SECURITY ANALYSIS OF AUTHENTICATION SCHEMES IN M-COMMERCE BASED ON FUZZY COMPREHENSIVE EVALUATION*

Rui Hua, Runtong Zhang and Dandan Li
Institute of Information Systems, Beijing Jiaotong University, Beijing 100044, China

Keywords: Identity authentication, M-commerce, Fuzzy comprehensive evaluation, Security analysis.

Abstract: The openness and transformation mode of the mobile network poses a serious problem of information security in mobile commerce applications, and identity authentication is one of the main methods to solve the problem. Along with the development of mobile commerce, considerable attentions on various identity authentication schemes have been paid. However, there is still lack of a systematic and practical evaluation system to evaluate these schemes. In this paper, an indicators analysis system of mobile commerce by using the fuzzy inference approach is proposed to evaluate different mobile commerce identity authentication schemes. Comprehensive simulation and comparsion show that the proposed indicator analysis systesm is quantified and efficient.

1 INTRODUCTION

M-commerce activities depend on wireless Internet and mobile terminal. Based on characteristics of wireless network, security of mobile commerce platform has become the key problem (Minglei S, 2009). Features such as small storage, low computational power supply and limited battery of mobile terminal increase the difficulty to solve the security problem of mobile platform (Kwok-Yan L, 2003). Limited to wireless networks and characteristics of mobile terminal, developed security system in traditional electronic commerce cannot be directly applied in mobile business, which brings mobile commerce a lot of dangers. Security is a primary issue in the development of mobile commerce, and identity authentication is the core of entire security problem (Neuman B and Ts'T, 1994). Identity authentication is the use of one or more mechanisms to prove that you are who you claim to be (Aloul F, 2009). In the absence of user identity authentication, confidentiality and integrity of user's information is of no significance. Currently, some researchers have improved some traditional identity authentication models for mobile environment (Oh HG, 2009 ; Soleymani B, 2009 and Xuefei C, 2009). These models use different key agreement method and encryption algorithm, and each of them have different emphases and defects. But there are only a few of methods to evaluate these models security, such as formal analysis method and simple comparison. The lack of a complete and effective security evaluation system makes the security performance of existing models cannot be comprehensive evaluated objectively. It becomes more difficult for researchers and users to choose authentication models.

According to characteristics of mobile terminal and wireless network, we establish a scientific and reasonable security analysis system based on mobile commerce environment. The fuzzy comprehensive evaluation method is used for modeling. To meet the demand of comparing different models' security, the quantitative and qualitative analysis method will be used to evaluate identity authentication models.

2 A BRIEF REVIEW

There are two mainly methods to evaluate the

* This work is partially supported by the Fundamental Research Funds for the Central Universities (with contract number 2009YJS034) and the Special Funds of Beijing Jiaotong Universities (with contract number 2009JBZ011)

Hua R., Zhang R. and Li D.
SECURITY ANALYSIS OF AUTHENTICATION SCHEMES IN M-COMMERCE BASED ON FUZZY COMPREHENSIVE EVALUATION.
DOI: 10.5220/0003268402450251
In *Proceedings of the Twelfth International Conference on Informatics and Semiotics in Organisations (ICISO 2010)*, page
ISBN: 978-989-8425-26-3

security of identity authentication models. One is formal security analysis; another one is building security evaluation system.

Formal security analysis is a kind of methods based on Dolev-Yao model (Hai-yan Q, 2008). This model hypothesizes encryption is "perfect", and attacker can intercept any text. Formal security analysis includes strand spacer method (Javier T, 1999), BAN method (Burrows M, 1990) and inductive approach method (Lawrence, 1998). These methods can prove whether the identity authentication scheme is security in ideal condition. But actual application environments of the identity authentication are not in ideal condition, so these methods can prove the security of identity authentication schemes only theoretically.

Identity authentication evaluation system can be divided into evaluation systems for similar models which have same authentication factor (such as having the same authentication encryption algorithm or having the same authentication technology, etc.) and evaluation systems for new models.

Identity authentication evaluation systems for similar models comprehensively compare models' security and performance in particular network environment. Wei Liang (2005) and other researchers divide analysis indictors into security indictors and quality of service (QoS) indictors. Based on the identity authentication data encryption, data integrity, privacy protection and non-repudiation, challenges / response models are divided into four security index. By using the method above, although boundaries clear to divide and easy to operate, it cannot effectively compare highly similarity identity authentication models. Charlott E and other researchers propose identity authentication evaluation system based on mobile platform IP Multimedia Subsystem (IMS). The system includes three basic parts: security, user-friendly and simplicity and researchers point out that three basic parts are interdependent. SWOT analysis method, user ranking method and simulation are used to compare different models (Charlott E, 2009). Although this paper put forward a complete and meticulous evaluation system, it does not give a clear solution about how to use the system to evaluation identity authentication models. Patroklos G.A. (2004) and other three researchers compare three security protocols (SSL, S/MINE and IPSec) which are widely used in normal network according to length of the key and time cost of mutual authentication execution. The research closes to reality application, but does not fit every model.

Evaluation systems for new models are established to compare new models with similar models, in order to indicate advantages of the new one. Researcher Vipul Gupta (2002) proposes a new SSL protocol based on ECC, and compares the performance between the new protocol and SSL protocol based on RSA. Yong-bin Zhou (2009) and other researchers improve MAKAP protocol and prove the security of the improved protocol as well as compare the improved protocol with the old one on calculate cost, communication cost and storage cost. Zhi-qiang Xie (2009) and other researchers propose new S/KEY authentication scheme and compare the improved protocol with the old one on mid-man-attack, decimal attack, secret key security and so on. This kind of research focus on discussing the model about it's resistance to attack and unfit for evaluation and comparison with other types of authentication schemes. Most of this researches limited in theoretical analysis and have no quantitative evaluation results.

3 THE M-COMMERCE SECURITY INDICATORS EVALUATION SYSTEM

The evaluation system is established to meet mobile commerce identity authentication schemes' characteristics, which can reflect the characteristics of mobile commerce properties and the effect of the identity authentication.

Characteristics of mobile commerce mainly embodies in three aspects: network environment, terminal characteristics and service features. Small bandwidth, high BER (bit error ratio) and the opening of interface make mobile communication network in numerous threats and these threats may lead to different kinds of attacks. Mobile terminal equipment has low storage capacity, battery power specialty and its high secrecy request makes the security of user information becoming more important. At the same time, mobile commerce customers generally require information immediately, which means the immediacy of the service. Evaluation system should be able to reflect the characteristics of mobile commerce and make mobile commerce identity authentication different from identity authentication applications in common net work environment.

Security is the most important part of identity authentication effect. Researcher Mangipudi Kumar V.K.N. (2005) proposes identity authentication design framework based on the wireless network,

Table 1: M-commerce authentication security evaluation indicators system.

Target Level	First level index	Second level index
Security Analysis	Authentication function U_1	Mutual authentication U_{11}
		Anonymity U_{12}
		Non-repudiation U_{13}
		Integrity U_{14}
		Key agreement U_{15}
		Multi-factor authentication U_{16}
	Encryption intensity U_2	Theoretically decoding year U_{21}
		Freshness of secret key U_{22}
		Type of cryptograph U_{23}
	Resistance of attack U_3	Type of cannot-resistance-attack U_{31}
		Serious degree of cannot-resistance-attack U_{32}

and security is one of the most important factors, which include security service and security requirements. Security requirements indexes are mainly about network attack, which must be satisfied in identity authentication design. And security services indexes, including mutual authentication, non-repudiation etc, are optional functions in identity authentication design.

To build a useable security evaluation system should considerate a lot of factors. The evaluation system can exert its effect only if the system is established scientific and reasonable and each index should reflect the evaluation objects. To establish a set of perfect, rational and scientific identity authentication model evaluation indicator system, should follow the scientific, comprehensive, feasibility and comparability principles. Indexes' selection should cover all security requirements of mobile commerce identity authentication. Besides, indexes' selection should avoid index correlate with others at the same time, in order to keep eventually evaluation result in a high quality. Otherwise, identity authentication technology is an actual operation process, so the evaluation index should be convenient to get information and possible to quantify information. This paper establishes mobile commerce authentication security evaluation indicators system shown in Table 1.

According to the traditional electronic commerce security problems and mobile commerce's characteristics, mobile commerce security should include mobile terminal security (Youqing G, 2005), wireless network security, mutual authentication and non-repudiation (Jiayuan L, 2006) four requirements. According to the above requirements, evaluation system is determined in Table 1. Authentication function is an index set to assess schemes' security function, so indexes cannot be quantitative evaluated. So a modeling method is introduced to quantization the evaluation result.

4 MODELING BASED ON FUZZY COMPREHENSIVE EVALUATION

Fuzzy comprehensive evaluation method is an important branch of the theory of fuzzy mathematics. It has been widely used in economics, management, environment, education and other fields. With the social, economic development and complexity of issues people consider, uncertainty and ambiguity of the human mind has been strengthening, which makes it very difficult for us to make an objective evaluation. Fuzzy comprehensive evaluation method as a solution of the problem is receiving more and more attentions (Zeshui X, 2001).

Authentication technology is a very complex issue. Variety of factors can impact the effect of authentication and their impact on the way and size are both different and vague. Fuzzy comprehensive evaluation method is more objective on reflection the ambiguity of the role of these effects and thus is more scientific and feasible. Specific steps are as follows:

The first step, determine the factor set U.

The factor set is divided into the target level U, the first level evaluation factors Ui and the second-level evaluation factors Uim.

$$U = (U_1, U_2, U_3 \ldots U_i)$$

$$U_i = (U_{i1}, U_{i2}, U_{i3} \ldots U_{im})$$

$$i, m, n > 0$$

Table 2: M-commerce authentication security evaluation criterion.

Target level	First level index	Second level index	Possible result	Optimal result
Security analysis	Authentication function U_1	Mutual authentication U_{11}	Yes/No	Yes
		Anonymity U_{12}	Yes/No	Yes
		Non-repudiation U_{13}	Yes/No	Yes
		Integrity U_{14}	Yes/No	Yes
		Key agreement U_{15}	Yes/No	Yes
		Multi-factor authentication U_{16}	Yes/No	Yes
	Encryption intensity U_2	Theoretically decoding year U_{21}	0- ∞	∞
		Freshness of secret key U_{22}	Fresh/not fresh	Fresh
		Type of cryptograph U_{23}	0- ∞	∞
	Resistance of attack U_3	Type of cannot-resistance-attack U_{31}	0- ∞	0
		Serious degree of cannot-resistance-attack U_{32}	Serious/not serious	Not serious

Determined three-level fuzzy comprehensive evaluation criteria are shown in Table 2.

The second step, determine the reviews set V. By reference to fuzzy comprehensive evaluation method application examples in other areas, this paper reviews set $V = \{V_1, V_2, V_3 ... V_n\}$ as $V =$ (Excellent, Good, General, Poor, Terrible). The optimal result or the compared optimal result will be the criterion of mark. Indexes which can not be quantitative evaluated will be marked according to the number of possible values and five levels as shown in Table 3.

Table 3: Evaluation set description.

Evaluation level	Reference Note
Excellent V_1	Fully in line with index for evaluation criteria
Good V_2	In line with the vast majority of index, criteria, only the individual projects failed to meet the index
General V_3	Basically in line with targets, criteria, does not meet the requirements of the less
Poor V_4	Basically does not meet the targets, criteria, does not meet the requirements of the more
Terrible V_5	The vast majority of judges do not meet targets, and only be able to meet the requirements of individual projects

The third step, determine the evaluation factors known to the weight vector W . Weight vector, which relative with factors set, is used to display the weight of each factor's value. Weight vector can be divided into three levels according to factor set. All levels of the weight vector can be expressed as

$$W = (w_1, w_2, w_3 ... w_i)$$

$$w_i \geq 0, \sum w_i = 1$$

For the establishment of mobile commerce authentication evaluation system, expert scoring method is used to get the initial data. We invite 10 experts for this research. Each questionnaire has been filled independently. Table 4 shows 10 experts' scoring statistics result of factors' weight.

The fourth step, determine fuzzy relationship matrix R. According to the scoring result of 3rd level factors of 10 experts, fuzzy relationship matrix R_{im} will be calculated as follows.

$$R_{im} = (\frac{k_1}{10}, \frac{k_2}{10}, \frac{k_3}{10}, \frac{k_4}{10}, \frac{k_5}{10})$$

$$= (r_{im1}, r_{im2}, r_{im3}, r_{im4}, r_{im5})$$

Using the same method, a particular mobile commerce authentication model's final fuzzy relationship matrix can be obtained.

The fifth step, determine fuzzy transformation method. Obtained the results of comprehensive evaluation through calculate $W \circ R$.

$$\begin{aligned} B &= W \circ R \\ &= (w_1, w_2, w_3 ... w_m) \circ \begin{pmatrix} r_{11} & r_{12} & r_{13} & r_{14} & r_{15} \\ r_{21} & r_{22} & r_{23} & r_{24} & r_{25} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ r_{m1} & r_{m2} & r_{m3} & r_{m4} & r_{m5} \end{pmatrix} \\ &= (b_1, b_2, b_3, ..., b_m) \end{aligned} \tag{1}$$

The sixth step, calculate the final evaluation result.

$$T = B \circ C = \sum_{x=1}^{5} b_x \bullet c_x \tag{2}$$

Table 4: Evaluation index weight result.

Target level	First level index	Score/ Weight	Second level index	Score/Weight
Security analysis	Authentication function U_1	19 (0.32)	Mutual authentication U_{11}	53 (0.26)
			Anonymity U_{12}	32 (0.15)
			Non-repudiation U_{13}	35 (0.17)
			Integrity U_{14}	45 (0.21)
			Key agreement U_{15}	32 (0.15)
			Multi-factor authentication U_{16}	13 (0.06)
	Encryption intensity U_2	19 (0.32)	Theoretically decoding year U_{21}	23 (0.38)
			Freshness of secret key U_{22}	23 (0.38)
			Type of cryptograph U_{23}	14 (0.24)
	Resistance of attack U_3	21 (0.36)	Type of cannot-resistance-attack U_{31}	17 (0.57)
			Serious degree of cannot-resistance-attack U_{32}	13 (0.43)

5 AN ILLUSTRATIVE EXAMPLE

In this paper, we will use mobile commerce authentication scheme based on OTP as an example to begin illustrative example.

In this paper, we will use mobile commerce authentication scheme based on OTP as an example to begin illustrative example.

The main idea of OTP is to add indefinite factors during the course of logging in and compress it to a length definite digest, and then make the digest viz. password used each time different to improve security. The OTP based schemes have two common advantages. One is the password is different each time when logging in and therefore the adversary capture cannot guess the password. Second is that all of the schemes are using of hash function to produce OTP. If the input information changes a little, the output information would change a lot. Therefore, this character can resist the probability that the password would be juggled.

Two-dimension bar code is a kind of high density bar code. It can record much information limited in a small districts and itself is an integrated data file. There are two common used two-dimension bar codes. One is the stack bar code, such as PDF417... Code49. The other is matrix bar code, such as Maxi Code... Code1, etc.

For the problems of existed schemes and the features of two-dimension bar code, a new OTP scheme based on two dimension bar code is proposed (Mu Yang, 2008). This new scheme absorbed the advantages of the existed schemes; it adopts the high security function-hash function. The password is changed every time. The secret password does not transmit directly in the network and it also does not preserve directly in the server's database.

In the new scheme, we take IMEI (International Mobile Equipment Identity Number, IMEI) , and the specific identity of mobile equipment, as an important factor of authentication. This new scheme takes the indefinite factor-Counter and the mobile identity-IMEI or the service identity-Serl to generate OTP. And then take advantages of two-dimension bar code to cipher the authentication information twice. Details about the new mobile commerce authentication scheme will be got from the paper written by Mu Yang in the reference.

The evaluation system factor set, evaluation set and weight of each factor have been confirmed above, so here start illustrative example from Step 4. 10 experts' scoring statistics results as shown in Table 5.

According to the formula (1), security evaluation process and the results are as follows.

According to the formula (2), calculate the final evaluation result as follows.

$$
\begin{aligned}
T &= B \circ C \\
&= \begin{pmatrix} 0.3936 & 0.16928 & 0.35072 & 0.0384 & 0.048 \end{pmatrix} \circ \begin{bmatrix} 5 \\ 4 \\ 3 \\ 2 \\ 1 \end{bmatrix} \\
&= 3.82208 \approx 3.8
\end{aligned}
$$

The evaluation result is close to four, so the security evaluation result of mobile

Table 5: OTP authentication scheme security score.

Target level	**First level index**	**Second level index**	**Membership grade**				
			V_1	**V_2**	**V_3**	**V_4**	**V_5**
Security analysis	Authentication function U_1	Mutual authentication U_{11}	1.00				
		Anonymity U_{12}					1.00
		Non-repudiation U_{13}	1.00				
		Integrity U_{14}	1.00				
		Key agreement U_{15}	1.00				
		Multi-factor authentication U_{16}	1.00				
	Encryption intensity U_2	Theoretically decoding year U_{21}		0.80	0.20		
		Freshness of secret key U_{22}	1.00				
		Type of cryptograph U_{23}			0.50	0.50	
	Resistance of attack U_3	Type of cannot-resistance-attack U_{31}		0.20	0.80		
		Serious degree of cannot-resistance-attack U_{32}		0.20	0.80		

$$B_1 = W_1 \circ R_1$$

$$= \begin{pmatrix} 0.26 & 0.15 & 0.17 & 0.21 & 0.15 & 0.06 \end{pmatrix} \circ \begin{bmatrix} 1.00 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1.00 \\ 1.00 & 0 & 0 & 0 & 0 \\ 1.00 & 0 & 0 & 0 & 0 \\ 1.00 & 0 & 0 & 0 & 0 \\ 1.00 & 0 & 0 & 0 & 0 \end{bmatrix}$$

$$= \begin{pmatrix} 0.85 & 0 & 0 & 0 & 0.15 \end{pmatrix}$$

$$B_2 = W_2 \circ R_2$$

$$= \begin{pmatrix} 0.38 & 0.304 & 0.196 & 0.12 & 0 \end{pmatrix}$$

$$B_3 = W_3 \circ R_3$$

$$= \begin{pmatrix} 0 & 0.20 & 0.80 & 0 & 0 \end{pmatrix}$$

$$B = W_1 \circ R_1$$

$$= \begin{pmatrix} 0.32 & 0.32 & 0.36 \end{pmatrix} \circ \begin{bmatrix} 0.85 & 0 & 0 & 0 & 0.15 \\ 0.38 & 0.304 & 0.196 & 0.12 & 0 \\ 0 & 0.20 & 0.80 & 0 & 0 \end{bmatrix}$$

$$= \begin{pmatrix} 0.3936 & 0.16928 & 0.35072 & 0.0384 & 0.048 \end{pmatrix}$$

commerce authentication scheme based on OTP is close to "good" category.

6 CONCLUSIONS

According to the characteristics of mobile commerce, this paper establishes mobile commerce authentication security evaluation index system. This system involves 11 specific indexes which basically have no interrelated problems. On the basis of evaluation index system, this paper use the method of fuzzy comprehensive evaluation to build evaluation model, and further to assess a mobile commerce authentication scheme based on OTP as an illustrative example.

Using the fuzzy comprehensive evaluation method to study the authentication problem in mobile commerce could theoretically consider all the factors and make research more reasonable. Factors' weights and membership adopts expert scoring. Although each expert scoring also has certain subjective, but from all the experts overall it can reflect the objective and scientific.

As mobile commerce authentication security involving many factors, some indexes can not be quantitative evaluated yet and the selection of index will be further discussed. Each index's weight need to be further optimized and researched, in order to meet objective requirement of evaluation.

REFERENCES

Minglei S, Chengxiang T, Haihang W. Mobile authentication scheme using SMS. *2009 IITA International Conference on Services Science, Management and Engineering*, 2009: 161–164.

Kwok-Yan L, Siu-Leung C, Ming G, Jia-Guang S. Lightweight security for mobile commerce transactions. *Computer Communications*, 2003, 26: 2052-2060.

Neuman B, Ts'T. Kerberos: Authentication service for computer networks. *IEEE Communication Magazine*, 1994, 32(9): 33-38.

Aloul F, Zahidi S, El-Hajj W. Two factor authentication using mobile phones, *IEEE/ACS International Conference on Computer Systems and Applications*, 2009, 5: 641-644.

Oh HG, Kang SY, Seo JT, Lee IY, Moon J. Study on a safe and efficient mOTP (mobile-OTP) authentication mechanism for the mobile environment. *Journal of Internet Technology*, 2009, 10(5): 521-531.

Soleymani B, Maheswaran M. Social Authentication Protocol for Mobile Phones. *CSE' 09 International Conference on Computational Science and Engineering*, 2009, 8: 436–441.

Xuefei C, Xingwen Z, Weidong K, Liangbing H. Identity-based anonymous remote authentication for value-added services in mobile networks. *Vehicular Technology, IEEE Transactions*, 2009, 58(7): 3508–3517.

Hai-yan Q. Compairing the inductive method and strand spaces for security protocol. *Verification Journal of Computer Research and Development*, 2008, 45(Suppl.): 137-142 (in Chinese).

Javier Thayer Fdbrega F, Jonathan Hermg C, Joshua Guttman D. Strand spacers: Proving security protocols correct [J]. *Journal of Computer Security*, 1999, 7(2-3): 191-230.

Burrows M, Abadi M, Needham R. A Logic of Authentication [J]. *ACM Trans on Computer Systems*, 1990, 8(1): 18-36.

Lawrence Paulson C. The inductive approach to verifying cryptographic protocols. *Journal of Computer Security*, 1998, 6(2): 85-128.

Wei L, Wenye W. On performance analysis of challenge/response based authentication in wireless networks. *Computer Networks*, 2005, 48: 267-288.

Charlott E, Markus F, Ivar J. A criteria-based evaluation framework for authentication schemes in IMS. *ARES '09. International Conference on Availability, Reliability and Security*, 2009, 3: 865-869.

Patroklos Argyroudis G, Raja V, Hitesh T, Donal O'Mahony. Performance analysis of cryptographic protocols on handheld devices. *Third IEEE International Symposium on Network Computing and Applications*, 2004: 169 – 174.

Vipul G, Sumit G, Sheueling C, Douglas S. Performance analysis of elliptic curve cryptography for SSL. *ACM Workshop on Wireless Security*, 2002: 87-94.

Yong-bin Z, Zhen-feng Z, Guo-deng D. Analysis and Improvement of a Security-Provable Mutually Authenticated Key Agreement Protocol. *Journal of Software*, 2006,4(17): 868-875 (in Chinese).

Zhi-qiang X, Jun G, Jing Y. Analysis and design of new S/KEY authorization solution. *Computer engineering*, 2009 35(5): 175-176, 193 (in Chinese).

Kumar V.K.N. Mangipudi. New authentication and key agreement protocols for wireless applications [Graduate], *North Dakota State University*, 2005.

You-qing G, Xiao-jun W, Xiao-yan D. Electronic commerce security technology. *Beijing: Beijing university of posts an telecommunications press*, 2005 (in Chinese).

Jia-yuan L. Enaluation model based on status authentication system. *Computer knowledge and technology*, 2006, 7: 51-52, 57 (in Chinese).

Ze-shui X, Zhen-jun Y. Tow algorithms for fuzzy synthetic judgment. *Journal of PLA university of science and technology (Natural science edition)*, 2001, 2(4):5-8 (in Chinese).

Yang M, Runtong Z, Qin W, New Authentication Scheme for M-Commerce Based on Two Dimension Bar Code. *IEEE International Conference on Service Operations and Logistics, and Informatics*, 2008: 1029-1034.