Journal of Information Hiding and Multimedia Signal Processing ©2015 ISSN 2073-4212
Ubiquitous International Volume **6**, Number **4**, July **2015**

MAPMP: A Mutual Authentication Protocol for Mobile Payment

Eric Ke Wang[1], Zhenjie Cao[2],Tsu-Yang Wu[3], Chien-Ming Chen[3]

[1]Harbin Institute of Technology, Shenzhen Graduate School,
Shenzhen, China, wk_hit@hitsz.edu.cn
[2]International SchoolBeijing University of Posts and Telecommunications,
Beijing 102209, China, 470413717@qq.com
[3]Shenzhen Key Laboratory of Internet Information Collaboration, Shenzhen Graduate School,
Harbin Institute of Technology, Shenzhen, China
wutsuyang@gmail.com, chienming.taiwan@gmail.com

Received November, 2014; revised February, 2015

Abstract. *Mobile payment has been a key part of mobile commerce. However, security problems are still challenging mobile payment. Several security techniques have been developed and applied in order to tackle these problems. Most security measures only authenticate user side. They may improve the user security in some way, but are not able to defend against man-in-the-middle attacks. We propose a secure mobile payment with SMS-based mutual authentication protocol to enable the payment server and the user to authenticate each other. Further, we analyze and prove that our scheme with the security protocol is able to defend man-in-the-mobile attacks and other attacks.*
Keywords: Communicating sequential processes; Short message services; Mutual authentication; Man-in-the-middle attacks;

1. **Introduction.** Mobile-commerce (M-commerce), which is considered the next generation e-commerce, can be defined as any electronic transaction or interaction conducted using a mobile device such as a mobile phone or personal digital devices(Hu, 2006). M-commerce has been used for a variety of products and services ranging from basic applications such as mobile marketing to high security mobile payment applications. One of key applications of M-commerce is Mobile payment which is now becoming a widely used medium for carrying out financial transactions. Researchers estimate that the mobile payment market will yield a profit of 20 billion Euros by 2015(Goyal, 2012). However, the security issues that arise with the growth in this field began to be concerned recently since more and more security problems occurs (Goth, 2012; Goyal, 2012). A mobile payment application must provide best means for carrying out secure authentication and financial transactions. But it is a difficult trade-off when security and convenience are considered at the same time. How to balance both in the mobile payment system has been a practical research problem. The major problem is that most existing secure protocols are too complicated or cost too much to use for common users. Commonly the users are expecting a convenient payment with enough safety. In this paper, we proposed a convenient way Mutual Authentication for Mobile Payment which shows that using a platform independent authentication method (SMS based) is adequate without compromising the security of the authentication solution.

2. **Related Works.** Some researchers have paid effort in the area of security measures for mobile payments. Some research work (Aloul, 2009; Ying, 2009; Thanh, 2009) discussed about the different techniques that can be used to build a secure authentication method for mobile applications. These techniques include two-factor, single sign-on, Some researchers have paid effort in the area of security measures for mobile payments. Some research work (Aloul, 2009; Ying, 2009; Thanh, 2009) discussed about the different techniques that can be used to build a secure authentication method for mobile applications. These techniques include two-factor, single sign-on, strong and social authentication. However, most research has been focusing on platform (operating systems e.g. iPhone OS, Android etc.) dependent authentication solutions, while less attention have been paid on platform independent solutions. Besides, in order to enhance the safety of financial transaction, cryptography schemes were employed such as ECC-based Wireless Local Payment Scheme (Strangio, 2005), it presented a local payment scheme via mobile phone based on public key infrastructure. This does provide a solution for making transactions via mobile phones; however, the solution is platform dependent and the computing cost for mobile devices is much higher than common apps. Actually, although the secure protocols for electronic payment have been studied a lot, most protocols have not been used in the market. The major problem is that most secure protocols are too complicated or cost too much to use for common users. With our work, we proposed a convenient way which shows that using a platform independent authentication method (SMS based) is adequate without compromising the security of the authentication solution. Short Message Service (SMS), as being familiar and convenient for users, has recently become a popular approach for complementing authentication methods (Tiwari, 2007; Choi, 2012). Nowadays, some researchers have been attempting to develop authentication systems based on SMS and some of them have been used particularly in financial systems (Chong, 2006). One case is that, a Push Pull services offering SMS (Short Messaging Service) based m-Banking system (Mousumi, 2010) is able to provide several essential banking services only by sending short messages to bank server from any remote location. However, most of the SMS based authentication systems for mobile payment are for one way authentication, primarily for the authentication of the user side. A common scenario is that, before performing a transaction requested by a user, the bank concerned sends an SMS confirmation message to the user, requiring a PIN code of the users credit card. If the user sends back an incorrect response, the transaction would not be processed and the merchant would be notified. A one-time password could be generated by the Bank Secure Access Gateway to be distributed to the users mobile phone as a flash SMS. Then the user can input the one-time password online to confirm the transaction. The one-time password expires once it has been used or its scheduled lifecycle has expired. Since most current SMS based authentication systems only involve the authentication of the user, they could easily be attacked by Man-in-the-middle attack (Salam, 2013). Attacks arise because users are unable to trace the transaction process and cannot authenticate who in the other side they are communicating with. Thus, how to design a secure mutual authentication protocol which is able to defend against both kinds of attacks has become a hot topic.

3. **Mutual Authentication Protocol.** We propose a new practical, user-friendly and secure mobile payment (SMP) based on SMS Mutual Authentication Protocol for online transaction authentication which is able to defend against multiple kind of attacks, and realize the mutual authentication by simple SMS scheme. The scheme is based on an assumption that the hackers are not able to capture Flash SMS (Iosif I. Androulidakis, 2012) from the mobile payment SMS center to the users. It involves the following two steps:

3.1. **Register step.** Users submit a table including some answers to corresponding questions securely to the mobile payment server when they register in the payment systems. The secure way could be offline submission. The questions could be something like Who is your father, Who do you admire, When did you graduate which are given by table 1.

Table 1. Users'Q/A

Questions	**Answers**
Who is my father?	Answer1
Who do I admire?	Answer2
When did I graduate?	Answer2
.	..

3.2. **The process of the payment.** [Figure 1.]
1. A user initializes one transaction process, such as transferring $1000 to a mobile commerce company account. The initialization process includes three steps:
- Login into the payment system with correct username and password, request a payment.
- Present the questions choices which were submitted when the user registered before.
- User picks one question or several questions from current transaction page.
2. The mobile payment gateway processes in three parts:
- Generates a one-time PIN code for this transaction;
- Retrieve the questions answers for the users chosen questions;
- Retrieve information of the transaction, such as account number and the amount of involved money. After that, payment system sends the three parts of information to SMS center. The message format could be set as [Question Answer][Transaction Key Information][One Time PIN Code].
3. The SMS center sends out the packed message including the above information as Flash SMS.
4. The user inputs the one-time PIN code online to confirm this transaction after he/she verifies the answer and the payment information of the received Flash SMS.
5. Once receiving the transaction confirmation, the mobile payment system starts to process the transaction.
6. After finishing the transaction, the SMS center sends out a notification of completing transaction to the user. Note: [Transaction Information] can be described as subject->acting->object, for example, *Eric is going to transfer $3000 to the some company account*

3.3. **One time PIN code generation.** The involved one time PIN code (OTP) generation algorithm is based on an increasing time value function and a static symmetric key known only to the server. In order to create the OTP value, a HMAC- SHA1 algorithm(Krawczyk, 1997) is adopted. Since the output of the HMAC-SHA1 calculation is 160 bits, we need to truncate this value to a smaller digit so that it can be easily entered.

$OTP(Key,\{Username,CurrentTime\}) = Truncate\ (HMAC\text{-}SHA\text{-}1(Key,\{Username,\ CurrentTime\}))$

where *Truncate* converts the value generated through *HMAC-SHA1*to an *OTP* value.

Generation of *OTP* Value

The algorithm can be described in 2 steps shown in figure 2:

Step 1: Generate the value Let $HSM = HMAC\text{-}SHA\text{-}1(Key,\{Username,\ CurrentTime\})$ where *HSM* is a 20-byte string

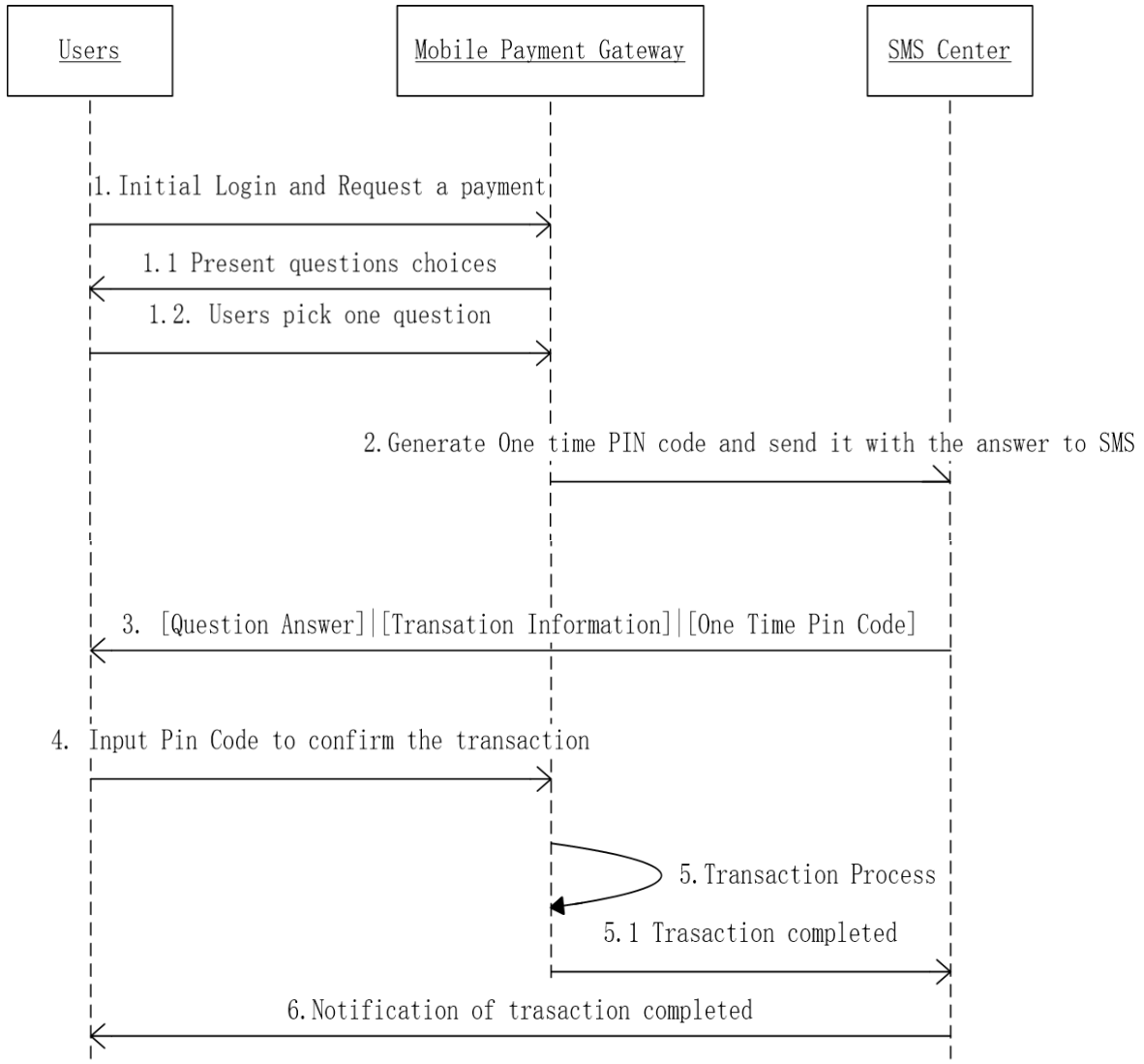

FIGURE 1. Process of the protocol

Step 2: Extract the 8-digit OTP value from the string
OTP = Truncate (HSM)
The Truncate function in Step 2 does the dynamic truncation and reduces the *OTP* to 8-digit.

3.4. **Flash SMS.** In this scheme, we adopt Flash SMS to provide short message service. Flash SMS is an SMS which is displayed on the phone screen immediately upon arrival. Most of SMS providers can provide Flash SMS. The main aim of this is to eliminate the possibility of storing retrieving the SMS from the inbox of the mobile phone. This makes it impossible for spyware (which have the capabilities of stealing stored SMS) to retrieve the sensitive OTP.

4. **Implementation.** Based on the design described above, we have implemented a prototype.

The prototype is implemented as a solution for an m-commerce online application/store that needs to execute mutual authentication between buyers and payment systems when they need make purchases. The prototype is based on client-server architecture with a very slim client. It was implemented in ASP.NET and targeted at .NET framework 4.

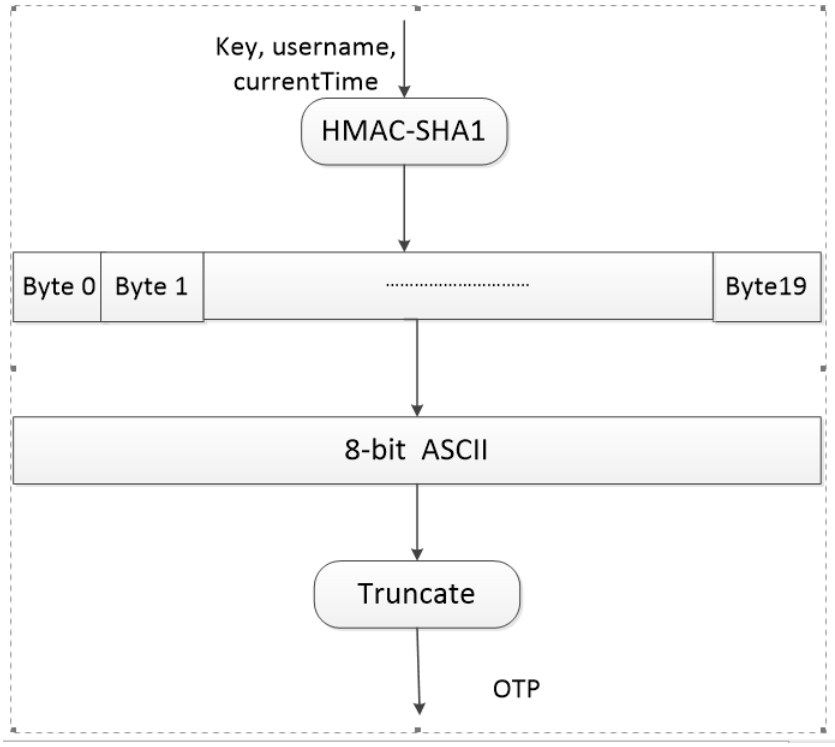

FIGURE 2. One time PIN code generation

We uses a SMS gateway called GSM Modem with a SIM card inside for sending one time passwords(OTP) to buyers mobile phones. The mobile commerce application prototype has been implemented on the Windows 2012 Server, with CPU Intel© Core 2 CPU @3.5GHZ, RAM 4G.

Besides, in order to implement Flash SMS, the message should be class 0, thus these messages appear on the screen immediately upon arrival, without the need to press any buttons on the phone. If the data coding scheme is set to 16-bit unicode, and the message starts with "0001", it will appear as a blinking flash message (most kind of cellphones obey the rules). The maximum length of such a message will then be 69 unicode characters.

The figure 3 presents a live run of our solution prototype implementation. The scenario is a mobile commerce provider who sells electronics such as laptops, cameras etc. The user firstly makes an order and then goes to payment page. The payment system authenticates the buyer by requesting for is username and password. On receipt of a valid username and password, the system returns the questions which submitted by the user when he registered. The user can pick one question and the system generates an OTP with the question answer and sends them to the registered buyers phone by short message service. The user verifies the answer and enters the OTP into the application and is granted access to input the credit card information after successful verification of the OTP. After that, the payment system completes the transaction and returns confirmation. At the same time SMS center sends a short message to notify users again. The prototype has been tested on an IOS and an Android OS.

5. **Security analysis.** Our protocol can effectively defeat against multiple attacks such as eavesdropping, replay and XSS attacks. Besides, it can also defeat against Man-in-the-mobile attacks.

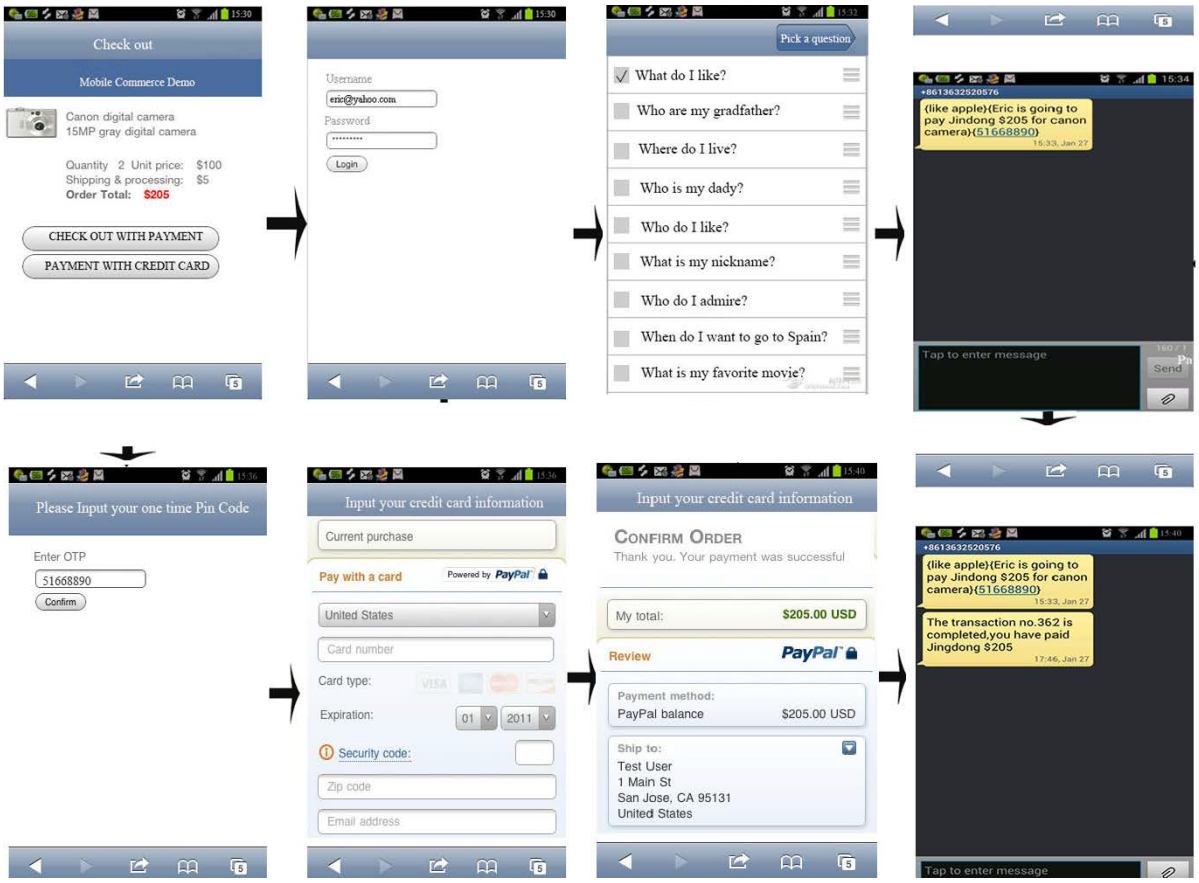

FIGURE 3. Prototype implementation

5.1. **Eavesdropping Attack.** A pre-installed eavesdropping spyware can steal usernames and passwords via key loggers. If this is allowed to happen, then the security of the SMP method which depends on the secrecy of passwords and OTPs is at risk. However, the SMP method was designed with preventive measures which eliminate the possibility of this to occur. In our scheme, we adopt Flash SMS to deliver OTP which are not stored in the message boxes where Spyware can retrieve

5.2. **Replay Attacks.** This attack mainly targets to intercept data between two parties and maliciously use the data later. Interception can happen either in real-time during active communication between the involved parties, or by obtaining communicated data later from any of the concerned parties. Several known techniques are used for defend replay attacks. One such approach is the use of OTP which is a key feature of the SMP authentication method. During the process of authentication with the SMP, an OTP is sent from the m-commerce site to the customers mobile phone. The customer then authenticates himself by sending the OTP back to the m-commerce site. The interception of the OTP by an adversary to be used later in a replay attack will be unsuccessful since an OTP is only valid once and also only for a short period of time.

5.3. **Cross-site scripting attacks.** A cross-site scripting attack can be used to insert malicious scripts or commands into m-commerce applications in order to steal user data. In the case of the SMP authentication method, the security of the method depends on the inability of an adversary to compromise authentication data (username, password, OTP). Thus, it is required that cross-site scripting mitigating techniques should be implemented in any m-commerce applications that use the SMP authentication method. However

the SMP method is by itself secure against cross-site scripting attacks using OTP. For example, as shown in Figure 4, even if an adversary is successful in compromising an m-commerce site and is able to steal a legitimate username and password, as illustrated in the figure below, he will still not be able to be authenticated using the stolen credentials. This is assured based on the two-factor authentication employed by the SMP method. The adversary cannot log in since he is not in possession of the generated OTP and the legitimate user will find out that his account is compromised when he receives the SMS.

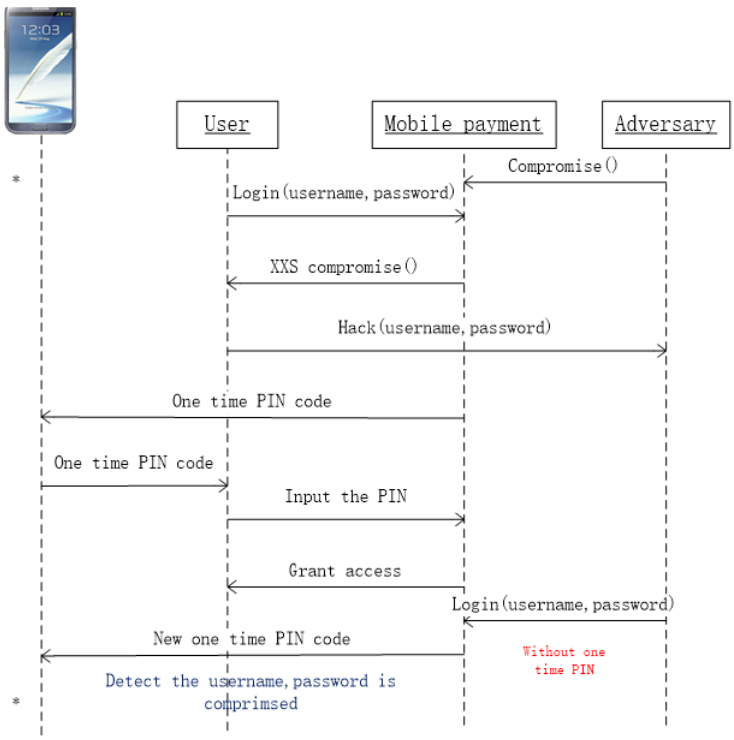

FIGURE 4. Sequence of cross-site attack

5.4. **Man in the mobile attack.** Man-in-the-mobile (MITB), a form of mobile threat related to man-in-the-middle (MITM), is a proxy Trojan horse that infects a mobile phone by taking advantage of vulnerabilities in activity security to modify mobile app, modify transaction content or insert additional transactions, all in a completely covert fashion invisible to both the user and host application. The attack is a new class of attack vectors that have started to emerge as the advancement of mobile phones as computing devices has led to the possibility of malware being maliciously loaded onto them. The malware can spy on SMS OTPs by retrieving SMS box and relay them back to the hackers.

In our scheme, we adopt Flash SMS to deliver OTPs which are not stored in SMS box in SIM card. Malware in the mobile phone cannot retrieve Flash SMS. In order to prove the protocol to be against man in the mobile attack, we formally prove the security by Communicating Sequential Processes.

- **Introduction to CSP**

Communicating Sequential Processes (CSP) is a formal language for describing patterns of interaction in concurrent systems (Arpit, 2012) . It is a member of the family of mathematical theories of concurrency which is known as process algebras or process calculi. CSP is influential in the development of the occam programming language. CSP was first described by C. A. R. Hoare in 1978, and has evolved substantially since then. It

has been used as a tool in practice for specifying and verifying the concurrent aspects of different systems. CSP has been shown to be particularly successful in analyzing protocols. Several works make use of CSP to analyze security properties, such as confidentiality and authentication, etc. The most famous approach is based on the CSP model checker FDR. A small system running the protocol is modeled as a CSP process; the most general intruder who can interact with the protocol is also modeled as a CSP process. FDR is then used to test whether the resulting system satisfies various properties such as ensures secrecy or achieves authentication. If it does not, FDR returns a trace of the system that causes the desired properties to fail: this trace corresponds to an attack in the protocol.

- **Formal analysis of SMP**

1. Create the finite state model
The mainly involved parties are listed as follows:
I. Initiator A(User)
II. Responder B(Mobile Payment)
III. Attacker H(Hacker)
The set of actors are defined as:
Initiators: $\{A, H\}$
Responders:$\{B, H\}$
Initial Temp Nonce:$\{N_B\}$
Nonce received from SMS center:$\{N'_B\}$
Initial Submitted Answers:$\{An_B\}$
Answers received from SMS center:$\{A'n_B\}$
Temp Questions:Q1
Original Key Transaction Information :$\{T_1\}$
Key Transaction Information received from SMS center:$\{T'_1.\}$

2. Define the communication channels
(1) Comm: The normal channel of main parties
(2) Fake: The channel in which the attacker fakes the messages
(3) Intercept: The channel in which the attacker intercepts messages
(4) I_running.a.b : Initiator A believes that he is talking to the responder B.
(5) R_running.a.b: Responder B believes that he is talking to the initiator A
(6) I_commit.a.b: Initiator A believes that he has finished the conversation with responder B
(7) R_commit.a.b: Responder B believes that he has finished the conversation with initiator A
$A \rightarrow B : \{AT_1Q_1\}$
$B \rightarrow A : \{BN_BAn_BT_1\}$
$A \rightarrow B : \{N_B\}$
$MSG1 = \{Msg1.A.B.A.T_1.Q_1\}$
$MSG2 = \{Msg2.B.A.B.N_B.An_B.T_1\}$
$MSG3 = \{Msg3.A.B.N_B\}$
$INITIATOR(A, T_1, Q_1) \cong userA.B \rightarrow I\_running.A.B \rightarrow$
$comm.Msg1.A.B.A.T_1.Q_1 \rightarrow Comm.Msg2.B.A.\ B.\ N_B.An'_B.T'_1 \rightarrow If\ An'_B = An_B\ and\ T'_1 = T_1\ then\ comm.\ Msg3.A.B.\ N_B \rightarrow I\_commit.A.B \rightarrow Skip$
$Else$
$Stop$
where

$An'_B \in TempAnswers$
$N_B \in TempNonce$
$T_1 \in TempQuestions$
$RESPONDER(N_B, An_B) \cong$

$$\cong R_running.A.B \rightarrow \left\{ \begin{array}{l} Comm.Msg1.A.B.A.\ T_1.Q_1 \rightarrow \\ Comm.Msg2.B.A.\ B.\ N_B.An'_B.T_1 \rightarrow \\ Comm.\ Msg3.A.B.\ N'_B \rightarrow \\ If N'_B = N_B\ then \\ R\_commit.A.B \rightarrow Skip \\ Else \\ Stop \end{array} \right\}$$

where
$A'n_B \in TempAnswers$
$N_B \in TempNonce$
$T_1 \in TempQuestions$

In order to simulate the behavior of an attacker, we assume that, for the Initiator A, MSG1 and MSG3 can be intercepted and faked; for the responder B, MSG1 and MSG3 can be faked. MSG2 cannot be intercepted. (According to the assumption, the Flash SMS cannot be captured by the hackers)

$$H(M1, M2, M3, ns, qs, ts) \cong$$
$$\left\{ \begin{array}{l} intercept.Msg1.A.B.A.\ T_1.Q_1 \rightarrow H(M1, M2, M3, ts\ U\ \{T_1\}, qs\ U\ \{Q_1\}, ns) \\ intercept.Msg2.B.A.B.N_B.An_B.T_1 \rightarrow H(M1, M2U\ \{B.N_B.An_B.T_1\}, M3, ts, qs, ns) \\ intercept.Msg3.A.B.\ N_B \rightarrow H(M1, M2, M3, ts, qs, ns\{N_B\}) \\ fake.Msg1.A.B.\ A.\ T_2 : ts.Q_1 : qs \rightarrow H(M1, M2, M3, ns, qs, ts) \\ fake.\ Msg3.A.B.\ M : M3 \rightarrow H(M1, M2, M3, ns, qs, ts) \end{array} \right\}$$

where
$A \in Initiator$
$B \in Responder$
$A'n_B \in TempAnswers$
$N_B \in TempNonce$
$T_1 \in TempQuestions.$
From the CSP description above, we can get the traces from FDR:
$User.A.H.\ ,\ I\_running.A.H,\ comm.Msg1.A.H.\ A.\ T_1.Q_1,\ fake.Msg1.A.B.A.T_1 : ts\ Q_1 : qs, Comm.Msg2.B.A.\ B.\ N_B.An_BT_2,\ stop.$
According to the description above, we can find out that SMP can effectively stop the protocol when attackers try to launch Man-in-the-middle attacks.

- **Discussion**

Most existing online transaction authentication protocols based on SMS are one side authentication, inwhich the server authenticates user by sending one SMS including one-time random code and push user to type it. If the user inputs the correct one-time code, the transaction can be processed. However, the biggest problem of those existing protocols is that they cannot defend Man-in-the-middle attacks. However, SMP successfully realizes mutual authentication with SMS. Thus, it can effectively defend Man-in-the-middle attacks.

6. **Conclusion.** In this paper, we propose a practical, user-friendly and secure mobile payment scheme with mutual authentication protocol based on SMS for mobile transaction applications. And we implement a prototype which is platform-independent payment

TABLE 2. Defending capabilities

Attacks	Mitigation	MAPMP	Mousumi 2010	Salam 2013
Cross-sites attacks	Filtering, Escaping	√	√	√
Eavesdropping	Scanning, Encryption	√	√	√
Replay	OTP,Time Stamping,MAC, Session Token	√	√	√
Man-in-the-mobile attack	Mutual authentication with OTP	√	*	*

approach for m-commerce applications. The security analysis has shown that it is able to defend against multiple kinds of attacks. The major contribution of this paper is that we formally prove that the proposed scheme can defend against man-in-the-mobile attacks. One additional advantage of the scheme is that it can easily be understood and used by the user.

Acknowledgment. This research was supported by National Natural Science Foundation of China (No.61100192), Research Fund for the Doctoral Program of Higher Education of China(No.20112302120074), and was partially supported by Shenzhen Strategic Emerging Industry Development Foundation (No.JCYJ20120613151032592), National Key Technology R&D Program of MOST China under Grant No. 2012BAK17B08. The authors thank the reviewers for their comments.

REFERENCES

[1] F. Aloul, S. Zahidi and W. El-Hajj, Two factor authentication in mobile devices, *IEEE/ACS International conference on Computer Systems and Applications*, Rabat, Morocco, pp. 641-644, 2009.

[2] I. I. Androulidakis, SMS Security Issues, Mobile Phone Security and Forensics-SpringerBriefs in Electrical and Computer Engineering, pp. 63-74, 2012.

[3] A. B. Shafie, W. F. B. W. Ahmad, An introduction on extensions of process algebra: Concurrent and communicating systems, *International Conference on Computer & Information Science*, Shanghai, China, 2012.
A. B. Shafie, and W. F. Binti Wan Ahmad, An introduction on extensions of process algebra: Concurrent and communicating systems, *Computer & Information Science (ICCIS)*, 2012 International Conference on, vol. 2, pp. 857-862. IEEE, 2012.

[4] S. S. A. Tiwari, A. Abraham, S. J. Knapskog and S. Sanyal, 2007. A Multi-Factor Security Protocol for Wireless Payment - Secure Web Authentication using Mobile Devices, *IADIS International Conference on Applied Computing Proceedings of the IADIS International Conference on Applied Computing*, Salamanca, Spain.

[5] M. K. Chong, Security of Mobile Banking: Secure SMS Banking, *Data Network Architectures Group*, University of Cape Town, South Africa, 2006.

[6] D. V. Thanh, J. I. Jonvik, T. and Do van Thuan, 2009. Strong authentication with mobile phone as security token, 6th IEEE International conference on Mobile Adhoc and Sensors Systems, pp. 777-782. I. Jrstad, and T. Jonvik. Strong authentication with mobile phone as security token, Mobile Adhoc and Sensor Systems, *MASS'09. IEEE 6th International Conference*, pp. 777-782. IEEE, 2009.

[7] G. Goth, Mobile Security Issues Come to the Forefront, *IEEE Internet Computing 16*, pp.7-9, 2012.

[8] F. M. S. Jamil, Push Pull Services Offering SMS Based m-Banking System in Context of Bangladesh, International Arab Journal of e-Technology 1, 79 - 88, 2010.

[9] J. C. H. Kimy, A Novel Approach for SMS security, *International Journal of Security and Its Applications 6*, 2012.

[10] G. M. S. EC-PAY- An Efficient and Secure ECCbased Wireless Local Payment Scheme, *Third International Conference on Information Technology and Applications*, pp. 442 - 447, 2005.

[11] Z. Y. Z. H. N. Ying, The study of multi-level authentication based single sign-on system, *2nd IEEE international conference on Broadband Network & Multimedia Technology*, Beijing, China, pp. 448 - 452, 2009.

[12] M. A. Salam, Detect ability of Man-in-the-Middle Attacker in Mobile Sensor Networks, *International Journal of Advanced Computer Science 3*, 2013.

[13] B. M. Soleymani, Social Authentication Protocol for Mobile Phones, *International Conference on Computer Science and Engineering*, Canada, pp. 436 -441, 2009.

[14] H. Krawczyk, R. Canetti, and M. Bellare, HMACKeyedHashing for Message Authentication[M], *Interuet Engineering Task ForceRequest for Comments(RFC)*, 1997

[15] V. Goyal, U. S. Pandey, and S. Batra, Mobile Banking in India: Practices, Challenges and Security Issues, *International Journal of Advanced Trends in Computer Science and Engineering 1*, pp. 56 - 66, 2012.

[16] W. C. Hu, J. H. Yeh, H. J. Yang, and C. W. Lee, Mobile handheld devices for mobile commerce, Encyclopedia of E-Commerce, E-Government and Mobile Commerce, pp. 792-798, 2006.