Survey on Secured Password Authentication for IOT

Vanitha M

School of Information and Technology, VIT University, Vellore - 632014, Tamilnadu,India

Abstract
Password is easy and mostly used method to provide security and authentication. Now in IOT environment many devices like RFID, smartcard, and wireless sensor devices use passwords for security. But passwords are susceptible to many attacks like loss of password, eavesdropping, forgetting passwords, etc., By saving passwords in a single server it is more prone to loss of password if the server is compromised. In order to avoid this it is better to divide and save passwords in multiple server and this helps us to overcome loss of password on servers. This paper has used light weight cryptographic algorithm to secure these passwords in the network because this type of algorithm occupies less space and the execution speed will be high. Some of the recent light weight cryptographic algorithms are Humming bird, PRESENT, TEA, XXTEA and Humming Bird which was surveyed by Eisenbarth et al.[1]. These are specially designed for smart cards, RFID etc. This paper has implemented an algorithm that divides and saves password on two servers and use PRESENT algorithm on one server and use Humming Bird algorithm on another server for providing the efficient password security. So our model will be more secured than any other existing works.
Keywords RFID; Smart Card; IOT; PRESENT; Humming Bird

1 Introduction

Currently, Internet of Things (IoT) is a communication paradigm that predicts a near future, in which the objects of normal life will be prepared with microcontrollers for digital communication that will make them able to communicate with one another and with the users, becoming an essential part of the Internet discussed by L. Atzori et al.[2]. The IoT aims at making the Internet even more pervasive by enabling easy access and providing good security. This model finds application in different domains, such as home automation, medical aids ,industrial automation, elderly assistance, mobile healthcare, traffic management, intelligent energy management and smart grids, automotive, and many others. In order to provide security for those devices we require some sort of light weight cryptographic algorithms for the two reasons such as 1. For the low resource-devices, e.g. battery-powered devices, the cryptographic operation with a limited amount of energy. 2. Lower resource devices that are the footprint of the lightweight cryptographic primitives are smaller than the conventional cryptographic ones.

Previously password based authentication model transmitted the hash value of the password in the public channel which is easily accessible by the attacker. Burande et al surveyed the data and said that 55 percent of the password can be cracked in 8hours using the password recovery toolkit which is commercially available[3].

The first protocol for the password based authentication is PKI(Public Key Infrastructure) model. The purpose of a PKI is to validate the information being transferred in a network and to confirm the identity of the clients using passwords. This model is used by Gong et al[4], the client can send the password to the server by using public key encryption. Bellovin et al have proved that the password is unaffected to offline dictionary attack[5]. Halevi et al given the proofs for PKI model with the formal definitions[6].

The second protocol for the password authentication is password-only model, Bellare et al[7], Boyko et al[8] and Yang et al[9] have introduced a method called encrypted key exchange. The password is used as a secret key for key exchange. They were the first to give password only protocol which is more secure under cryptographic assumption. But consider the scenario that all the passwords are stored in the single server; if that server is compromised due to attacks the password will be disclosed.

The overcome this issue , the third protocol called two server password only model were introduced ,where two servers cooperate , even if one server is compromised the attacker cannot act like a client with the information from the compromised server. Katz et al protocol called KOY protocol can run in parallel and generates secret session key between client and the two servers[10]. Goldreich et al discussed about the session key generation[11]. Due to denial of service attack if one of the servers shuts down another server can continue to provide services to the clients.

All the above mentioned protocols two servers share the random password $pw1$ and $pw2 = pw$. Yi et al proposed a new symmetric solution for the Password only authenticated Key Exchange (PAKE)[12], one server $s1$ with an encryption of the password $pk1$ and another server $s2$ with the encryption of the password $pk2$, where $pk1$ and $pk2$ are the encryption keys of $s1$ and $s2$. They have concluded that their protocol is secure against passive and active attacks even if one of the servers is compromised.

This paper has propose the new solution for the two servers PAKE. Current works considered Diffie-Hellman Key Exchange protocol for the clients to establish a shared key over a communication channel. Another protocol they have used is ELGamal encryption which consists of encryption, decryption and key generation algorithms. We use light weight cryptographic algorithm which is specifically designed for smart cards, RFID tags, and wireless sensor devices. Password is

divided in to two halves, one in server1 and second in server2. Both the servers are not aware of each others encryption keys. Security analysis has shown that our protocol is secure against the attacks like smart card loss attack, forgery attack and DOS attack. Moreover proposed work have improved the efficiency of the system by reducing the execution speed as well as the memory occupied by the algorithm is also reduced.

The paper is organized as follows, section 2 introduces related work, and light weight cryptographic algorithm named Humming Bird algorithm in section 3 and section 4 discusses the proposed work, section 5 shows the security analysis and last section deliberates the conclusion.

2 Related work

Password-authenticated key exchange is an authentication method where a client and a server who share a password and verify each other with that password and both will agree on a cryptographic key discussed by Katz et al[13]. Passwords which are required to verify the clients are stored on a particular server. If the server is cooperated, due to some horrible operations like hacking or fixing a Trojan horse, passwords which are stored in the server gets discovered. To overcome this problem, Ford et al proposed the threshold password authenticated key exchange with n servers[14]. Di Raimando et al proposed a protocol[15], which requires 1/3 of the servers to be compromised. Brainard et al developed the first two server protocol with PKI based setting and implemented using the public key techniques such as SSL[16]. Katz et al proposed a KOY protocol with the proof of security[10]. Here two servers cooperate to authenticate a client and if one server is cooperated, the hacker still cannot act as a client with the evidence from the granted server. This protocol was based on Katz-Ostrovsky-Yung protocol called KOY protocol proposed by Katz[17]. In this protocol the client randomly choose a password pwC, and two servers A and B are delivered with random password parts pwC1 and pwC2 where pwC1+pwC2=pwC. At higher level this protocol can be seen as implementation of two KOY protocol, One between client and server A where server B helps for confirmation and one between client and server B where server A helps for confirmation. KOY protocol is symmetric in the sense two servers correspondingly contribute to the authentication and key exchange. This protocol is secure under passive adversaries but everyone roughly performs twice work as KOY protocol. In order to be secure from active attacks the user work remains same but the servers work increases by 2-4 times. The advantage of KOY protocol is its structure and its disadvantage is ineffectiveness of practical use. Subsequently in 2005, Yang et al[18] system built on Brainard et al.[16] work, Yang et al suggested an asymmetric setting, where a service server, interacts with the client and a back-end server called control server. Control

server helps service server with the authentication, and only service server and the client decide on a secret session key in the end. They suggested a PKI based asymmetric two-server PAKE protocol in 2005 and several PAKE protocols has been proposed.

Recently in 2013, Yi et al proposed a two server Password-authenticated key exchange (PAKE) will share a password between the client and two servers for authentication[12]. So it is difficult to hack both the servers because if one server is compromised , the attacker wont pretend to be the client on other server. They proposed a solution for two-server PAKE, where the client found a different cryptographic keys with the two servers and it runs in parallel and is more efficient. In their protocol they have proved $H(K1,1) \bigoplus b1 = H(K1,1) \bigoplus (H(K1,0) \bigoplus h1) = h1$, the server1 accepts the message M6 and computes the secret session key $sk1 = sk1$ because $k1 = k1$. Also they proved that their protocol is secured against the active and passive attacks in case that one of the two servers is compromised.

3 Preliminaries

3.1 PRESENT Algorithm

PRESENT is a lightweight block cipher designed by Bogdanov et al[19], the algorithm is notable for its compact size i.e., 2.5 times smaller than AES algorithm. Light weight algorithms are suitable for constrained environments such as RFID tags, smart cards and sensor networks.

Following pseudocode shows that each of the 31 rounds consists of an XOR operation to familiarize a round key K_i for $1 \leq \ i \leq \ 32$, where K_{32} is used for post-whitening, a linear bit wise permutation and substitution layer. It uses a single 4-bit S-box , which is applied 16 times in parallel in each round.

```
genRoundKeys()
    for i = 1 to 31 do
        ARkey(STATE,K_i)
        sblayer(STATE)
        player(STATE)
    end for
ARKey(STATE,K_32)
```

In applications that claim efficient use of space, the block cipher will be implemented as encryption-only. In this way it can be used for challenge-response authentication protocols, it could be used for both encryption and decryption by using the counter mode. Taking such considerations into account so decided to make present a 64-bit block cipher. It supports both encryption and decryption is smaller than an encryption-only AES and produces an ultra-lightweight solution. The encryption sub keys can be calculated *on-the-fly* .

Differential cryptanalysis. The case of differential cryptanalysis is captured by the following theorem discussed by Biham[20].

Theorem 1. Characteristics that involve 10 Sboxes over 5 rounds. The following two-rounds involves two S-boxes per round and holds with probability 2^{-25} over five rounds.

$$\Delta = 0000000000000011$$
$$\rightarrow 0000000000030003$$
$$\rightarrow 0000000000000011 = \Delta$$

Linear cryptanalysis. The case of the linear cryptanalysis of present algorithm is handled by Wang[21] in the following theorem.

Theorem 2. Let ε_{4R} be the maximal bias of a linear approximation of four rounds of present.Then $\varepsilon_{4R} \leq \frac{1}{2^7}$. The theorem is formally proved in A. Bogdanov1 et al[19] paper, and it is used directly to bound the maximal bias of a 28-round linear approximation by

$$2^6 \times \varepsilon_{4R} = 2^6 \times (2^{-7})^7 = 2^{-43}$$

Therefore a cryptanalyst need only approximate 28 rounds in present to mount a key retrieval attack, linear cryptanalysis of the cipher would require of the order of 284 known plaintext/cipher texts. Such data requirements exceed the available text.

3.2 Humming Bird Algorithm

Hummingbird, which is recently designed by Smith et al[2] is an ultra-lightweight cryptographic basic for encryption and authentication in severely resource-constrained devices like passive RFID tags. It is an elegant combination of a block cipher and stream cipher with a 16-bit block size, 256-bit key size, and 80-bit internal state. The size of the key and the internal state of Hummingbird provide a security level which is adequate for many RFID applications. Moreover, Hummingbird is resistant to the most common attacks to block ciphers and stream ciphers including differential and linear cryptanalysis, structure attacks, algebraic attacks, birthday attacks and cube attacks.

Hummingbird Encryption Process

Differential Cryptanalysis: Here $E_k(x)$ denote the encryption function of Hummingbird with 256-bit key K. Recall that $E_k(x)$, denotes the 16-bit block cipher encryption . Then $E_k(x)$ is the composition of four $E_k(x)$. For a function $F(x)$ from F_2^m to F_2^m, the differential between $F(x)$ and $F(x+a)$, where $+$ is the bit-wise addition by $D_F(a,b)$, is given by

$$D_F(a,b) = |x|F(x) + F(x+a) = b, x\varepsilon F_2^m$$

Engels et al proved that, the differential of $E_k(x)$ has the same upper bound as $E_k(x)$, the block cipher component in EK[22]. They have tested the reduced version of Hummingbird for more instances of different pairs. From those experimental results, the standard differential cryptanalysis method is not valid for

Table 1 Add caption

Algorithm : Encryption Process
Input: A 16-bit plaintext PT_i *and four rotors* $Ri^a(i = 1, 2, 3, 4)$
Output: A 16-bit cipher text CT_i *[Block Encryption]*
1: $V12_a = ESR_1(PT_i + nR1_a)$
2: $V23_a = ESR_2(V12_a + nR2_a)$
3: $V34_a = ESR_3(V23_a + nR3_a)$
4: $CT_i = ESR_4(V34_a + nR4_a)$
[Internal State Updating]
5: $LFSR_{a+1} \leftarrow LFSR_a$
6: $R1_{a+1} = R1_a + nV34_a$
7: $R3_{a+1} = R3_a + nV23_a + nLFSR_{a+1}$
8: $R4_{a+1} = R4_a + nV12t + nR1_{a+1}$
9: $R2_{a+1} = R2_a + nV12t + nR4_{a+1}$
10:return CT_i

Hummingbird with time complexity.

Linear Cryptanalysis: For the linear cryptanalysis of $E_k(x)$, consider $|E_k(a, b)|$, the absolute value of the Walsh transform of $E_k(x)$, where

$$E_k(a, b) = \Sigma_{x \in F_2^{16}} - 1^{<a, E_k(x)><b, x>}, a, b \in F_2^{16}, a \neq 0$$

where $< x, y >$ is the inner product of two binary vectors x and y. The absolute value of the Walsh transform of encryption function could be limited by the square root of 2^{16}. So, Hummingbird is resistant to linear cryptanalysis attack in IOT applications.

4 Novel Protocol for Two-server Password only Authentication

In this work , used two different light weight cryptographic algorithms for encrypting the passwords in two servers. Algorithms such as PRESENT and Humming Bird help to encrypt the password and store it in the servers. Two servers jointly work to authenticate the client and offer services proposed by Yang et al[23]. Client broadcast the message to both the servers , the servers cooperate to authenticate the password. Our protocol uses two different algorithms so it will be very hard for the attacker to break because even if one of the servers is compromised its very difficult to hack the other one. Our model used more efficient algorithm which is specially designed for the resource constraint devices when compared to the other. The protocol runs mainly in three stages Initialization, Registration and Authentication. Fig.1 explains the working process of password authentication.

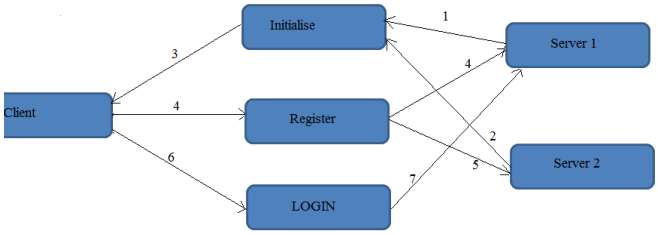

Fig. 1 Working process of proposed work

1. Server1 initialises runs PRESENT and sends its secret key of server1 to client.
2. Server2 initialises runs Humming Bird and sends its secret key of server2 to client.
3. Server1s secret key and sever2s secret key are received by client.
4. Client Registers to server1 and sends information after encrypting using secret key of respective server to respective server. The password is separated and sent to server1 and server2.
5. Id and pwd1 is sent to server1.
6. Id and pwd2 is sent to server2.
7. User logins to server1 with his registered id and password.
8. Server1 and server2 communicates each other and server2 receives the full password and compares with user entered password. Returns success if password matches else returns FAILURE.

4.1 Initialization

The server then performs the following operations.

1. The server1 S1 generates the secret key according to PRESENT algorithm.
2. The server2 S2 generates secret key according to Humming Bird algorithm.

4.2 Registration

Before authentication, each client C is essential to register to both S1 and S2 through different channels. First of all, the client C accesses the secret key of both servers S1 and S2. Next, the client C picks a password pwC and encrypts the password using the secret key. After that, the client C recalls the password pwC. The two secure channels are essential for all two server PAKE protocols, where a password is encrypted by means of two different secret keys, which are safely broadcasted to the two servers, during registration. Although, the idea of private key cryptosystem, the encryption key of one server should be unfamiliar

to another server and the client needs to memorize the secret code or password just behind registration. The two servers S1 and S2 have settled on the password confirmation information of the client C during registration. The id of each client has to be unique.

4.3 Authentication/Login

1. The client C broadcast a request message M1 to the s1 server. The message includes the authentication information of the client and a nonce.

2. The two servers exchange messages M2 and M3 based on the authentication information gathered during the registration phase.

3. Now if the client is genuine (based on password check) then the client is allowed to have access. Else the request for login is denied.

Advantage is to achieve better performance because parallelism is used and it prevents replay attack because of nonce.

4.4 Encryption

1.Here the plain text is the password which is divided as per the two-server password only authentication and according to novel architecture each half of the passwords are encrypted by client using PRESENT and Humming Bird.

2.But the change here is the password are not sent to same receiver but are sent to different servers and they use different algorithms namely PRESENT and Humming Bird. The detailed process of encryption is illustrated in Fig.2.

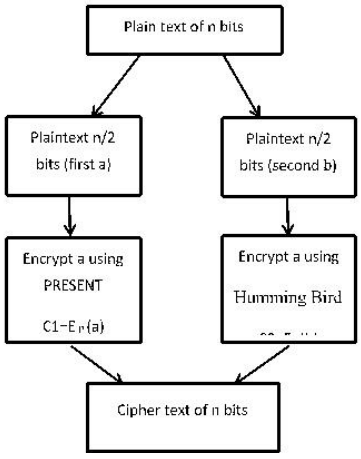

Fig. 2 Encryption Process

4.5 Decryption

Here the two parts of plain text are sent to different servers which use PRESENT and Humming Bird algorithms and these receive the respective plain text and decrypt them using PRESENT and Humming Bird. The two parts of plain text are merged only during LOGIN phase. The detailed process of decryption is illustrated in Fig.3.

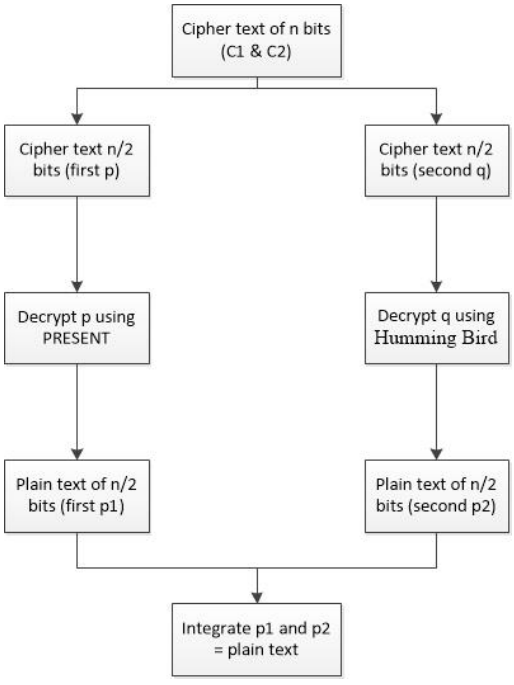

Fig. 3 Decryption Process

5 Security Analysis

5.1 Smart Card Loss Attack

Suppose if the customer lost his/ her smart card, by accessing the storage medium the attacker can try to access the data. Then the attacker may try to use this information to login to the server. In out model its very hard to hack the password because passwords are divided and stored in two different servers. Our protocol is against to smart card loss attack.

5.2 DOS Attack

Suppose an attacker has stolen the smartcard, and the attacker try to update the information. In that case our model is not vulnerable to the attacker because two different algorithms have been used. Even if one server is compromised the other server wont respond. Smart card will be logged if it exceeds the number of login attempt limit. Therefore out protocol can withstand DOS attack.

5.3 Forgery Attack

The attacker cannot create legal login request and cannot act as an authorized user, because without knowing the users password the attacker has no way to get the exact value.

6 Conclusion

This project presents a novel protocol for Two Server Password Only Authentication. This protocol is secure against many attacks in case if one of the servers is compromised still the intruder will not be able to gain access to the password because only half of the password will be revealed. The performance is also efficient because of the parallel computation. Therefore, our scheme is more suitable, particularly for applications which need enhanced security in the IOT environment since making use of efficient light weight cryptographic algorithm.

References

[1] T. Eisenbarth, S. Kumar, C. Paar, A. Poschmann, A. and Uhsadel, L. (2007), "A survey of lightweight-cryptography implementations", *IEEE Design & Test of Computers*, (6), 522-533.

[2] Atzori, Luigi, Antonio Iera and Giacomo Morabito. (2010),"The internet of things: A survey", *Computer networks*, 54.15, pp. 2787-2805.

[3] Burande, N. and Gumaste, S. V. (2013), "Survey on public key encryption for two server password only authenticated key exchange", Available at *http://www.schneier.com/blog/archives/2006/12/ realworld_passw.html.*

[4] Gong, L., Lomas, M., Needham, R. M. and Saltzer, J. H. (1993), "Protecting poorly chosen secrets from guessing attacks", *Selected Areas in Communications*,IEEE Journal on, 11(5), 648-656.

[5] Bellovin, S. M. and Merritt, M. (1992), "Encrypted key exchange: Password-based protocols secure against dictionary attacks", *In Research in Security and Privacy, Proceedings*, 1992 IEEE Computer Society Symposium , pp. 72-84.

[6] Halevi, Shai and Hugo Krawczyk. (1999), "Public-key cryptography and password protocols", *ACM Transactions on Information and System Security (TISSEC) 2.3*, pp. 230-268.

[7] M. Bellare, D. Pointcheval and P. Rogaway. (2000), "Authenticated key exchange secure against dictionary attacks", *Proc. 19th Intl Conf.Theory and Application of Cryptographic Techniques (Eurocrypt 00)*, pp. 139-155.

[8] V. Boyko, P. Mackenzie and S. Patel. (2000), "Provably secure password-authenticated key exchange using diffie-hellman", *Proc. 19thIntl Conf. Theory and Application of Cryptographic Techniques(Eurocrypt 00)*, pp. 156-171.

[9] Yang, Y. and Bao, F. (2010), "Enabling use of single password over multiple servers in two-server model", *IEEE 10th International Conference on In Computer and Information Technology (CIT), 2010*, Vol.34, pp. 846-850.

[10] Katz, P. MacKenzie, G. Taban and V. Gligor,(2005), "Two-server password-only authenticated key exchange", *roc. Applied Cryptography and Network Security (ACNS 05)*, pp. 1-16.

[11] Goldreich, O. and Lindell, Y. (2001), "Ession-key generation using human passwords only", *In Advances in Cryptology-CRYPTO 2001*, pp. 408-432.

[12] Yi, Xun, San Ling and Huaxiong Wang. (2013), "Efficient two-server password-only authenticated key exchange.", *IEEE Transactions on Parallel and Distributed Systems*, 24.9,pp. 1773-1782.

[13] Katz, J. and Yung, M. (2007), "Scalable protocols for authenticated group key exchange", *Journal of Cryptology, 20(1)*, Vol.18, pp. 85-113.

[14] Ford, W. and Kaliski Jr, B. S. (2000), " Server-assisted generation of a strong secret from a password", *In Enabling Technologies: Infrastructure for Collaborative Enterprises, 2000.(WET ICE 2000). Procedings*, IEEE 9th International Workshops, pp. 176-180.

[15] M. Di Raimondo and R. Gennaro. (2003), "Provably secure threshold password authenticated key exchange", *Proc. 22nd Intl Conf.Theory and Applications of Cryptographic Techniques (Eurocrypt 03)*, pp. 507-523.

[16] Brainard, J. G., Juels, A., Kaliski, B. and Szydlo, M. (2003), "Ultra-lightweight cryptography for low-cost rfid tags: hummingbird algorithm and protocol, a new two-server approach for authentication with short secrets",*In USENIX Security*, Vol.3, pp. 201-214.

[17] Jonath Katz, Philip MacKenzie, Gelareh Taban and Virgil Gligor. (2005), *Two-Server Password only Authenticated Key Exchange*, Springer, pp. 1-16.

[18] Y. Yang, F. Bao and R.H. Deng,(2005), "A new architecture for authentication and key exchange using password for federated enterprise", *Proc. 20th IFIP Intl Information Security Conf. (SEC05)*, pp. 95-111.

[19] A. Bogdanov, L. R. Knudsen, G. Leander, C. Paar, A. Poschmann, M. J. B. Robshaw, Y. Seurin and C. Vikkelsoe (2007), "PRESENT - An Ultra Lightweight Block Cipher", *Proc. CHES, Springer*, pp. 450-453.

[20] Biham, E. (1994),"New types of cryptanalytic attacks using related keys", *Journal of Cryptology*, 7(4), 229-246.

[21] M.Wang(2007), "Differential cryptanalysis of PRESENT", *Proc .CHES*, pp. 1-4.

[22] Engels, X. Fan, G. Gong, H. Hu and E. M. Smith (2009), "Ultra-lightweight cryptography for low-cost rfid tags: hummingbird algorithm and protocol", *Centre for Applied Cryptographic Research (CACR) Technical Reports CACR.*

[23] Y. Yang, R.H. Deng and F. Bao (2006), "A practical password-based two-server authentication and key exchange system", *IEEE Trans. Dependable and Secure Computing*, Vol. 3, No. 2, pp. 105-114.

Corresponding author

Vanitha M can be contacted at: mvanitha@vit.ac.in.