying the Message Meaning rule and according to Supposition 3 of the MCAP protocol, we get that $(SPAN \mid \equiv SPAN < K3 > SBAT, SPAN \triangleleft \{XRES3\}K3/SPAN \mid \equiv SBAT \mid (XRES3)$, thus, $SPAN \mid \equiv SBAT \mid (XRES3))$. If we say that $(SQN_{SSnew} == SQN_{SSnew}(output\ of\ f4*))$, then we can deduce the following.

$$SPAN \mid \equiv SPAN < K3 > SBAT \tag{GB1}$$

By applying the Nonce Verification rule and according to the fact that $(SQN_{SSold} == SQN_{SSnew})$, then the value of $(XRES3)$ is fresh. Furthermore, $(SPAN \mid \equiv \#(RES3), SPAN \mid \equiv SBAT \mid (XRES3)/SPAN \mid \equiv SBAT \mid \equiv (XRES3))$. This leads to $(SPAN \mid \equiv SBAT \mid \equiv (XRES3)$ and $SPAN \mid \equiv SBAT \mid \equiv \#(XRES3))$.

By applying the Jurisdiction rule, we can prove that $(SPAN \mid \equiv SBAT \mid \Rightarrow (XRES3), SPAN \mid \equiv SBAT \mid \equiv (XRES3)/SPAN \mid \equiv SBAT)$. This leads to deduce that $(SPAN \mid \equiv (XRES3))$, and hence,

$$SPAN \mid \equiv \#(XRES3) \tag{GB2}$$

By applying the Message Meaning rule and according to Supposition 2 in the MCAP protocol, $(SBAT \mid \equiv SBAT < K3 > SPAN, SBAT \triangleleft \{RES3\}K3/SBAT \mid \equiv SPAN \mid (RES3))$, and thus, $(SBAT \mid \equiv SPAN \mid (RES3))$. Since $(AMID == AMID(output\ of\ f6*))$, then we can prove the following.

$$SBAT \mid \equiv SBAT < K3 > SPAN \tag{GB3}$$

By applying the Nonce Verification rule and according to the fact that $(AMID == AMID)$, then the value of $(RES3)$ is fresh. $(SBAT \mid \equiv \#(RES3), SBAT \mid \equiv SPAN \mid (RES3)/SBAT \mid \equiv SPAN \mid \equiv (RES3))$. This leads to the following. $(SBAT \mid \equiv SPAN \mid \equiv (RES3)$ and $SBAT \mid \equiv SPAN \mid \equiv \#(RES3))$.

By applying the Jurisdiction rule, we can show that $(SPAN \mid \equiv SBAT \mid \Rightarrow (RES3), SPAN \mid \equiv SBAT \mid \equiv (RES3)/SPAN \mid \equiv SBAT)$. This can lead to $(SBAT \mid \equiv (RES3))$, and this proves the following.

$$SBAT \mid \equiv \#(RES3) \tag{GB4}$$

C) CIFI and SPAN:

The third set of goals is to prove CIFI believes that the per-loaded shared key with SPAN and SPAN believes that the per-loaded shared key with CIFI. It also aims to prove that CIFI and SPAN believe that the value of $(XRES4)$ is fresh. Below are the set of goals that we aim to prove in this part.

$$CIFI \mid \equiv CIFI < K4 > SPAN \tag{GC1}$$

$$CIFI \mid \equiv \#(XRES4) \tag{GC2}$$

$$SPAN \mid \equiv SPAN < K4 > CIFI \tag{GC3}$$

$$SPAN \mid \equiv \#(RES4) \tag{GC4}$$

By applying the Message Meaning rule and according to Supposition 3 of the MCAP protocol, we can say that $(CIFI \mid \equiv CIFI < K4 > SPAN, CIFI \triangleleft \{XRES4\}K4/CIFI \mid \equiv SPAN \mid (XRES3))$, and thus $(CIFI \mid \equiv SPAN \mid (XRES4))$. If we say that $(AMID(output\ of\ f12*) == AMID(output\ of\ f1*))$, then we can deduce the following.

$$CIFI \mid \equiv CIFI < K4 > SPAN \tag{GC1}$$

By applying the Nonce Verification rule and according to the fact that $(AMID == AMID)$, then the value of $(XRES4)$ is fresh. This leads to $(CIFI \mid \equiv \#(XRES4), CIFI \mid \equiv SPAN \mid (XRES4)/CIFI \mid \equiv SPAN \mid \equiv (XRES4))$, $(CIFI \mid \equiv SPAN \mid \equiv (XRES3))$, and $(CIFI \mid \equiv SPAN \mid \equiv \#(XRES4))$.

By applying the Jurisdiction rule, we can prove that $(CIFI \mid \equiv SPAN \mid \Rightarrow (XRES4), CIFI \mid \equiv SPAN \mid \equiv (XRES4)/CIFI \mid \equiv SPAN)$. This leads to deduce that $(CIFI \mid \equiv (XRES4))$, and hence this proves the following.

$$CIFI \mid \equiv \#(XRES4) \tag{GC2}$$

By applying the Message Meaning rule and according to Supposition 4 in the MCAP protocol, $(SPAN \mid \equiv SPAN < K4 > CIFI, SBAT \triangleleft \{RES4\}K4/SPAN \mid \equiv CIFI \mid (RES4))$, and thus $(SPAN \mid \equiv CIFI \mid (RES4))$. Since $(SQN_{CSold} == SQN_{CSnew}(output\ of\ f5*))$, then we can prove the following.

$$SPAN \mid \equiv SPAN < K4 > CIFI \tag{GC3}$$

By applying the Nonce Verification rule and according to the fact that $(SQN_{CSold} == SQN_{CSnew})$, then the value of $(RES4)$ is fresh.

Since $(SPAN \mid \equiv \#(RES4), SPAN \mid \equiv CIFI \mid (RES4)/SPAN \mid \equiv CIFI \mid \equiv (RES4))$, then this leads to the following $(SPAN \mid \equiv CIFI \mid \equiv (RES4))$ and $(SPAN \mid \equiv CIFI \mid \equiv \#(RES4))$.

By applying the Jurisdiction rule, we can show that $(CIFI \mid \equiv SPAN \mid \Rightarrow (RES4), CIFI \mid \equiv SPAN \mid \equiv (RES4)/CIFI \mid \equiv SPAN)$. This leads to $(SPAN \mid \equiv (RES4))$ which proves the following.

$$SPAN \mid \equiv \#(RES4) \tag{GC4}$$

4.3.2 Indirect class security proof

In this section, we aim to prove the fourth set of goals of the MCAP protocol. This aims to prove that CIFI believes that the per-loaded shared key with an ATM terminal, and that ATM terminal believes that the per-loaded shared key with the CIFI (Mutually authentication key establishment between CIFI and ATM terminal). In this section, we also aim to prove that the CIFI believes that the value of $(XACI)$ is fresh and the ATM terminal believes that the value of $(RES1)$ is fresh. The set of principles which we aim to prove in this part are as follows.

$$CIFI \mid \equiv CIFI < K1 > ATM\ Terminal \tag{GD1}$$

$$CIFI \mid \equiv \#(XACI) \tag{GD2}$$

$$ATM\ Terminal \mid \equiv ATM\ Terminal < K1 > CIFI \tag{GD3}$$

$$ATM\ Terminal \mid \equiv \#(RES1) \tag{GD4}$$

By applying the Message Meaning rule and according to Supposition 3 of the MCAP protocol, we can say that $(CIFI \mid \equiv CIFI < K1 > ATM\ Terminal, CIFI \triangleleft \{XACI\}K1/CIFI \mid \equiv ATM\ Terminal \mid (XACI))$, hence $(CIFI \mid \equiv ATM\ Terminal \mid (XACI))$. If we say that $(ACI == ACI)$ and $(AMID == AMID(output\ of\ f12*))$, then we can deduce the following.

$$CIFI \mid \equiv CIFI < K1 > ATM\ Terminal \tag{GD1}$$

By applying the Nonce Verification rule and according to the fact that $(ACI == ACI)$ and $(AMID == AMID)$, then the value of $(XRES1)$ is fresh. This leads to $(CIFI \mid \equiv \#(XACI), CIFI \mid \equiv ATM\ Terminal \mid (XACI)/CIFI \mid \equiv ATM\ Terminal \mid \equiv (XACI))$, $(CIFI \mid \equiv ATM\ Terminal \mid \equiv (XACI))$, and $(CIFI \mid \equiv ATM\ Terminal \mid \equiv \#(XACI))$.

By applying the Jurisdiction rule, we can prove that $(CIFI \mid \equiv ATM\ Terminal \mid \Rightarrow (XACI), CIFI \mid \equiv ATM\ Terminal \mid \equiv (XACI)/CIFI \mid \equiv ATM\ Terminal)$. Then, this leads to deduce that $(CIFI \mid \equiv (XACI))$ which proves the following.

$$CIFI \mid \equiv \#(XACI) \tag{GD2}$$

By applying the Message Meaning rule and according to Supposition 1 in the MCAP protocol, $(ATM\ Terminal \mid \equiv ATM\ Terminal < K1 > CIFI, ATM\ Terminal \triangleleft \{RES1\}K1/ATM\ Terminal \mid \equiv CIFI \mid (RES1))$, and $(ATM\ Terminal \mid \equiv CIFI \mid (RES1))$. Since $((RAND(output\ of\ f0) == RAND(output\ of\ f3*))$, then we can prove the following.

$$ATM\ Terminal \mid \equiv ATM\ Terminal < K1 > CIFI \tag{GD3}$$

By applying the Nonce Verification rule and according to the fact that $(RAND(output\ of\ f0) == RAND(output\ of\ f3*))$, then the value of $(RES1)$ is fresh. Since $(ATM\ Terminal| \mid \equiv \#(RES1), ATM\ Terminal| \mid \equiv CIFI \mid (RES1)/ATM\ Terminal \mid \equiv CIFI \mid \equiv (RES1))$, then this leads to $(ATM\ Terminal \mid \equiv CIFI \mid \equiv (RES1)$ and $ATM\ Terminal \mid \equiv CIFI \mid \equiv \#(RES1))$.

By applying the Jurisdiction rule, we can show that $(CIFI \mid \equiv ATM\ Terminal \mid \Rightarrow (RES1), CIFI| \equiv ATM\ Terminal \mid \equiv (RES1)/CIFI \mid \equiv ATM\ Terminal)$. This leads to $(ATM\ Terminal \mid \equiv (RES1))$ which proves the following.

$$ATM\ Terminal \mid \equiv \#(RES1) \tag{GD4}$$

Table 1. Mutual Authentication Deduction Rules for MCAP

Keys	Authentication Entities	Mutual Authentication Deduction Rules	Fresh Message Deduction Rules
K1	ATM Terminal & CIFI	$CIFI \mid \equiv CIFI < K1 > ATM\ Terminal$ and $ATM\ Terminal \mid \equiv ATM\ Terminal < K1 > CIFI$	$ATM\ Terminal| \mid \equiv \#(RES1)$ and $CIFI| \equiv \#(XACI)$
K2	ATM Terminal & SBAT	$SBAT \mid \equiv SBAT < K2 > ATM\ Terminal$ and $ATM\ Terminal \mid \equiv ATM\ Terminal < K2 > SBAT$	$ATM\ Terminal| \mid \equiv \#(RES2)$ and $SBAT| \equiv \#(XRES2)$
K3	SBAT & SPAN	$SPAN \mid \equiv SPAN < K3 > SBAT$ and $SBAT \mid \equiv SBAT < K3 > SPAN$	$SBAT \equiv \#(RES3)$ and $SPAN| \equiv \#(XRES3)$
K4	SPAN & CIFI	$SPAN \mid \equiv SPAN < K4 > CIFI$ and $CIFI \mid \equiv CIFI < K4 > SPAN$	$SPAN \equiv \#(RES4)$ and $CIFI| \equiv \#(XRES4)$

4.4 Summary of security proofs

By following the notations and deduction rules that are presented in the previous section, we prove that MCAP protocol is resistant against the replay attacks. These Mutual Authentication Deduction Rules for MCAP can be summarized as shown in Table 1.

Table 1 shows that if the initiator's challenge request message in the MCAP protocol has never been sent to the responder and the initiator receives the response message which depends on the freshness from the responder, then the initiator ought to believe that the responder's message is fresher than its message. It also shows that if all initiators believe that only the responder knows the pre-loaded shared key, then the initiator ought to believe that any encrypted message has been received is from a legal responder. In this paper, we have also shown that all suppositions in Section 4 are achieved, and therefore the MCAP protocol can be considered secure against the replay attack.

5 Conclusion

This paper has shown how to analyze and verify that the MCAP protocol is secure against replay attacks. In order to achieve this goal, we had to analyze the differences between the mutual authentications whether during

direct or indirect authentication entities. Then, we provided a formal analysis of the MCAP protocol using the BAN logic approach. The formal analysis proved that the trusted relation between the authentication entities can be achieved by preventing the acceptance of any challenge or response messages that do not have fresh values. Therefore, the MCAP protocol sets up a secure connection between the authentication entities and prevents the possibility of replay attacks.

Competing Interests

Authors have declared that no competing interests exist.

References

[1] Nashwan S, Alshammari B. Mutual chain authentication protocol for SPAN transactions in Saudi Arabian banking. International Journal of Computer and Communication Engineering. 2014;3(5):326-333.

[2] AdeoyeO. Evaluating the performance of Two-Factor authentication solution in the banking sector. International Journal of Computer Science. 2012;9(2):457- 62.

[3] Cryptomathic AS. Two factor authentication for banking. [Online]; 2012.
Available: http://www.cryptomathic.com

[4] Xie Qi. A new authenticated key agreement for session initiation protocol. International Journal of Communication Systems (IJCS). 2012;25(1):47-54.

[5] Malekzadeh Mina, Ghani Abdul, Azim Abdul, Subramaniam Shamala. A new security model to prevent denial-of-service attacks and violation of availability in wireless networks. International Journal of Communication Systems. 2012;25(7):903-925.

[6] Singh U, Pathak M, Malhotra R, Chauhan M. Secure communication protocol for ATM using TLS handshake. Journal of Engineering Research and Applications (IJERA). 2012;2(2):838-948.

[7] Stallings W. Cryptography and network security. (4th edn). Pearson Hall Education; 2010.

[8] Han S, Liu W, Chang E. Deniable Authentication protocol resisting Man-in-the-middle attack. International Journal of Computer, Information Science and Engineering. 2007;3(3):696-699.

[9] Duvey A, Goyal D, Hemrajani N. A Reliable ATM protocol and comparative analysis on various parameters with other ATM protocols. International Journal of Communication and Computer Technologies. 2013;1(6):192-197.

[10] Lavanya K, Raju C. A comparative study on ATM security with multimodal biometric system. International Journal of Computer Science and Engineering Technology (IJCSET). 2013;4(6)808-812.

[11] Chen Ruey-Maw, Hsieh Kuo-Ta. Effective allied network security system based on designed scheme with conditional legitimate probability against distributed network attacks and intrusions. International Journal of Communication Systems (IJCS). 2012;25(5):672-688.

[12] Marcos A. Simplicio Jr, Sakuragui Rony RM. Cryptanalysis of an efficient three-party password-based key exchange scheme. International Journal of Communication Systems (IJCS). 2012;25(11):1443-1449.

[13] AL-Saraireh J, AL-Saraireh M, AL-Saraireh S, AL-Nabhan M. Formal analysis of a novel mutual authentication and key agreement protocol. Journal of Computer Science and Technology. 2011;11(2):86-92.

[14] Dua G, Gautam N, Sharma D, Arora A. Replay attack prevention in Kerberos authentication protocol using triple password. International Journal of Computer Networks and Communications (IJCNC). 2013;5(2):59-70.

[15] Thilagavathi K, Rajeswari P. Efficiency and effectiveness analysis over ECC based direct and indirect authentication protocols: An extensive comparative study. ICTACT Journal on Communication Technology. 2012;3(1):515-524.

[16] Yang L, Yu P, Bailing W, Yun Q, Xuefeng B, Xinling Y, Zelong Y. Hash-based RFID mutual authentication protocol. International Journal of Security and Its Applications. 2013;7(3).

[17] Juan W, Hongxin H, Bo Z, Fei Y, Huanguo Z, Qianhong W. Formal analysis of information card federated identity-management protocol. Chinese Journal of Electronics. 2013;22(1).

[18] Amin A, Agooz S, Shehata A, Amer E. Design, verification and implementation of enhanced PKM WiMAX authentication protocol. International Journal of Computer Science and Telecommunications. 2013;4(3).

[19] Fan K, Li H, Wang Y. Security analysis of the kerberos protocol using BAN logic. Fifth International Conference on Information Assurance and Security, IAS '09. 2009;467-470.

[20] Georgoulas Stylianos, Moessner Klaus. Toward efficient protocol design through protocol profiling and performance assessment: Using formal verification in a different context. International Journal of Communication Systems (IJCS). 2012;25(11):1415-1431.

[21] Degefa F, Lee D, Kim J, Choi Y, Won D. Performance and security enhanced authentication and key agreement protocol for SAE/LTE network. Computer Networks. 2016;94:145-163.
ISSN 1389-1286

[22] Bellare M, Pointcheval D, Rogaway P. Authenticated Key Exchange Secure Against Dictionary Attacks. Advances in CryptologyEUROCRYPT 2000, Proc. Intl Conf. Theory and Application Cryptographic Techniques, LNCS 1807, Springer. 2000;139-155.

[23] Liang W, Wang W. A quantitative study of authentication and QoS in wireless IP networks. In: Proceeding IEEE INFOCOMS; 2005.

[24] Forsberg D, Horn G, Moeller W, Niemi V. LTE Security. John Wiley and Sons, United Kingdom; 2013.

[25] Feng Z, Ning J, Broustis I. Coping with packet replay attacks in wireless networks. 8th Annual IEEE Communications Society Conference on Sensor, Mesh and Ad Hoc Communications and Networks; 2011.

[26] Marcos A. Simplicio Jr, Sakuragui Rony RM. Cryptanalysis of an efficient three-party password-based key exchange scheme. International Journal of Communication Systems (IJCS). 2012;25(11):1443-1449.

[27] Al-fayoumi M, Nashwan S, Yousef S. A New Hybrid Approach of Symmetric/Asymmetric Authentication Protocol for Future Mobile Networks. In: 3rd IEEE International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob 2007). White Plains, New York, USA; 2007.

[28] Thakur T, Dogra S, Sood Y. Replay attack prevention by using a key with random number in kerberos authentication protocol. International Journal of Innovative Research in Science, Engineering and Technology. 2015;4(7).

[29] Pinkas B, Sander T. Securing Passwords Against Dictionary Attacks. Proc. 9th ACM Conf. Computer and Comm. Security, ACM Press. 2002;161-170.

[30] Kim I, Cho Y. Hash-Based password authentication protocol against phishing and pharming attacks. Journal of Information Science and Engineering. 2015;31:343-355.

Peer-review history:
The peer review history for this paper can be accessed here (Please copy paste the total link in your browser address bar)
http://sciencedomain.org/review-history/19003