A NOVEL PARADIGM IN AUTHENTICATION SYSTEM USING SWIFI ENCRYPTION /DECRYPTION APPROACH

Shadi R. Masadeh[1] , Ahmad Azzazi[2], Bassam A. Y. Alqaralleh[3] and Ali, Mousa.Al Sbou[4]

[1] Computer Networks Department, Isra University, Amman, Jordan
[2] Computer Information Systems Department, Applied Science University, Amman, Jordan
[3]Computer Science Department, Al-Hussein Bin Talal University, Ma'an, Jordan
[4]Computer Science Department, Al-Hussein Bin Talal University, Ma'an, Jordan

ABSTRACT

Maintaining the security of your computer, network and private/sensitive data against unauthorized access and a wide variety of security threats can be challenging. Verifying data integrity and authentication are essential security services in order to secure data transmission process. In this paper we propose a novel security technique which uses new encryption and decryption algorithms to achieve authenticated communication and enhanced data integrity. The proposed technique is very complex for attackers to decode, and it is applicable to client-server architecture.

KEYWORDS

Authentication, PGP, sWIFI, HMAC, Encryption\Decryption, integrity.

1. INTRODUCTION

("Internet security and encryption," 2012) All Network users aim to access information and transfer data safely. To ensure secure transmission of information between the parties; a group of challenges must met. We confined these challenges to three areas: data Integrity, authentication and privacy (Alaidaros, Rasid, Othman, & Abdullah, 2007).

Privacy refers to secure and valuable data (Diffie & Hellman, 1979) which should not be accessible unless the parties concerned are allowed to do so. Many techniques can be used to maintain and improve user privacy such as cryptography techniques (Griffin, 1998), passwords and firewall. In an unsecure environment, it is easy to break through privacy in several ways. For example, viewing data without certificate, behavior scanning or movement tracking (Hajny, Pelka, & Zeman, 2010) and eavesdropping. Recently, there is an attempt to break the privacy of the users on encrypted channels (Dusi, Gringoli, & Salgarelli, 2008).

Integrity refers to the consistency and accuracy of data to ensure that unauthorized parties are prevented from modifying data Authentication (Serwan Waleed, 2011). As a result, the data which is received must be to be the same as the data sent. Protecting data transmission process is necessary to avoid any intentional or unintentional changes of these data. Any damage or distort of data will affect the feasibility of these data or information; it becomes not beneficial and not

safe to use. Data can use multiple techniques such as encryption, Digital signature and Checksum to avoid any damage or distort.

Authentication is the process of verifying if a user or entity or device is who claims to be. In other words it's a combination of **verification** and **Identification**. Authentication falls into three categories (Al-Assam, Sellahewa, & Jassim, 2010):

- Knowledge factors: something you know (e.g. Password, personal identification number)
- Ownership factors: something you have (e.g. Smart Card, cell phone, ID card)
- Inherence factors: something you are (e.g. fingerprint, signature, voice, iris, biometric).

To enhance security, different types of authentication are combined. The client, host and transmission channel are the locations where authenticators can be attacked (O'Gorman, 2003).

In this paper, we propose a novel approach to enhance the data integrity, authentication and privacy depending on some encryption / decryption methods by combining PGP, sWIFI and HMAC Systems. The proposed system provides the protection and safety to secure data transfer across networks against spoofing, tampering, repudiation, security attacks and Information disclosure**.**

The rest of this paper is organized as follows: Section 2 describes the related work. Proposed Authentication model is discussed in Section 3. Finally, conclusions are drawn in section 4.

2. RELATED WORK

According to (American Bankers, 2000), the HMAC is a technique that uses cryptographic hash functions for message authentication. This technique combines any iterative cryptographic with a shared secret key. The HMAC has two parameters, the message and a shared secret key which is known only to the sender and receiver. The sender uses HMAC to produce a value which is represents the combination of the secret key and the message input, the new value is called MAC the sender appends the MAC message and sends all to the receiver. The receiver uses HMAC and a shared secret key, that the sender used before, by applying the MAC algorithm to the received message and compares the result with the received MAC. We can insure that the message has been correctly received if the two values match. This process also provides assurance that the message comes from sender who shares the key.

(Krovetz, 2006) in their paper mentioned that only the sender and receiver know the hash function which is used by sender to hash message and produce the hash value, then the sender encrypts the resulting hash value by using cryptographic function to create a message tag which is sent to receiver with the message. On the receiver's side, the user needs to verify that the receiver's tag is valid for the receiver message based on the hash function and cryptographic key which are known only to the sender and receiver.

(Aljawarneh, Masadeh, & Alkhateeb, 2010), proposed a secure Wireless Fidelity (sWIFI) system which provides more efficiency, security and authentication for transmitted data over the network. Basically, sWIFI are based on HMAC Algorithm.

There are many steps to use sWIFI : First, the sWIFI is split into two parts: The first part is the plain text for key purposes, the second part is split into four pieces; to generate and encrypt the key using logical OR-ing and bit shifting of the data in a certain pattern in the four portions. In order to generate the key, encrypt the first part and disrupt the probabilistic phenomena of the letters in the language. Finally, within the blocks the encrypted data is shuffled to make sure that there is no similarity with original data. (Aljawarneh et al., 2010) Pretty Good Privacy, is one of the most important encryption and security applications that use efficient and confidential algorithms to secure data transmission. The PGP as a encryption program founded by Phil Zimmerman on 1991 provides complete verification and encryption for message files (McLaughlin, 2006).

The PGP is considered the most key cryptographic used by the public with PGP in a secure manner so there is no need for any specific infrastructure (Chadwick, Young, & Cicovic, 1997).The security of PGP Model is trusted since it is an open Source so professional people can close any weaknesses if found, it is based on symmetric-key cryptography and use combination of data compression, hashing and public-key cryptography (Kurniawan, Albone, & Rahyuwibowo, 2011) .

(Abdul-Rahman, 1997),(Guibing, Jie, & Vassileva, 2011) The PGP is the first successful attempt of a free cryptographic model which is available for the public. The sender who has the private key is able to create a digital signature for corresponding public key. Digitally, PGP gives other users the ability to sign certificates that they think it is authentic, so the owner of the public key is an owner of the certificate. To verify a public key, the user needs to check if there are any digital signatures that are signed by the trusted users.

PGP compresses the message and creates a public key and a private key for the sender through cryptography software. When the plain text is encrypted, the public key is encrypted to the receiver's private key which can be used by the receiver to decrypt the message (Abdul-Rahman, 1997).

Although the PGP is considered as one of the best encryption techniques, it does have some disadvantages. The PGP process is considered a complex process to use on a regular basis since it is very difficult for many people to grasp the meaning of Cryptography. Also, The PGP is a two-way street that the sender and the recipient must use it, otherwise the recipient will not be able to view the encrypted data(Gibson, 2002). Managing keys for a new user using PGP will be a challenge. Lost or corrupted keys lead to high risk and will not allow users to view encrypted data.

3. PROPOSED AUTHENTICATION MODEL

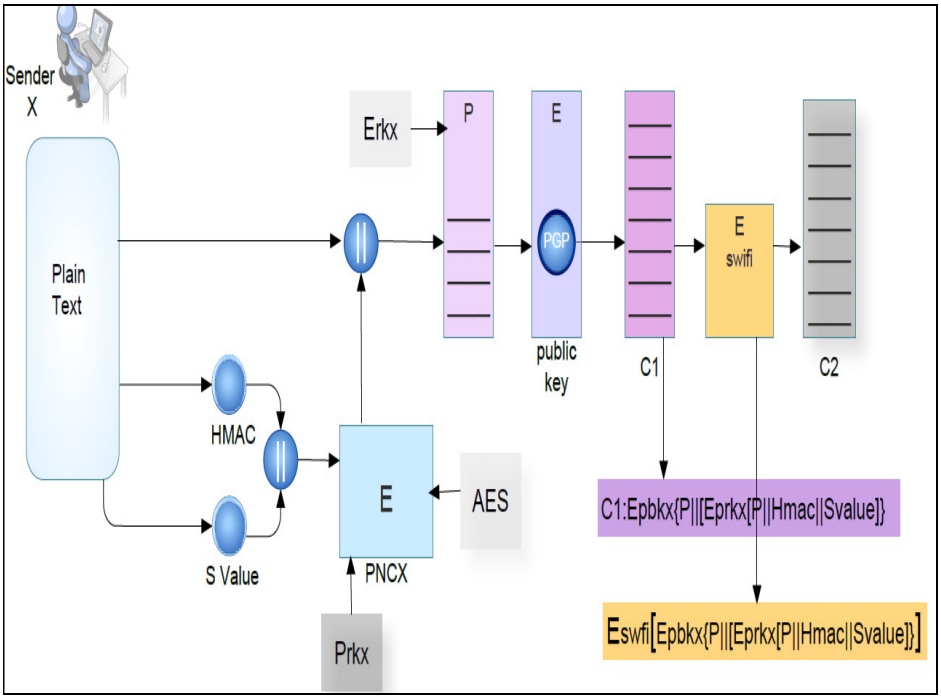

Figure 1: Authentication model in Sender side

In this method the sender submits a plain text message, and uses an HMAC generator to generate an HMAC for to the text. A local program generates a secure value (S_Value) which is in turn concatenated with the HMAC that is previously generated.

The message is then fed to AES encryptor that generates an encrypted version of the concatenated (HMAC II S_VALUE) and concatenates the result with the original plain text message. The message is then encrypted using PGP using the receiver public key to generate the PGP encrypted message.

The encrypted message is then further encrypted using sWIFI encryptor to generate the final message in order to be sent to the receiver as depicted in the steps below:

1- Enter the message (plain text) and then insert the Hash message authentication code (HMAC) and secured value (S_value) to the original message.

2- Concatenate the HMAC with S_value.

3- Encrypt the result from step 2 using private key as follows

C → (Eprk (HMAC II S_value))

4- Concatenate the result from step 3 with the original message (plain text) as follows:

C → (P II (Eprk (HMAC II S_value))).

5- Encrypt the result from step 4 using PGP as follows:

C → Epbk (P II (Epr (HMAC II S_value))).

6- Encrypt the result from step 5 using sWIFI as follows:

C → E sWIFI [Epbk (P II (Epr (HMAC II S_value)))].

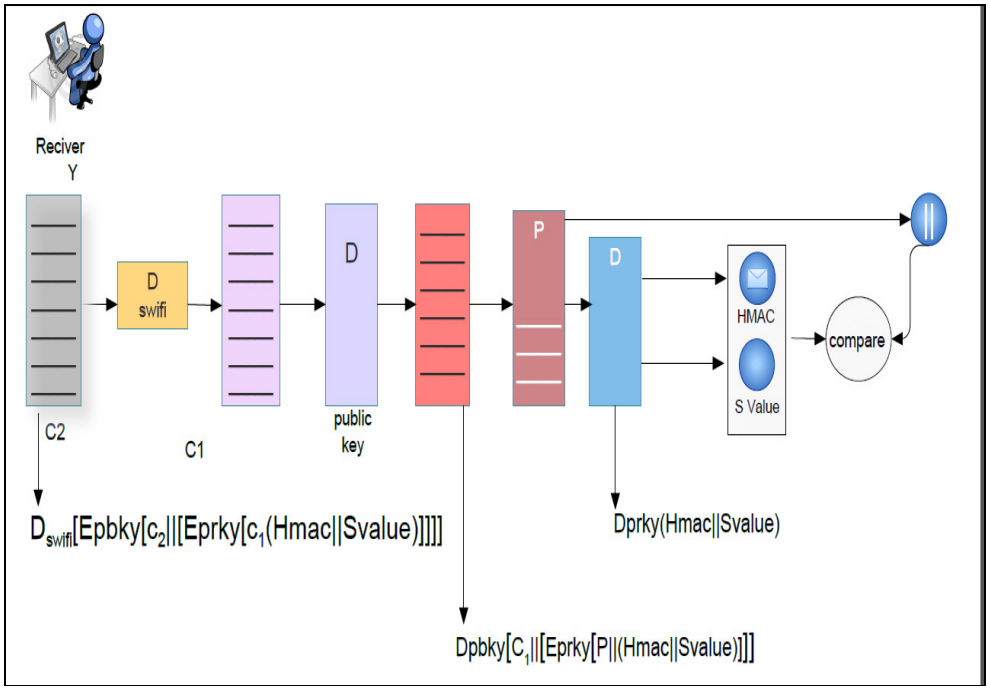

Figure 2: Authentication model in Receiver side

On the receiver's side, the receiver uses the sWIFI decryptor to get the PGP encrypted message, which is then decrypted using the sender's Public key with the receiver's private key.

The receiver then uses the AES decryptor to retrieve the encrypted message that contains the HMAC and S_VALUE at the end of the message.

The receiver then extracts the HMAC and S_VALUE, and generates a new HMAC from the received message.

The receiver then compares both HMACs. If both HMACs match, the message is authenticated and has not been altered, or otherwise, the receiver sends the sender a request to resend the message.

The full process is illustrated by the following steps:

1- Receive the message (cipher text) from the sender as follows:

C → E sWIFI [Epbk (P II (Eprk (HMAC II S_value)))]

Then the receiver decrypts the formula as follows:

P → D sWIFI [Epbk (C II (Eprk (HMAC II S_value)))]

2- Decrypt the result from step1 using PGP as follows:

P → Dpbk (C II (Eprk (HMAC II S_value))).

3- Decrypt the result from step 2 as follows:

P → Dprk (HMAC II S_value))).

4- Extraction the HMAC with S_value.

5- Compare the plain text (original message) from sender side with the message from receiver side. If there is no alteration of the message was found then the message is authenticated.

4. CONCLUSION

A novel design approach for authentication system was presented in this paper. Our approach can reduce the security risk across networks by combining PGP, sWIFI and HMAC systems. The proposed system is expected to present, protect, and enhance the data integrity, Authentication and privacy. Also, it increases the strength against network risks. Furthermore, our authentication system is very complex, which means that it is almost impossible to decrypt the method.

REFERENCES

[1] Abdul-Rahman, A. (1997). The PGP Trust Model. EDI-Forum: The Journal of Electronic Commerce, 10(3), 27-31. doi: citeulike-article-id:8251892

[2] Al-Assam, H., Sellahewa, H., & Jassim, S. (2010). Multi-factor biometrics for authentication: a false sense of security. Paper presented at the Proceedings of the 12th ACM workshop on Multimedia and security, Roma, Italy.

[3] Alaidaros, H. M., Rasid, M. F. A., Othman, M., & Abdullah, R. S. A. (2007, 14-17 May 2007). Enhancing security performance with parallel crypto operations in SSL bulk data transfer phase. Paper presented at the Telecommunications and Malaysia International Conference on Communications, 2007. ICT-MICC 2007. IEEE International Conference on.

[4] Aljawarneh, S., Masadeh, S., & Alkhateeb, F. (2010). A secure wifi system for wireless networks: an experimental evaluation. NETWORK SECURITY(Jun), 6-12.

[5] American Bankers, A. (2000). Keyed hash message authentication code : X9.71-2000. Wash., D.C.: ABA.

[6] Chadwick, D. W., Young, A. J., & Cicovic, N. K. (1997). Merging and extending the PGP and PEM trust models-the ICE-TEL trust model. Network, IEEE, 11(3), 16-24. doi: 10.1109/65.587045

[7] Diffie, W., & Hellman, M. E. (1979). Privacy and authentication : An introduction to Cryptography. Proceedings of the IEEE, 397.

[8] Dusi, M., Gringoli, F., & Salgarelli, L. (2008, 8-10 Sept. 2008). A Model for the Study of Privacy Issues in Secure Shell Connections. Paper presented at the Information Assurance and Security, 2008. ISIAS '08. Fourth International Conference on.

[9] Gibson, D. (2002). Email Security Risks and How To Reduce Them. 1.4.

[10] Griffin, J. A. (1998, 12-13 Jun 1998). Privacy and security in the Digital Age. Paper presented at the Technology and Society, 1998. ISTAS 98. Wiring the World: The Impact of Information Technology on Society., Proceedings of the 1998 International Symposium on.

[11] Guibing, G., Jie, Z., & Vassileva, J. (2011, 22-27 Aug. 2011). Improving PGP Web of Trust through the Expansion of Trusted Neighborhood. Paper presented at the Web Intelligence and Intelligent Agent Technology (WI-IAT), 2011 IEEE/WIC/ACM International Conference on.

[12] Hajny, J., Pelka, T., & Zeman, V. (2010, 26-28 July 2010). Privacy protection for user authentication. Paper presented at the Security and Cryptography (SECRYPT), Proceedings of the 2010 International Conference on.

[13] Internet security and encryption. (2012) Retrieved 18/12/2012, from http://www.hazemsakeek.com/Scientifc_Assay/internet/security.htm

[14] Krovetz, T. (2006). Message Authentication on 64-bit Architectures. IACR Cryptology ePrint Archive, 37.

[15] Kurniawan, Y., Albone, A., & Rahyuwibowo, H. (2011, 17-19 July 2011). The design of mini PGP security. Paper presented at the Electrical Engineering and Informatics (ICEEI), 2011 International Conference on.

[16] McLaughlin, L. (2006). Philip Zimmermann on What's Next after PGP. Security & Privacy, IEEE, 4(1), 10-13. doi: 10.1109/msp.2006.20

[17] O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. Proceedings of the IEEE, 91(12), 2021-2040. doi: 10.1109/jproc.2003.819611

[18] Serwan Waleed, J. (2011). IMPROVEMENT OF DATA INTEGRITY USING DIFFERENT ENCRYPTION ALGORITHMS. IRAQI JOURNAL OF COMPUTERS,COMMUNICATION AND CONTROL & SYSTEMS ENGINEERING المجلة العراقية لهندسة الحاسبات والاتصالات والسيطرة والنظم, 11(2), 1-6.

Authors

Shadi R. Masadeh received a BSc degree in Computer Science and Computer Information System in 2000 and MSc degree in Information Technology in 2003. with a Thesis titled "A Mathematical Approach for Ciphering and Deciphering Techniques" After that, I received PhD from department of Computer Information System in 2009 with a Thesis titled "A New Embedded Method for Encryption/Decryption Technique Using Self Approach" My research interests including E-learning Management and Security Issues, Encryption and Decryption Systems. Networking and Wireless security. Currently, I'm working at Al-ISRA University in Computer Networks Department as assistant Prof. I have submitted a number of conference papers and journals.

Ahmad Azzazi is an assistant professor in the Department of Computer Information Systems at the Applied Science University. Dr. Azzazi's research interests include software engineering frameworks, speech processing, software security, expert systems and expert systems.

Bassam A. Y. Alqaralleh received a BSc degree in Computer Science in 1992, graduate Diploma in Computer Information Systems in 2002 and Masters degree in Computer Science in 2004. After that, I received PhD from University of Sydney in 2010 with a Thesis titled " Addressing Data and Access Skew Problems in Data-Indexed Overlays". My research interests including Distributed Systems, Load-Balancing, Networking, Security Systems. and Wireless security. Currently, I'm working at Al-Hussein Bin Talal University in Computer Science Department as assistant Prof. I have published a number of conference papers and journals.

Ali Mousa Al Sbou has got the BSc degree in computer science from Mutah University, Jordan in 2001.Andhe has got master degree in information technology from Universiti Utara Malaysia, Malaysia in 2010. He is works as a Computer lab supervisor at Al Hussein Bin Talal University, Jordan.