Multi-Factor Authenticated Key Exchange Scheme for Mobile Communications using Applied Cryptography

[1]Azhagarasan. T [2]Jeeva. V [3]Nareen Kumar. S [4]Anand N
[1,2,3]UG Scholar [4]Assitant Professor
[1,2,3,4]Department of Computer Science and Engineering
[1,2,3,4]P. A. College of Engineering and Tech, Pollachi, India

Abstract

Authenticated key exchange is one of the most important applications in applied cryptography, the user interacts with a server to set up a session key to pre-registered information, authentication factor, like password or biometrics of the user is stored. Single-factor AKE is widely used in practice. Higher security concerns call for MFAKE schemes, e.g. combining passwords, biometrics and device simultaneously. Casually designed schemes, security is even weakened in the sense that leakage of one authentication factor will defeat the whole MFAKE protocol. An inevitable by-product arises that the usability of the protocol often drops greatly. To summarize, the existing multi-factor protocols did not provide enough security and efficiency simultaneously. It proposes a very efficient MFAKE protocol. It defines the security model and gives the according to security analysis. It also implements our proposed method as textual, graphical, biometric and device password to access the user accounts. The theoretic comparisons and the experimental results show that this scheme achieves both security and usability operating conditions is demonstrated through simulation results using MATLAB/Simulink followed by an experimental validation.

Keyword- AKE, MFAKE Protocol, AKE, Cryptography

I. Introduction

User authentication is a very important part for many information systems. In practice, it is often done via the following methods:

A. Password-Based Authentication

Is the most popular way, quite insecure in some cases. E.g., in the Worst Password List compiled by Splash Data [1], among 3.3 million passwords used for test, almost 20,000 were in fact ”123456”. The statistics show that most passwords in use are not so hard to guess.

B. Hardware-Based Authentication

With storage space for long secret keys and computation power for authentication, hardware provides higher security than password. But if it was stolen or lost, usually happens in daily life occasionally, the authentication fails completely.

C. Biometrics-Based Authentication

Utilizes the unique and life-long invariant property of the biometrics. But it is not so reliable, e.g., biometric characteristics such as fingerprint can be easily “copied” without the awareness of the owner.

II. Challenges

Single-factor authentication only provides limited security, then combining many methods together is considered as a good way to achieve higher security. Many multi-factor authentication schemes are quite insecure.

This again raised the need for secure multi-factor authentication schemes. There are several issues should be addressed by multi-factor authentication schemes:

A. Efficiency

Complex protocol design should be avoided, it may cause expensive computation and communication costs. In practice, a device with high computation power is usually not cheap, and heavy bandwidth occupation due to authentication will make an information system unsalable, and vulnerable to DOS attacks.

B. Robustness

There is one factor uncorrupted, the authentication scheme should remain secure, it is a basic security requirement for multi-factor authentication. But many existing schemes could not meet it: e.g., using redundant authentication, even worse, introducing more weakness.

C. Privacy

Biometric characteristics are acknowledged as one kind of private information it must be protected to avoid leakage. In addition, the leakage of biometric will not only break the security in the authentication and it can lead to further social damage.

D. Session Key Agreement

Authentication is just a way to prevent illegal users from entering a system. The subsequent communications also need to be protected. So, it is ideal to set up a session key between the client and server by the end of an authentication.

E. Usability

The participation of people requires the authentication schemes be friendly to use: e.g., most people cannot remember long and random passwords, and hate to carry many different devices, even taking long and random enough passwords and more different devices can improve the security.

III. EXISTING SYSTEM

Textual passwords are commonly used in existing systems. Users do not follow their requirements. Users tend to choose meaningful words from dictionaries, it makes textual passwords easy to break and vulnerable to dictionary or brute force attacks. The authentication scheme has its disadvantages based on several factors such as consistency, uniqueness and acceptability. One of the main drawbacks of applying is its intrusiveness upon a user’s personal characteristic. This schemes require the user to willingly subject there to a low-intensity infrared light. Systems require a special scanning device to authenticate users, which is not applicable for remote and Internet users.

Single-factor authentication only provides limited security, then combining together is considered as a good way to achieve higher security. For SMS-based two-factor authentication was widely adopted and has been used in many applications, e.g., Gmail. It dominates the research of authenticated key exchange AKE protocols for a long time. Among different factors, password was preferred. The first password-only authenticated key exchange protocol, encrypted key exchange the client shares a plaintext password with the server and exchanges encrypted information.

The limited human memory and the increasing attacker ability have made PAKEs less secure than expected. The protocol designers chose to add other authentication factors to improve security. Many two-factor AKE protocols as well as multi-factor AKE protocols have been proposed.

The computation cost of the client and server, are comparatively inefficient among all schemes, the key reason for which is that both of them authenticate biometric templates bit by bit. The communication traffics of them are also relative higher than others. FMA works by executing a series of sub-protocols. Some of them can be executed parallel, the overall round complexity keeps high.

Two ways are used for biometric matching: Direct matching, comparing two templates bit by bit, as far as the total number of different bits is lower than a threshold, the two templates are considered to be matched.

Fuzzy extractor, only matched templates can reproduce same randomness. Fuzzy extractor to avoid the heavy computation and communication costs of direct matching. For privacy protection, the choice seems to be right, because adversaries may reconstruct a valid templates bit by bit from a complete transcript.

A. Limitations

1) Less security
2) Less efficiency
3) The Authentications are one or two factors are applied.
4) Session Key not applied.

- Use a zero before decimal points: “0.25,” not “.25.” Use “cm3,” not “cc.” (bullet list)

IV. PROPOSED SYSTEM

A. Graphical Password

The Multifactor Authentication scheme has been proposed, Users tend to resist using biometrics because of intrusiveness and the effect on their privacy and the hardware also USB devices. Graphical passwords are based on the idea that users can recall and recognize pictures better than words. Graphical password schemes require a long time to be performed. Present and evaluate our contribution, Multifactor authentication scheme. To be authenticated, it presents a 3-D virtual environment where the user navigates and interacts with various objects. The sequence of actions and interactions toward the objects inside the 3-D environment constructs the user's graphical password. The 3-D password can combine most existing authentication schemes such as textual passwords, graphical passwords, device passwords and various types of biometrics into a 3-D virtual environment. The design of the 3-D virtual environment and the type of objects selected determine the graphical password key space.

1) Advantages

1) High security.
2) Multifactor Authentication like, textual, graphical, biometric and USB device passwords.
3) The data can be exchanged to the receiver using session keys.
4) Robustness.
5) High Privacy.
6) Usability.

B. Algorithm

1) Triple DES Algorithm

Triple des uses a "key bundle" that comprises three des keys, k_1, $k_2$and k_3, each of 56 bits (excluding parity bits). The encryption algorithm is: cipher text = $e_{k3}(d_{k2}(e_{k1}(\text{plaintext})))$ i.e., des encrypt with k_1, des decrypt with k_2, then des encrypt with k_3. The decryption algorithm is: plaintext = $d_{k1}(e_{k2}(d_{k3}(\text{cipher text})))$. The following are step by step process.

Step 1: create 16 sub keys, each of which is 48-bits long.

The 64-bit key is permuted according to the following table, PC-1. Since the first entry in the table is "57", this means that the 57th bit of the original key K becomes the first bit of the permuted key K+. The 49th bit of the original key becomes the second bit of the permuted key. The 4th bit of the original key is the last bit of the permuted key. Note only 56 bits of the original key appear in the permuted key.

PC-1

57	49	41	33	25	17	9
1	58	50	42	34	26	18
10	2	59	51	43	35	27
19	11	3	60	52	44	36
63	55	47	39	31	23	15
7	62	54	46	38	30	22
14	6	61	53	45	37	29
21	13	5	28	20	12	4

From the original 64-bit key

K = 00010011 00110100 01010111 01111001 10011011 10111100 11011111 11110001

we get the 56-bit permutation

K+ = 1111000 0110011 0010101 0101111 0101010 1011001 1001111 0001111

Step 2: Encode each 64-bit block of data.

An initial permutation IP of the 64 bits of the message data m. This rearranges the bits according to the following table, where the entries in the table show the new arrangement of the bits from their initial order. The 58th bit of m becomes the first bit of IP. The 50th bit of m becomes the second bit of IP. The 7th bit of is the last bit of IP address.

Applying the initial permutation to the block of text M, given previously, we get

M = 0000 0001 0010 0011 0100 0101 0110 0111 1000 1001 1010 1011 1100 1101 1110 1111

IP = 1100 1100 0000 0000 1100 1100 1111 1111 1111 0000 1010 1010 1111 0000 1010 1010

Here the 58th bit of M is "1", which becomes the first bit of IP. The 50th bit of M is "1", which becomes the second bit of IP. The 7th bit of M is "0", which becomes the last bit of IP.

Next divide the permuted block IP into a left half L_0 of 32 bits, and a right half R_0 of 32 bits.

We now proceed through 16 iterations, for 1<=n<=16, using a function f which operates on two blocks--a data block of 32 bits and a key K_n of 48 bits--to produce a block of 32 bits. Let + denote XOR addition, (bit-by-bit addition modulo 2). Then for n going from 1 to 16, we calculate

$L_n = R_{n-1}$

$R_n = L_{n-1} + f(R_{n-1},K_n)$

Step 3: DES Modes of Operation

Triple ECB (Electronic Code Book)

1) This variant of Triple DES works exactly the same way as the ECB mode of DES.
2) This is the most commonly used mode of operation.

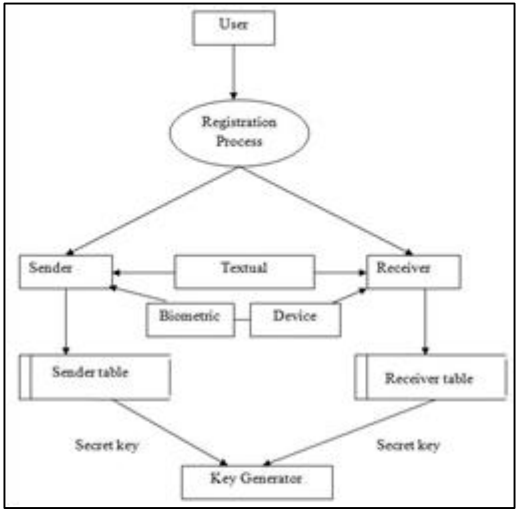
Triple CBC (Cipher Block Chaining)

1) This method is very similar to the standard DES CBC mode.
2) As with Triple ECB, the effective key length is 168 bits and keys are used in the same manner, as described above, but the chaining features of CBC mode are also employed.
3) The first 64-bit key acts as the Initialization Vector to DES.

4) Triple ECB is then executed for a single 64-bit block of plaintext.
5) The resulting cipher text is then XORed with the next plaintext block to be encrypted, and the procedure is repeated.

C. Data Flow Diagram

In Figure 1 is clearly shown the data to be registered from both the sender and receiver and then log in to their data for data transfer and about the session key and graphical password generation for both the users and then they verify their credentials. The data to selected and encrypted then it can be transferred to the receiver and it can be decrypted to see data.



V. CONCLUSION AND FUTURE SCOPE

A. Conclusion

The security model for multi-factor authenticated key exchange protocol that allows a significant amount of information leakage for the adversary. It formally proved the security and robustness of our scheme in the model, as long as one authentication factor remains unknown, the adversary cannot have any information regarding the agreed session key, and cannot impersonate a client or a server. It also implemented the scheme with practical parameters on a smartphone, and the results have shown that our scheme is highly efficient.

B. Future Scope

Nothing will be useful until it is updated and enhanced timely just like IT field. The software can have more future enhancement such as file storage used in this method is limited. And also the security level can enhance by sending OTP to the users, iris scanner it can be enhanced according to the client user-friendliness.

REFERENCES

[1] Arakala, A. and Jeffers, J. and Horadam, K. "Fuzzy Extractors for Minutiae-Based Fingerprint Authentication," in ICB, ser. Lecture Notes in Computer Science, vol. 4642, 2007, pp. 760–769.
[2] Bellare,v and Piontcheval,D. and Rogaway,P. "Authenticated Key Exchange Secure Against Dictionary Attacks," in EUROCRYPT,ser. Lecture Notes in Computer Science, vol. 1087, 2000, pp. 139–155.
[3] Bellovin,S. and Merritt,M. "Encrypted Key Exchange: Password-Based Protocols Secure Against Dictionary Attacks," in IEEE S&P, 1992, pp. 72–44.
[4] Bellovin,S. M. and Merritt,M. "Augmented Encrypted Key Exchange: A Password based protocol secure against dictionaryattacks and Password File Compromise," in ACM CCS, 1993, pp.244–250.
[5] Boyko,V. and MacKenzie,P. and Patel,S. "Provably Secure Password-Authenticated Key Exchange Using Diffie-Hellman," in EUROCRYPT, 2000, pp. 156–171.
[6] Gennaro,R. and Lindell,Y. "A Framework for Password-based Authenticated Key Exchange," ACM Transactions on Informationand System Security, vol. 2, no. 9, pp. 181–234, 2006.
[7] Goldreich,O. and Lindell,Y. "Session-key generation using human passwords only," in CRYPTO, 2001, pp. 408–432.
[8] Groce,A. and Katz,J. "A New Framework for Efficient Password-Based Authenticated Key Exchange," in ACM CCS, 2010, pp. 516–525.
[9] He, D. and Kumar, N. and Lee, J.-H. and Sherratt, R. S. "Enhanced Three-Factor Security Protocol for Consumer USB Mass Storage Devices," IEEE Transactions on Consumer Electronics, vol. 60, no. 1, pp.30–37, 2014.

[10] Huang, X. and Xiang,Y. and Bertino, E. and Zhou, J. and Xu,L.“Robust Multi-Factor Authentication for Fragile Communications,” IEEETransactions on Dependable and Secure Computing, vol. 6, no. 11, pp.568–581, 2014.

[11] Juang,W. and Wu,J. “Two Efficient Two-Factor Authenticated Key Exchange Protocols in Public Wireless LANs,” Computers &Electrical Engineering, vol. 35, no. 1, pp. 33–40, 2009.

[12] Lee,C. C. and Chen,C. T. and Wu,P. H. and Chen, T. Y. “Three-Factor Control Protocol Based on Elliptic Curve Cryptosystem for UniversalSerial Bus Mass Storage Devices,” IET, vol. 7, no. 1, pp. 48–55,2013.

[13] Park,Y. M. and Park,S. K. “Two Factor Authenticated Key Exchange (TAKE) Protocol in Public Wireless LANs,” in IEICE Transon Communications, vol. E87-B, no. 5, 2004, pp. 1382–1385.

[14] Pointcheval,D. and Zimmer,S. “Multi-Factor Authenticated Key Exchange,” in ANCS, ser. Lecture Notes in Computer Science, vol.5037, 2008, pp. 277–295.

[15] Slain,M. “Announcing Our Worst Passwords of2015,”https://www.teamsid.com/worst-passwords-2015/, 2015.

[16] Wang,X. and Zhang,W. and Zhang,J. and Khan,M K. “Cryptanalysis and Improvement on Two Efficient Remote User Authentication Scheme Using Smart Cards,” Computer Standards & Interfaces,vol. 29, no. 5, pp. 507–512, 2007.