Encrypted Fingerprint into VoIP Systems using Cryptographic Key Generated by Minutiae Points

[1]Mohammad Fawaz Anagreh
Department of Computer and Self Development, Prince
Sattam Bin Abdulaziz University,
Kharj, KSA

[2]Anwer Mustafa Hilal
Department of Computer and Self Development, Prince
Sattam Bin Abdulaziz University, KSA Kharj, KSA
Faculty of Computer Science and Information Technology,
Omdurman Islamic University, Khartoum, Sudan

[3]Tarig Mohamed Ahmed
Department of MIS, Prince Sattam Bin Abdulaziz University,
KSA, Kharj, KSA, Department of Computer Sciences,
University of Khartoum, Khartoum, Sudan

***Abstract*—The transmission of the encryption voice over IP is challenging. The voice is recorded, eavesdropping, change and theft voice, etc. The voice over IP is encrypted by using Advance Encryption Standard (AES) Algorithm. AES key is generated from Minutiae Points in fingerprint. By other way, we talk about biometric-cryptosystem, which is hybrid between one of the cryptosystems and biometric systems, such as fingerprint using for authentication as well as to generate cryptographic key to encrypt voice over IP by applying AES. In this paper, we define a new term which is Fingerprint Distribution Problem (FDP) based on Key Distribution Problem. Also, we suggest a solution for this problem by encrypted fingerprint before sending between users by using one of the public key cryptosystems which is RSA Algorithm.**

Keywords—IP; cryptography; fingerprint; minutiae Advance Encryption Standard (AES); RSA; information security

I. INTRODUCTION

Now a day, the computer networks allow sending different types of data via communication channels which connected with each other, audio, voice, text and video are different examples of data. Almost types before sending via communication channel will converted to the bits encapsulated in the packets. Voice over internet protocol *(VoIP)* is a generally term for a many transmission technologies to deliver voice over internet protocol *(IP)* using applications designed for this purpose [8], [11], VoIP should be known as IP Telephony also Voice over IP protocols carry telephony signals as digital audio.

Deliver voice over IP commonly used between massive numbers of users around of the world, but the problems are begin when attacker eavesdropping calls between users by attack communication channel, to avoid these problems many of researchers suggested solutions for this shortcoming by encrypt the voice before deliver via communication channels, one of these solutions is a system which encrypt the VoIP data packets using Advanced Encryption Standard *(AES)*, AES key is extracted from minutiae points from fingerprint authentication. There are some of shortcomings demonstrate when apply this technology, the main shortcoming is when send the fingerprint between users via unsecure communication channel because these fingerprint is not just for authentication but it will be used to generate key for AES algorithm [1], [2].

In this paper we suggest solution for this shortcoming. The rest of the paper is organized as follows: Section 2 provides a brief introduction to VoIP and its security vulnerabilities. As well as it provides a brief introduction to AES and RSA Algorithms also a brief Cryptographic Key Generated from Biometrics. Section 3 describes what the Fingerprint Distribution Problem is. Section 4 presents a solution for the fingerprint distribution Problem. Section 5 is the conclusion for our work.

II. RELATED WORK

A. VoIP Security Vulnerabilities

Internet Protocol Version 6 (IPv6) has been reached to become internet protocol for next generation. Especially that IPv6 consist of more updated compared with IPv4 in terms, number of new IP addresses (2^{128}). As well as add more improvements in area specially, IPv6 support a new mechanism which called flow label that allows to support traffic such as real-time audio and video, more than in IPv4, Support for more security about encryption and authentication options and a new options for additional functionalities [11]. Problems at voice over IP are more and different, we can divide the problems into two categories based on situation of occurred. The first one is threats to the network; the second is threats to end users. Voice over IP is converted to the packets before send to other users in the network by communications channels, the problems here if the data unencrypted, then anyone can access to the data when sending between sender and receiver. Therefore, the attackers can listen to the calls and they can record the conversation [8].

B. RSA and AES Algorithms

Encryption is one of security technology for computer, Encryption is based on transformation data or messages from original status called plaintext to a new status called cipher text, the features of a new status are unreadable for anyone except those possessing special knowledge, which are encryption algorithm and secret key. Decryption is the conversion cipher text into original status (plaintext), and also nobody can convert that just who has possessing secret key and encryption algorithm. There are two essentially types for encryption based on keys, the first one is public key cryptosystem which have two keys (public and private), public key is used to encryption, the private key is used for decryption. The other type is a private key cryptosystem, which have one key used for both encryption and decryption.

AES Algorithm: Is a block cipher. Advance Encryption Standard (AES) was established in 2001 by the National Institute of standards and Technology as a development on DES, AES takes a fixed data block size of 128 bits and unfixed key size of 128 bits, 192 bits or 256 bits. In encryption phase, AES depend on round transformation from plaintext to cipher text, number of rounds depend on key length. If the key is 128 bits then uses 10 rounds, 192 bits uses 12 rounds and 256 uses 14 round. The stages of all rounds are Sub Bytes, Shift Rows, Mix Columns and Add Round Key [7].

RSA Algorithm: Is a first published by the three researchers Ron Rivest, Adi Shamir and Len Adleman in 1977 [12].The name of algorithm came from the initials of surnames for the researchers. However, the RSA Algorithm using both digital signature and public key encryption, as any algorithm in this filed, RSA consist of two keys, the public key is used for encryption and private key for decryption.

RSA algorithm consists into three phases: key generation phase, encryption and decryption phases. The user of RSA applies the key generation phases to generate keys based on two big prime numbers. The prime number must be kept secret, then apply other steps in key generation phase to get the keys of RSA. As a rest of public key cryptosystems, any one has the public key can encrypt the plain text to get the cipher text, then send the cipher text to the user who generated keys to decrypt the cipher text to get the plain text. The first user (generator keys) transmit his public key *(n, e)* to the second user via communication channel, the private key d is never distributed any way. Suppose Bob (first user) would like to send massages (Palin text) *M* to the Alice (second user), Bob converts the Plain text *M* to the cipher text using Public key of Alice *e* according to the equation:

$$C = M^{e} \bmod n$$

After get *C*, Bob send the encrypted message C to the Alice. While Alice received the Cipher text *C*, She decrypts the cipher text *C* to get the Plain text *M* by using her private key exponent *d* according to the following equation:

$$M = C^{d} \bmod n$$

To generate the public and private keys of RSA algorithm by apply following steps:

- *Select two prime numbers p, q*
- *Compute* $n = p*q$
- Calculate $\varphi = (p-1)*(q-1)$
- Choose an integer number *e*, by $1 < e < \varphi,\ \gcd(e, \varphi)=1$
- *Compute d, by* $1 < d < \varphi,\ e*d = (1 \bmod \varphi)$
- Obtain the keys, Public key *(n, e)*, Private key *(d, p, q)*

The key length of RSA is referring to the modules n, it is now 1024 bits, 2048 bits or more. Key length with 512 bits is now no longer recommended secure. Therefore, the recommendation is to generate two big numbers p and q to insure a big modules number n. Key length with 1024 bits is a round 300 decimal digits as following example:

n=778777413433370950905552740560125564964460406966152750369852448195494305685115033383631595703771562029730000000770846689961510892212245457118060578888989517080042203063427376322274266393116193517839570773505455203096681121927337473973220312512599024851322250606006260066557538238517575390621262920956913963

Generate n above is composed of two big random prime numbers p and q:

P=4455716611517208830668471547999846502234541387456711212734562876700082258431302965521274970245344793522942129064489358577701861556582847914646983 63257581748

q=86149226453543817609370608821417489933942998101549682098342251385596444849727109106169673491102317237340789760111790217082898243965534121805148279973690446

III. Cryptographic Key Generated from Biometrics

The secret key generated from biometric is common used recently, easy to generate and no need to remember the strong secret key. As well as, key is a big size cause difficult for some people to manage the cryptographic key [5], [9]. Recently, many proposals have been suggested many methods to generate cryptographic key based on biometric such as fingerprint [3]-[5], [10], [13]-[15]. According to (Arul and Shanmugam), they selected fingerprint as the biometrics features to generate a cryptographic key, that can be done by extract minutiae points from the finger print. The group of points are managed together by some methods into seven phases to generate the cryptographic key of AES Algorithm.

A. Fingerprint Distribution Problem (FDP)

In this section, will assume two person, Alice as Sender and Bob as recipient. Suppose, Alice wants to begin calling Bob, the voice is delivering over internet protocol.

Assumptions

$\text{FP\_}_{\text{Alice}}$ → Alice Fingerprint
$\text{K\_}_{\text{Alice-Bob}}$ → AES key for both Alice and Bob
$\text{P\_}_{\text{Alice-voice}}$ → Original Voice Packets-Alic
$\text{C\_}_{\text{Ciphervoice}}$ → Cipher Voice Packets-Alice

G→ Generate AES Key from Minutiae Points in Fingerprint
E→ Encryption
D→ Decryption

Step 1: Alice send fingerprint to the Bob via communication channel.

Step 2: Bob receive the fingerprint from Alice and will compare automatically with fingerprints stored in database of Bob. When fingerprints are same authentications is done.

Step 3: Alice Generates AES Key from fingerprint by apply Arul and Shanmugam method [1] as denoted:

FP_Alice → G (K_Alice-Bob)

Step 4: Alice encrypts the voice packets using AES algorithm by use AES Key generated from minutiae points in Alice fingerprint as denoted:

$\mathbf{C}\_{}_{\text{Ciphervoice} =} \mathbf{E}\ \mathbf{(}P\_{}_{\text{Alice-voice}}\mathbf{)}$ by using $K\_{}_{\text{Alice-Bob}}$

Next, Alice sends the cipher voice to the Bob.

Step 5: Bob Generates AES Key from fingerprint by apply Arul and Shanmugam method as denoted:

FP_Alice → G (K_Alice-Bob)

Step 6: Bob decrypts the cipher voice using AES algorithm by use AES Key generated from minutiae points in Alice fingerprint as denoted:

P_Alice-voice = D (C_Ciphervoice) by using K_Alice-Bob

Bob will apply last steps before begin send voice over IP. According to steps above, we can summarize and detect some things. No need to generate key as a statically because the key automatically generated. As well as, there is no need to store the key because fingerprint generates AES key when needed. Consequently, we consider that as a solution for the key distribution problems because there is no need to send key via communication channel.

Both sender and recipient use the fingerprint to generate AES key for both encryption and decryption. AES key generated from minutiae points from fingerprint. By other way, the purpose of fingerprint is to generate cryptographic key and for authentication. The fingerprint should be saved in database for both sender and recipient for authentication purpose also to generate key for encryption\decryption voice before\after deliver over IP. Consequently, if attacker gets the fingerprint, he can generate the AES key by apply the same algorithm (see Fig. 1), here a new problem incoming, deliver fingerprint in unsecure communication channel allows attacker to exploit fingerprint to generate key by apply same algorithm like look sender or receiver. By other word, sending fingerprint in unsecure communication channel is similar to send a private key, then attacker can generate key and decrypt the cipher voice over IP. Here, we name a new term, which is a Fingerprint Distribution Problem (FDP).

To solve the Fingerprint Distribution Problem, we suggested encrypt fingerprint before sending between users also keep the fingerprint encrypted in the database. We solve FDP by using public key cryptosystem because this technique was proposed to solve key distribution problem, we mentioned that a sending fingerprint in the unsecured communication channel is same a key distribution problem.

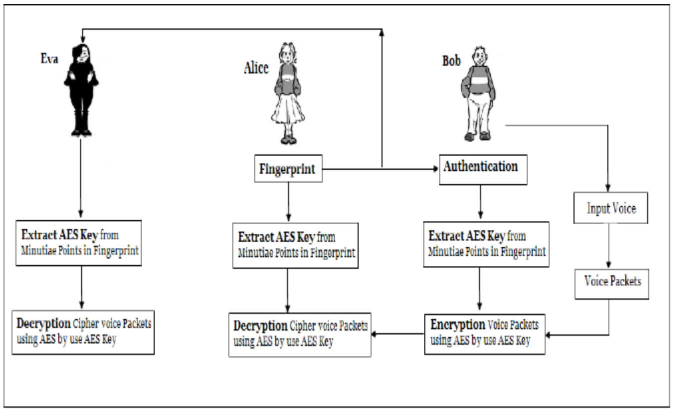
Eva
Alice
Bob
Fingerprint
Authentication
Input Voice
Voice Packets
Extract AES Key from Minutiae Points in Fingerprint
Extract AES Key from Minutiae Points in Fingerprint
Extract AES Key from Minutiae Points in Fingerprint
Decryption Cipher voice Packets using AES by use AES Key
Decryption Cipher voice Packets using AES by use AES Key
Encryption Voice Packets using AES by use AES Key

Fig. 1. Fingerprint distribution problem.

B. Preposed Solution of Fingerprint Distribution Problem

Public key cryptography was invented in 1976 by Diffie and Hillman [6], the main goal of public key cryptography is to solve Key Distribution Problem that obtain a protocol to pass the public key and ciphertext between users in communication channel and use private key for decryption, we solve the fingerprints distribution problem by encrypt the fingerprint before sending via unsecure communication channel. We use RSA Algorithm as a one of public key cryptography (see Fig. 2). Sending fingerprint in unsecure communication channel is as send private key to the other user because attacker can extract the AES key from fingerprint by apply the algorithm to extract Minutiae Points from fingerprint. Assume two users Bob and Alice as following steps:

Assumptions

K_{e_Bob}→ Public key for Bob generated by apply RSA algorithm
K_{d_Bob}→ Private Key for Bob generated by apply RSA algorithm
K_{e_Alice}→ Public key for Alice generated by apply RSA algorithm
K_{d_Alice}→ private key for Alice generated by apply RSA algorithm
$C\_{}_{\text{Cipherfingerprin-Alice}}$→ Encrypt Alice fingerprint by apply RSA algorithm using Bob public key
$C\_{}_{\text{Cipherfingerprint-Bob}}$→ Encrypt Bob fingerprint by apply RSA algorithm using Alice public key

Step 1: Alice and Bob generate keys by apply RSA Algorithm.

Bob → G (K_{e_Bob}, K_{d_Bob})

Alice → G (K_{e_Alice}, K_{d_Alice})

Step 2: Both Bob and Alice send the public key for each other.

K_{e_Bob}→ to Alice

K_{e_Alice} → to Bob

Step 3 Encrypt fingerprint by apply RSA algorithm using public key, send cipher fingerprint to each other and save in database as denoted:

$C_{\_\text{Cipherfingerprin-Alice}}= E\ (FP_{\_Alice})$ by apply RSA Algorithm using K_{e_Bob}

$C_{\_\text{Cipherfingerprin-Alice}}$ → Send to Bob

Also Bob apply as denoted:

$C_{\_\text{Cipherfingerprint-Bob}}= E(FP_{\_Bob})$ applying RSA Algorithm using K_{e_Alice}

$C_{\_\text{Cipherfingerprint-Bob}}$ → Send to Alice

Both Alice and Bob receipt the cipher fingerprint from the other and save in their database .

Bob saves in database → C_Cipherfingerprin-Alice

Alice saves in database → C_Cipherfingerprint-Bob

Step 4: Each one has encrypted fingerprint in their database, assume Alice want call Bob:

Alice send cipher finger print to Bob

$C_{\_\text{Cipherfingerprin-Alice}}$ → Send to Bob

Bob Decrypt the cipher finger print of Alice by use RSA algorithm using Bob private key K_{d_Bob} as denoted:

$FP_{\_Alice} = D\ (C_{\_\text{Cipherfingerprin-Alice}})$ by apply RSA algorithm using Kd_Bob.

Step 5: Bob compare the finger print $FP_{\_Alice}$ which is came from Alice with fingerprint of Alice saved in Bob database, if two fingerprints are same then the authentication is done.

Step 6: Begin calling between Alice and Bob by apply AES algorithm (Section 3) to send encrypted voice packets via communication channel.

The goal from all above to avoid transmit fingerprint using to generate cryptographic key via unsecure communication channel.

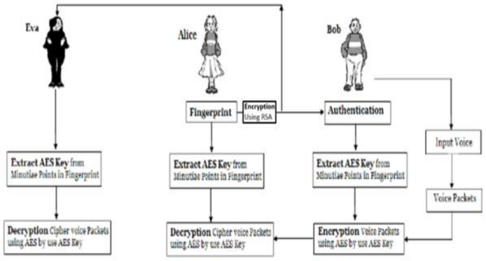
Eva
Alice
Bob
Fingerprint
Encryption Using RSA
Authentication
Input Voice
Extract AES Key from Minutiae Points in Fingerprint
Extract AES Key from Minutiae Points in Fingerprint
Extract AES Key from Minutiae Points in Fingerprint
Voice Packets
Decryption Cipher voice Packets using AES by use AES Key
Decryption Cipher voice Packets using AES by use AES Key
Encryption Voice Packets using AES by use AES Key

Fig. 2. Fingerprint distribution resolved.

IV. Conclusion

This paper proposed a method to stream cipher voice packets encrypted by using key generated from Minutiae Points from fingerprint also define a Fingerprint Distributed Problem. We suggested a solution for the FDP. This approach has reduced of probability attack this system by increasing layers of security, especially by suggested using RSA algorithm to encrypt fingerprint before send them in unsecure communication channel.

References

[1] Arul, P., Shanmugam, A. (2009). Generate A Key for AES Using Biometric for Voip Network Security. Journal of Theoretical and Applied Information Technology, Vol, l5, No.2, pp. 107-112.

[2] Arul, P., Shanmugam, A. (2008). "New-Fangled Fingerprint Engendered Key For A Secured VoIP". In proc. 7th WSEAS International Conference on Electronics, Hardware, Wireless and Optical Communications, pp. 45-48, England, UK.

[3] Bais, R., Mehta. K. (2012). Biometric Parameter Based Cryptographic Key Generation, International Journal of Engineering and Advanced Technology (IJEAT), Vol.1, pp.157-160.

[4] Ballard, L., Kamara, L., Monrose, F. (2008). "Towards Practical Biometric Key Generation with Randomized Biometric Templates", Proceedings of the 15th ACM conference on computer and communication security, pp. 235-244, Alexandria.

[5] Balakumar, P., Venkatesan, R. (2011). Secure Biometric Key Generation Scheme for Cryptography using Combined Biometric Features of Fingerprint and Iris, IJCSI International Journal of Computer Science Issues, Vol. 8, No. 2, pp. 349-356.

[6] Diffie, W., Hellman, M. (1976). A new directions in cryptography, IEEE Transactions on Information Theory Vol. 6 Num, 22 PP. 644–65

[7] FIPS (2001). 197: Announcing the advanced encryption standard (AES).

[8] Goode, B., (2002). "Voice over Internet protocol (VoIP)," Proceedings of the IEEE , vol.90, no.9, pp.1495-1517, USA.

[9] John, J., Rajesh, T. (2013). Multiple Key Generation using Elliptic Curve Cryptography Fusion Algorithm for Biometric Source. International Journal Of Engineering And Computer Science, Vol.2, Issue.3, pp. 732-740.

[10] Murugesh, R., (2012). "Advanced biometric ATM machine with AES 256 and steganography implementation," Advanced Computing (ICoAC), 2012 Fourth International Conference on, vol., pp.1-4, Munich, Germany.

[11] Nisar, K., Said, M., Hasbullah, H. (2010) "Enhanced performance of packet transmission using system model over VoIP network", proceeding of Information Technology (ITSim), 2010 International Symposium, vol.2 . pp. 1005-1008. Malaysia.

[12] Rivest, R., Shamir, A. Adleman, L. (1978). A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, COMMUNICATIONS OF THE ACM, pp. 120-126.

[13] Sharma, R., (2012). Generation of Biometric Key for use in DES. IJCSI International Journal of Computer Science Issues, Vol. 9, Issue.6, No.1, pp.312-315.

[14] Uludag, U., Pankanti, S., Prabhakar, S., Jain, A., (2004) "Biometric cryptosystems: issues and challenges," Proceedings of the IEEE , vol.92, no.6, pp.948-960, USA.

[15] Abuguba, S., Milosavljevic, M. M., & Macek, N. (2015). An efficient approach to generating cryptographic keys from face and iris biometrics fused at the feature level. International Journal of Computer Science and Network Security (IJCSNS), 15(6), 6.