International Journal of Electrical, Electronics and Computer Engineering **3**(1): 218-222(2014)

ISSN No. (Online): 2277-2626

Review of Security Analysis and Performance Evaluation of an Enhanced Two-Factor Authenticated Scheme

***Divya Jyoti*[*] *and Raman Kumar*[**]**

**Research Scholar, Department of Computer Science and Engineering,*
DAV Institute of Engineering and Technology, Jalandhar, (PB), India.
***Assistant Professor, Department of Computer Science and Engineering,*
DAV Institute of Engineering and Technology, Jalandhar, (PB), India.

(Corresponding author: Divya Jyoti)

(Received 05 March, 2014 Accepted 7 June, 2014)

ABSTRACT: Authentication is any protocol or process that permits one entity to establish the identity of another entity. It relies on three factors: 1) Something a user knows, such as a password or PIN 2) Something a user has, such as a key, a card, or another kind of token 3) Something a user is, such as a retina scan, or fingerprint. We can increase the reliability and security of the authentication mechanism by combining multiple authentication factors into a single model. The two factors together provide a much higher confidence in the authentication. This paper reviews various two-factor authentication schemes.

Keywords: Two-factor, smart card, authentication scheme, WSN.

I. INTRODUCTION

The key exchange problem is how to exchange whatever keys or other information needed so that no one else can obtain a copy. Key exchange protocols are used by which cryptographic keys are exchanged between users, allowing use of a cryptographic algorithm. Key exchange protocols allow two or more parties communicating over a public network to establish a common secret key called a session key. Due to their significance in building a secure communication channel, a number of key exchange protocols have suggested over the years for a variety of settings. In order to prevent man-in-the-middle and related attacks we can use various authentication means to provide authenticated key exchange protocols. The authentication means can be based on the following factors:

- The knowledge factors: Something the user knows (a password, pass phrase, or personal identification number (PIN), challenge response (the user must answer a question), pattern)
- The ownership factors: Something the user has (e.g., wrist band, ID card, security token, software token, or cell phone)
- The inherence factors: Something the use is or does (fingerprint, retinal pattern, face, voice, or other biometric identifier).

Based on these factors authentication can be one-factor or multi-factor. If a protocol contains only one authentication factor, it would be risky because the password can be recovered through social engineering (phishing or malwares), and the device can be stolen, open or cloned, even when some tamper-resistant techniques are used to protect it.

A proxy is basically another computer which serves as a hub through which internet requests are processed. By connecting through one of these servers, computer sends your requests to the proxy server which then processes the request and returns the result. A proxy signature allows a delegator to give partial signing rights to other parties called proxy signers on its behalf for example in the case of temporal absence, lack of time or computational power, etc. A multi proxy multi signature represents a certain number of proxy signers signing a given message. Number of signers is not fixed and signer's identities are evident from a given multi-signature the delegated proxy signer can compute a proxy signature that can be verified by anyone with access to the original signer's certified public key.

In 1996, Mambo et al. first introduced the concept of a proxy signature. A proxy signature scheme allows an original signer to delegate its signing power to a designated person, called the proxy signer, who can generate the proxy signature of a message on behalf of the original signer. The verifier can verify and distinguish between the original signature and the proxy signature at the verification stage.

Digital signature provides three important cryptographic functions: Confidentiality, Integrity and Availability. We have used CIA cube to illustrate this concept briefly. CIA cube stands for confidentiality, integrity and availability. Confidentiality means that only relevant information given to relevant people. Integrity means data must be available in original form. Availability means when we need data, it is available for use for information purpose to take decisions.

Proxy signatures have found numerous practical applications, particularly in distributed computing where delegation of rights is quite common. Examples include distributed systems, grid computing, mobile agent applications, distributed shared object systems, global distribution networks, and mobile communications.

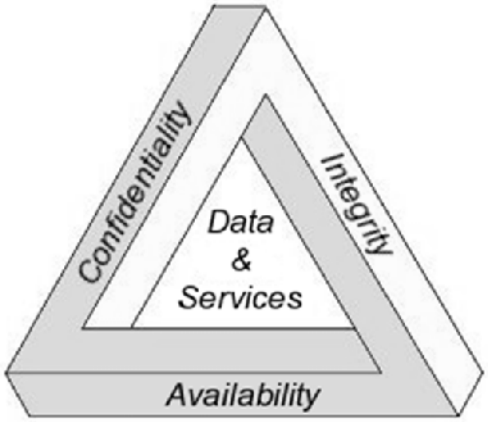

Fig. 1. CIA representation for multi proxy multi signature scheme

The proxy signature was introduced by Mambo, Usuda and Okamoto. Since then proxy signature schemes have been emerged from. New security considerations and constructions have been proposed, old schemes have been broken, followed by more constructions.

All multi proxy multi signature schemes use Public Key Infrastructure (PKI) setting, where each entity holds a public and secret key pair. Each user can sign messages using the signing algorithm of a standard digital signature scheme, and his or her secret key. When a user (the original signer) desires to delegate his or her signing ability to another user (the proxy signer), the users run a possibly interactive proxy-designation protocol. Through a successful execution of this protocol, the proxy signer obtains a proxy signing key. It can then sign messages on behalf of the original signer using a proxy signing algorithm and the proxy signing key. Anyone can verify the validity of such signatures using a proxy verification algorithm and the original signer's public key. The following are the security requirements should be satisfied for all the proxy signature schemes.

Secrecy: The original signers' private keys are very important. They must be kept secret. If they are discovered, the security of the system is ruined. Therefore, the system must ensure that the private keys never get derived from any information, such as the sharing of the proxy signing key or the original signers' public keys. Furthermore, no proxy signers should be able to cooperatively derive the original signers' private keys.

Proxy protection: Only the delegated proxy signer can generate valid partial proxy signatures. Even the original signers cannot create partial signatures.

Unforgeability: A valid proxy signature can only be cooperatively generated by t2 or more proxy signers. This means that valid proxy signatures cannot be created by t2 − 1 or less proxy signers, or any third parties who are not designated as proxy signers.

Non-repudiation: Any valid proxy signature must be generated by t2 or more proxy signers. Therefore, proxy signers cannot deny that they have signed the message. In addition, the original signers cannot deny having delegated the power of signing messages to the proxy signers.

Time constraint: The proxy signing keys can be used during the delegated period only. Once they expire, the proxy signatures generated by using those keys become invalid.

Known signers: From a proxy signature, the identities of the actual original signers and the identities of actual signers can be determined [36 and 37].

A. Two-Factor Authentication

Two-factor authentication requires the use of two of the three authentication factors stated above. The most commonly used authentication factors in two factor authentication are:

1. Something you know (as a secret password).
2. Something you have (as an unclonable secure device with a secret key).

Combining the two factors in the same authentication protocol could increase the security since the adversary would have to break the two protections in order to win [16].

The most common example of two-factor authentication is bank ATM, or debit cards. One authentication factor is the physical ATM card the customer slides into the machine ("something the user has"). The second factor is the PIN the customer enters through the keypad ("something the user knows"). Smart-card-based password authentication is one of the most convenient and commonly used two-factor authentication mechanisms. This technology has been widely deployed in various kinds of authentication applications which include remote host login, online banking, access control of restricted vaults, activation of security devices, and many more. A smart-card based password authentication scheme involves a server *S* and a client *A* (with identity *ID*). At first, *S* securely issues a smart-card to *A* with the smart-card being personalized with respect to *ID* and an initial password. This phase is called the *registration phase* and is carried out only once for each client. Later on, *A* can access *S* in the *login-and-authentication phase*, and this phase can be carried out as many times as needed. However, in this phase, there could have various kinds of passive and active adversaries in the communication channel between *A* and *S*. They can eavesdrop messages and even modify, remove or insert messages into the channel.

II. TWO-FACTOR AUTHENTICATION SCHEMES

There have been many smart-card-based password authentication schemes [7,8,9,12,18,20,21, 24] suggested in literature. In Lee *et al.*'s scheme [12], two password-based two-factor authentication and key exchange protocols are proposed. The first protocol does not provide pseudo identity and the second protocol provides identity protection. Both protocols require only two messages exchanging. These proposed protocols are suitable for low-power devices such as PDAs in public wireless LANs which require mutual authentication, low computation cost, identity protection, and less exchanged messages. In Hwang *et al.*'s scheme[8], a secure mutual authentication method is introduced. In Wu and Zhu's scheme[24], a secure authenticated key exchange protocol is presented that achieves fully two-factor authentication and provides forward security of session keys. They have used user's unique identity to accomplish authentication, instead of using public keys. They used nonces instead of timestamps to avoid the clock synchronization problem. Their scheme allows users to change their password freely without any interaction with the server. They have also given a security proof of their protocol using random-oracle model. In Rakesh Maharana's scheme [31], a smart card based user authentication scheme based on elliptic curve cryptography for large scale hierarchical wireless sensor networks is presented. This scheme combined ECDH (Elliptic curve Diffie–Hellman) and cryptographic hash function to provide authentication as well as a session key for further communication between user and cluster head. Here, feasibility of ECC in context of WSN is demonstrated. It provides mutual authentication between user and base station as well as base station and cluster head. The proposed scheme also provides option for dynamic node addition where there is no need to update any information in user smart card for accessing real time data for any addition or replacement of cluster heads in the networks. It provides a secret session key for further communication between user and the cluster head. This scheme implements merit of using ECC-based mechanism in WSN and enhances the WSN authentication with higher security than other protocols.M.L.Das[25] proposed a two-factor user authentication protocol for WSN using only hash function. The proposed protocol avoids *many* logged in users with the *same* login-id and stolen-verifier attacks, which are prominent threats for a password-based system if it maintains verifier table at the GW-node or sensor node. In addition, the proposed protocol resists other attacks in WSN except the denial-of-service and node compromise attacks. They have showed the efficiency of the proposed protocol in comparisons with the related ones. Khan and Alghathbar [26] have shown in their scheme that a recently proposed two-factor user authentication scheme in WSN environment is insecure against different kinds of attack and should not be implemented in real applications. They have demonstrated that in the M.L. Das-scheme [25], there is no provision for users to change or update their passwords, the GW-node bypassing attack is possible, it does not provide mutual authentication between GW-node and sensor node, and it is susceptible to privileged-insider attack. To remedy the fore mentioned flaws, they have proposed security patches and improvements, which overcome the weak features of the M.L. Das-scheme. The presented security improvements can easily be incorporated in the M.L. Das-scheme for a more secure and robust two-factor user authentication in WSNs. Nyang *et al.*[28] pointed out that Das's[25] two-factor user authentication protocol is weak against the off-line password guessing attack by insiders, and showed that a simple patch that appends secret parameter to the authentication information can eliminate this weakness without sacrificing any efficiency and usability. Also, to protect query responses from wireless sensor nodes to a user, they proposed an efficient method which can be easily implemented using a built-in AES function in sensor nodes. Finally, they gave a guideline for secure implementation of authentication protocols which prevents the outsider who captures a sensor node from mounting password guessing attack and from impersonating the gateway node. Binod Vaidya *et al.*[29]have proposed an improved two-factor user authentication scheme to overcome the security weaknesses of the previous schemes [25,26] for WSN. Their scheme is resilient to stolen verifier attacks as well as other common types of attacks. They have provided security evaluation and efficiency analysis, which show that their protocol is more robust and secure than the existing schemes and as efficient as them. However, their scheme does not provide session key agreement and mutual authentication between user and sensor node/gateway node. Qiong Pu [30] suggested that in addition to the five desirable properties (client authentication, server authentication, server knows no password, freedom of password change and prevention from guessing attack), key compromise impersonation resilience should also be added as one more important security requirement for two factor smart-card-based password mutual authentication[21]. It means the adversary should not be able to to masquerade any user to access the server's service once if the long-term key of the server is compromised. They provided an attack to illustrate the adversary is able to masquerade any user to access the server's service in their protocol once if the long-term key of the server is compromised. Finally, they have proposed such an improved protocol that eliminates the security weakness existing in Yang *et al.'s* protocol [21] i.e. allowing key-compromise impersonation.

III. PROBLEM FORMULATION

From the literature survey it was found that various two factor authentication schemes have been proposed in different settings. These schemes resist various security attacks. Security analysis of these schemes will lead to comparison of their efficiency. Further, an Enhanced Two-Factor Authentication Scheme is to be proposed that can resist various security attacks.

IV. PROPOSED WORK

In the proposed work, an Enhanced Two-Factor Authentication Scheme is proposed that can resist various security attacks. In the proposed work we have provided a two-factor authentication scheme which will prevent the attacks in network by eliminating the attack races by matching it with knowledge available in the network. Best way to fetch results based on the proposed scheme is to provide secure matching of malicious traffic with knowledgebase available in the backend but due to delay in matching, we have chosen pseudonym combo concept for matching which could be very useful in cutting delay from matching process. The server stores information of register users with pseudonyms and actual ID of users to reveal the anonymity in case of a problem.

V. CONCLUSION

In this paper we have provided the overview of various two-factor authentication schemes and proposed an enhanced two-factor authentication scheme which will prevent the attacks in network by providing matching of malicious traffic with knowledge available in the network.

REFERENCES

[1] Abdalla M., Bellare M., and Rogaway P., “The Oracle Diffie-Hellman Assumptions and an Analysis of DHIES,” in *Proceedings of the Cryptographer's Track at RSA*, pp. 143-158, 2001.

[2] Abdalla M., Chevassut O., and Pointcheval D., “One-Time Verifier-Based Encrypted Key Exchange,” in Proceedings of Public Key Cryptography, pp. 47-64, 2005.

[3] Bellare M., Pointcheval D., and Rogaway P., “Authenticated key Exchange Secure Against Dictionary Attacks,” in Proceedings of international conference on Theory and application of cryptographic techniques EUROCRYPT, pp. 139-155, 2000.

[4] Bresson E., Chevassut O., and Pointcheval D., “New Security Results on Encrypted Key Exchange,” in Proceedings of Public Key Cryptography, pp. 145-158, 2004.

[5] Chien H., Jan J., and Tseng Y., “An Efficient and Practical Solution to Remote Authentication: Smart Card,” *Computer Journal of Secures*, vol.**21**, no. 4, pp. 372-375, 2002.

[6] Hankerson D., Menezes A., and Vanstone S.,Guide to Elliptic Curve Cryptography, Springer-Verlag, USA, 2004.

[7] Hwang M., “Cryptanalysis of Remote Login Authentication Scheme,” *Computer Journal of Communications*, vol. **22**, no. 8, pp. 742-744, 1999.

[8] Hwang M., Chong S., and Chen T., “DoS- Resistant ID-Based Password Authentication Scheme Using Smart Cards,” *Computer Journal of Systems and Software*, vol. **83**, issue 1, pp. 163-172,2010.

[9] Hwang M., Lee C., and Tang Y., “An Improvement of SPLICE/AS in WIDE Against Guessing Attack,” *Internet Journal of Information*, vol. **12**, no. 2, pp. 297-302, 2001.

[10] Koblitz N., “Elliptic Curve Cryptosystem,” *Computer Journal of Mathematics Computation,* vol. **48**, no. 3, pp. 203-209, 1987.

[11] Lamport L., “Password Authentication with Insecure Communication,” *Computer Journal of Communications ACM*, vol. **24**, no.11, pp. 770-771, 1981.

[12] Lee Y., Kim S., and Won D., “Enhancement of Two-Factor Authenticated Key Exchange Protocols in Public Wireless LANs,” *Computers and Electrical Engineering,* vol. **36**, issue 1, pp.213-223, 2010.

[13] Liao I., Lee C., and Hwang M., “A Password Authentication Scheme over Insecure Networks,” *Computer Journal of System Science*, vol. **72**, no. 4, pp. 727-740, 2006.

[14] Mitchell C., Ward M., and Wilson P., “On Key Control in Key Agreement Protocols,” *Computer Journal of Electronics Letters*, vol. **34**, no. 3, pp.980-981, 1998.

[15] Okamoto T. and Pointcheval D., “The Gap-Problems: a New Class of Problems for the Security of Cryptographic Schemes,” in *Proceedings of Public Key Cryptography*, pp. 104-118, 2001.

[16] Pointcheval D. and Zimmer S., “Multi-Factor Authenticated Key Exchange,” in Proceedings of Applied Cryptography and Network Security, pp.277-295, 2008.

[17] Quisquater J., “Side Channel Attacks-Stat, October, http://www.ipa.go.jp/security/enc /CRYPTREC/fy15/doc/1047_Side_Channel _report .pdf, Last Visited 2002.

[18] Scott M., “Cryptanalysis of an Id-Based Password Authentication Scheme Using Smart Cards and Fingerprints,” *Computer Journal of SIGOPS Operation System Review*, vol. **38**, no. 2, pp. 73-75, 2004.

[19] Sklavos N., Alexopoulos E., and Koufopavlou O., “Networking Data Integrity: High Speed Architectures and Hardware Implementations,”. *The International Arab Journal of Information Technology*, vol. **1**, no. 2, pp. 54-59, 2003.

[20] Wang B., Li J., and Tong Z., “Cryptanalysis of an Enhanced Timestamp-Based Password Authentication Scheme,” *Computer Journal of Secures,* vol. **22**, no. 7, pp. 643-645, 2003.

[21] Yang G., Wonga D., Wang H., and Deng X., “Two-Factor Mutual Authentication Based on Smart Cards and Passwords,” *Journal of Computer and System Sciences*, vol. **74**, no. 7, pp. 1160-1172, 2008.

[22] Yoon E., Ryu E., and Yoo K., “Efficient Remote User Authentication Scheme Based on Generalized Elgamal Signature Scheme,” *Computer Journal of IEEE Transaction Consumer Electronic*, vol. **50**, no. 2, pp. 568-570, 2004.

[23] Yoon E. and Yoo K., “New Authentication Scheme Based on a One-Way Hash Function and Diffie-Hellman Key Exchange,” in *Proceedings of Cryptology and Network Security*, China, pp. 147-160, 2005.

[24] Shuhua Wu, Yuefei Zhu” Improved Two-Factor Authenticated Key Exchange Protocol” *The International Arab Journal of Information Technology*, Vol. **8**, No. 4, October 2011.

[25] M. L. Das, "Two-Factor User Authentication in Wireless Sensor Networks" IEEE Trans. *Wireless Comm. 2009*, 8, pp. 1086-1090.

[26] M. K. Khan, and K. Alghathbar, "Cryptanalysis and Security Improvements of ‘Two-Factor User Authentication in Wireless Sensor Networks’", Sensors 2010, **10**(3), pp. 2450-2459.

[27] Juang W. “Efficient password authenticated key agreement using smart card,” Computers & Security, 2004; 23:167–.73.

[28] Nyang, DH.; Lee M.K. Improvement of Das’s Two-Factor Authentication Protocol in Wireless Sensor Networks, Cryptology ePrint Archive 2009/631. Online PDF: http://eprint.iacr.org/2009/631.pdf (accessed on 28 February 2010).

[29] Binod Vaidya, Dimitrios Makrakis, Hussein T. Mouftah “Improved Two-factor User Authentication in Wireless Sensor Networks” Second international workshop on network assurance and security services in ubiquitous environment, 600-606, October 2010.

[30] Qiong Pu “An Improved Two-factor Authentication Protocol” *Second International Conference on MultiMedia and Information Technology*,2010.

[31] Rakesh Maharana, Pabitra Mohan Khilar “An Improved Authentication Protocol for Hierarchical Wireless Sensor Networks using ECC” *International Journal of Computer Applications* (0975 – 8887) Volume **67**, No.22, April 2013.

[32] Harsh Kumar Verma, Kamalpreet Kaur and Raman Kumar, "A Comparison of Threshold Proxy Signature Scheme", *The 2008 International Conference on Security and Management, USA*, 14-17 July, 2008.

[33] Raman Kumar and Harsh Kumar Verma, "An Advanced Secure (t, n) Threshold Proxy Signature Scheme Based on RSA Cryptosystem for Known Signers", *IEEE 2nd International Advance Computing Conference*, Thapar University, India, 19-20 February, 2010.

[34] Raman Kumar and Harsh Kumar Verma, ”Secure Threshold Proxy Signature Scheme Based on RSA for Known Signers", *Journal of Information Assurance and Security, JIAS,* Vol. **5**, Issue 1, pp. 319-326, 2010.

[35] Raman Kumar, Harsh Kumar Verma and Renu Dhir, "Security Analysis and Performance Evaluation of Enhanced Threshold Proxy Signature Scheme Based on RSA for Known Signers", *International Journal of Computer Network and Information Security, IJCNIS, Hong Kong*, Vol. **4**, No. 9, pp. 63-76, 2012.

[36] Raman Kumar, Harsh Kumar Verma and Renu Dhir, "Cryptanalysis and Performance Evaluation of Enhanced Threshold Proxy Signature Scheme Based on RSA for Known Signers", Mathematical Problems in Engineering, Hindawi, USA, Vol. **2013**, Article ID 790257, pp. 1-24, 2013.

[37] Raman Kumar and Nonika Singla, " Cryptanalytic Performance Appraisal of Improved CCH2 Proxy Multisignature Scheme", *Mathematical Problems in Engineering*, vol. 2014, Article ID 429271, 13 pages, 2014. doi:10.1155/2014/429271.

[38] Zuowen Tan, Zhuojun Liu , Chunming Tang, “Digital Proxy Blind Signatures schemes based on DLP and ECDLP” in MMRC, AMSS , Academia , Sinica , Beijing No.21., 2002, pp.212-216.

[39] Alexandra Boldyreva and Adriana Palacio and BogdanWarinschi, “Secure Proxy Signature Schemes for Delegation of Signing Rights” at: http://eprint.iacr.org/2003/096, 2003.

[40] Guilin Wang, FengBao, Jianying Zhou and Robert H. deng, “A Practical (t, n) threshold proxy signature scheme based on RSA Cryptosystem”, *in Transactions on knowledge and data engineering, In: IEEE,* vol. **16**, no. 10,2004, pp.1309-1311.