Confidentiality of VOIP Data Using Efficient ECDH Key Exchanging Mechanism

T.Subashri [1] , Kalluri Krishna Reddy [2] , V.Vaidehi [3]

Department of Electronics Engineering,
Madras Institute of Technology,
Anna University, Chennai-44.
[1]tsubashri@annauniv.edu
[2]kalluri_88@yahoo.co.in
[3]vaidehi@annauniv.edu

***Abstract*—The most demanding low cost technology is voice over internet protocol (VoIP). However, VoIP packets are easy to eavesdrop by hackers on public and private cryptosystems. Because symmetric key cryptosystems such as Advanced Encryption Standard (AES) uses weak keys for VoIP packet encryption. So in this work, an approach for strengthening AES algorithm is developed. Instead of using AES key directly from its own key expansion algorithm and Diffie Hellman (DH) based key for AES algorithm, the hashed Elliptic Curve Diffie Hellman (ECDH) based AES key is used to enhance confidentiality of VoIP data. Hashed ECDH based AES key provides high computational complexity to break the key compared to AES self generated key and DH based AES key. So, this approach makes it hard for the hacker to estimate encryption key values.**

***Keywords*— cryptosystems, confidentiality, hashed.**

1. INTRODUCTION

VoIP (Voice over Internet Protocol), where voice and video communication, which have traditionally run on the PSTN (Public Switched Telephone Network), are transported on IP networks [4]. VoIP technologies are being adopted in the business and home environments as they provide low call rates. The biggest challenge that the voice over internet systems faces is the security of the packets that are transmitted. The information transmitted should be confidential to both sender and the receiver. So security is the major challenge faced by VoIP. We are interested in confidentiality [3] area from the field of data security and hence we do not discuss the protection of the VoIP infrastructure from malicious attacks. A standard installation of VoIP using SIP, H.323 [4] or IAX protocols will not provide any form of security for voice traffic. To overcome this, it is necessary to add some form of security schemes such as encryption at the transport layer. By providing the security schemes for VoIP system it becomes difficult for the hacker to hack the data packet. In public-key cryptosystems, the public key is freely distributed, while its paired private key must be secret. The public key is typically used for encryption, while the private key is used for decryption.

Diffie and Hellman showed that public-key cryptography was possible by presenting the Diffie-Hellman key exchange mechanism. Public-key algorithms are most often based on the computational complexity of "discrete logarithmic" problems. Elliptic curve cryptography has developed in which security is based on elliptic curves. Because of the difficulty of the above problems, most public-key algorithms involve operations such as modular multiplication and exponentiation, which are very much computationally expensive than the methods used in most block ciphers, especially with typical key sizes. As a result, public-key cryptosystems are commonly hybrid cryptosystems, in which a fast high-quality symmetric-key encryption algorithm such as AES is used for voip packet encryption.

2. ELLIPTIC CURVE CRYPTOGRAPHY (ECC)

Elliptic Curve Cryptography (ECC) is a public key cryptography. In this public key cryptography each user or the device which is taking part in the communication generally have a pair of keys, one public key and other private key, and a set of operations associated with the keys to do the cryptographic operations. Only the specific user knows the private key whereas the public key is distributed to all users which are taking part in the communication. Some public key algorithm may require a set of already defined constants to be known by all the devices taking part in the communication. Domain parameters used in ECC is an example of such constants. The Public key cryptography, unlike private key cryptography, does not require any shared secret between the communicating parties but this is much slower than the private key cryptography.

The mathematical operations of ECC [9][12] is defined over the elliptic curve

$$Y^2=X^3+aX+b, \quad (1)$$

where, $4a^3+27b^2\neq 0$. (2)

Each value of the ‘a’ and ‘b’ gives a different form of elliptic curve. All points (x, y) which satisfies the above equation and the point at infinity lies on the elliptic curve. The public key is a point on the curve and the private key is

some random number. The public key is obtained by multiplying the private key with G the generator point in the curve. The generator point G, the curve parameters 'a' and 'b', together with few more constants constitutes the domain parameter of ECC. One main advantage of ECC is its smaller key size. A 256-bit key in ECC is considered to be as equivalently secured as 3072-bit key in RSA and DH. The security of ECC depends on the difficulty of Elliptic Curve Discrete Logarithm Problem.

The discrete logarithm problem for elliptic curves is defined as follows, we have the problem of finding m (given that m exists) such that mP = Q where P and Q be two points on an elliptic curve such that mP = Q, here m is a scalar. Given P and Q, it is computationally very difficult to obtain m, if m is large then m is the discrete logarithm of Q to the base P. Hence the main operation which is involved in ECC is point multiplication. That is multiplication of a scalar m with any point P on the curve to obtain another point Q on the curve. Point multiplication can be achieved by two basic elliptic curve operations one by point addition and other by point doubling. Let P be a point on an elliptic curve. The point multiplication basically uses point addition and point doubling repeatedly to find the result. For elliptic curve in prime field Fp adding two points J and K to obtain another point N that is $N = J + K$.

Consider two distinct points J and K such that $J = (X_J, Y_J)$ and $K = (X_K, Y_K)$ in figure 1

Let $N = J + K$ where $N = (X_L, Y_L)$, then

$$X_L=(M^2-X_J-X_K) \bmod p \quad (3)$$

$$Y_L=(-Y_J)+M(X_J-X_L) \bmod p \quad (4)$$

$$M=(Y_J-Y_K)/(X_J-X_K) \bmod p, \quad (5)$$

M is the slope of the line through J and K.

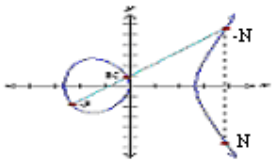

Fig.1 Addition of two points in ECC

Point doubling, adding a point J to itself to obtain another point N that is N = 2J.

If K = J then J + K = 2J then point doubling equations will be used. Consider a point J such that $J = (X_J, Y_J)$, where $Y_J \neq 0$ as in figure2

Let $N = 2J$ where $N = (X_L, Y_L)$, Then

$$X_L=(M^2-2X_J) \bmod p \quad (6)$$

$$Y_L=(-Y_J)+M(X_J-X_L) \bmod p \quad (7)$$

$$M = (3X^2_J + a) / (2\,Y_J) \bmod p. \quad (8)$$

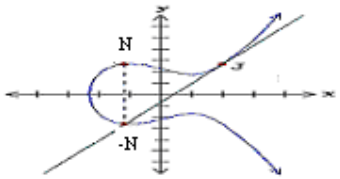

Fig.2 Point doubling in ECC

The domain parameters for Elliptic curve over Fp are p, a, b, G and q. Where p is the prime number defined for finite field Fp . a and b are the parameters defining the curve

$$Y^2 \bmod p=(X^3+aX+b) \bmod p. \quad (9)$$

G is the generator point, a point on the elliptic curve chosen for cryptographic operations, q is the order of the elliptic curve. The scalar for point multiplication is chosen from a number between 0 and q – 1.

2.1 ECDH-Elliptic Curve Diffie Hellman Key Exchanging Mechanism

ECDH is a key agreement protocol that allows two parties to generate a shared secret key that can be used for private key algorithms. Both parties exchange some public information to each other. Using this public data and their own private data these two parties calculates the shared secret. Any third party, who doesn't have access to the private details of each device, will not be able to calculate the shared secret from the available public information.

For generating a shared secret between user A and user B using ECDH, both have to agree up on Elliptic Curve domain parameters. Both end have a key pair consisting of a private key N_a for user A and N_b for user B (a randomly selected integer less than n, where n is the order of the curve, an elliptic curve domain parameter) and a public key $P_a = N_a * G$ for user A and $P_b = N_b * G$ for user B.(where G is the generator point, an elliptic curve domain parameter).

The user A then calculates the secret key by taking user B pubic key and multiplying it with its private key which gives shared secret key $K= N_a * P_b$ in the same method user B calculates the shared secret key $L= N_b * P_a$,Here K=L that is both the keys are same.

3. SHA-256 HASH ALGORITHM

Secure hash algorithm SHA-256[1] is used for computing a condensed representation of electronic data . When a message of any length is given as input to an algorithm, the result is an output called a message digest. The algorithm basically has a message schedule of sixty- four 32-bit words, eight working variables of each 32 bits, and a hash value of eight 32- bit words. The final result of SHA-256 is a message digest of size 256-bit. The words of the message schedule are labeled W_0, W1… W79. The eight working variables for SHA-256 are labelled a, b, c, d, e, f, g, and h. The words of the hash value are labeled $H^{(0)}$ to $H^{(7)}$ which will hold the initial hash value, $H^{(0)}$ replaced by each successive

intermediate hash value, $H^{(i)}$ and ending with the final hash value, $H^{(7)}$.

Thus we get an output of 256 bit digest as a common shared key which is very strong.

4. ADVANCED ENCRYPTION STANDARD

AES is a block cipher with a block length of size 128 bits. AES[4] allows three different key lengths: 128, 192, and 256 bits. The key length of 128 bit Encryption consists of 10 rounds of processing , 12 rounds for 192-bit keys and 14 rounds for 256-bit keys. Except for the final round in each case, all other rounds are similar. Each round of processing consists of one single-byte substitution step,then followed by a row-wise permutation step, and followed by a column-based substitution step, followed by the addition of the round key.

To understand the basic steps used in a single round, it is best to think of a 128-bit block consisting of a matrix of size 4×4 bytes. Thus, the first four bytes of a 128-bit input block occupy the first column in the 4 ×4 matrix of bytes. The next four bytes occupy the second column, and this continues till end. By this non linear relation ship with every rounds of key in AES algorithm is increased which strengthens the key. AES also has a word. A word consists of four bytes, which is 32 bits. Therefore, each column of the state array is a word, as is each row. Each round of processing works on the input state array and then produces an output state array. The output state array produced in the last round is rearranged into a 128-bit output block. Decryption algorithm differs substantially from the encryption algorithm. Although, the same steps are used in encryption and decryption.

5.CONFIDENTIALITY AND INTEGRITY OF VOIP DATA USING EFFICIENT ECDH KEY EXCHANGING MECHANISM

5.1 Need of ECDH for VOIP

The public-key cryptosystems such as DH (Diffie-Hellman) algorithm is being used for VoIP security systems. The drawback of DH key exchanging mechanism is that the hacker can easily break the secret key and decrypt the encrypted VoIP packet because of this confidentiality of VoIP packet is lost. The reason behind this is discrete logarithmic problem in DH which leads to weaker keys for VoIP packet encryption.

The Elliptic Curve Diffie-Hellman(ECDH) key agreement scheme can be used as an alternative to traditional DH algorithm of key exchange which offers strong keys with equivalent security as DH but with smaller key sizes resulting in faster computations. There is a high security for the key generated by ECDH because the discrete logarithmic problem is very difficult in this scheme.The implementation for the secured ECDH scheme for voip packet is shown in Figure 3.

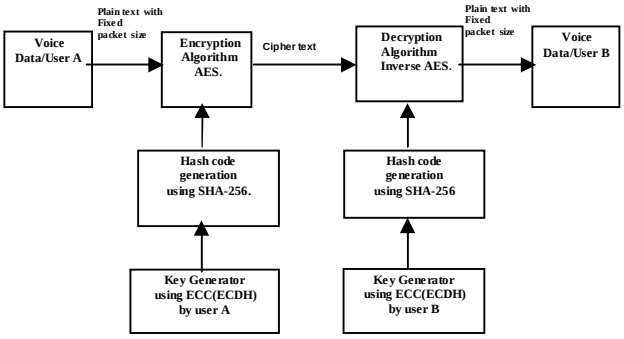

Fig.3 ECDH Secured VOIP System

5.2 VOIP User A/VOIP User B

The VoIP user A or VoIP user B any one among them can initiate the call. Both the users use the compression techniques such as PCM and use ADC and DAC(analog to digital and digital to analog converter) to convert voice in to digital form and grouped in to packets each of size 300 bytes which is referred as plain text at the receiving end the plain text is obtained from cipher text and applied to DAC to obtain the speech signal.

5.3 Key Generation using ECC (ECDH)

The parameters for ECC are chosen from prime field F_p from the equation 2.8 . Let (N_a, P_a) be the private key and public key pair of A and (N_b, P_b) be the private key public key pair of B.

1. The user A computes $K = (X_K, Y_K) = N_a * P_b$
2. The user B computes $L = (X_L, Y_L) = N_b * P_a$
3. Since $N_a * P_b = N_a * N_b * G = N_b * N_a * G = N_b * P_a$ therefore K = L and hence $X_K = X_L$.
4. Hence the shared secret is X_K,

The computation complexity for ECDH is $\sqrt{n}$, where n is number of key bits. For DH/RSA the computation complexity is $\exp(1.923(\log n)^{1/3}(\log \log n)^{2/3})$.That means DH/RSA have exponential complexity, where as ECDH has square root of n as complexity of breaking the key.

5.4 Generation of Hash Code Using SHA-256

From the figure 3 it is shown that the key generated by ECDH is applied to hashing function SHA-256. SHA has the advantage of smaller rounds which is 64 compared to SHA-0 and SHA-1which has 80 rounds in each. The another advantage is that there are no attacks found for SHA-256.The SHA-256 generates 256 bit hashed ECDH key which provides data integrity for VoIP packet and can be applied as a key for AES encryption.

5.5 AES Encryption/Decryption Algorithm for VOIP Packet

The generated 256 bit digest key will be applied to AES Encryption Algorithm (Provides confidentiality) along with the plain text (digitized voice data in fixed packet size) to generate cipher text. At the receiving side user A or user B uses the shared key to decrypt the cipher text and generate plain text this is explained in figure 3. In this work VoIP packets of sizes 300,600 and 900 bytes are taken as plain text

and performed encryption and decryption using 256 bit hashed DH and ECDH keys.

6. SIMULATION AND RESULTS

The simulation is carried out in Java Jdk 1.5 with Netbeans 6.0 as IDE(Integrated Development Environment). Here first the simulation of DH key Exchanging mechanism was done with the simulation software and then the simulation of ECDH Key Exchanging is performed. This Key generated is applied to the SHA-256 message integrity algorithm to generate aShared and bShared 256 bit keys for the two VoIP users for both DH and ECDH schemes as shown in the figure4 and figure5 .

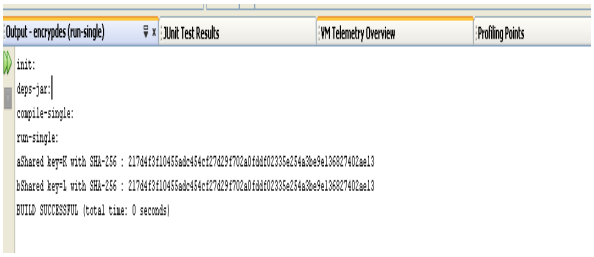

Fig.4 Generation of 256 bit hashed DH key

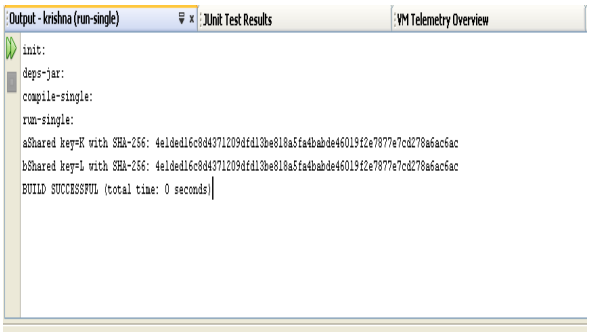

Fig.5 Generation of 256 bit hashed ECDH key

Then the encryption of VoIP packet is done with the previously generated hashed keys. This work provides an approach for the complete security infrastructure for VoIP data security.

Here we compare the ECDH and DH key generation computation time for hashed 160 bit and 256 bit using netbeans profiler.The figure 6 shows that for generating 160 bit hashed ECDH Key and 256 bit hashed ECDH key computation time is slightly high for ECDH than DH. But this does not affect the VoIP performance because this key is generated initially before packet is transmitted.

The computational complexity for breaking the 160 bit ECDH key based AES algorithm for VoIP packet is in the order of 12.649 and for 256 bit of ECDH key it takes 16 as complexity, which is normally higher than the computation complexity of breaking DH based AES key which has 3.41 and 3.88 for 160 and 256 bit key respectively.

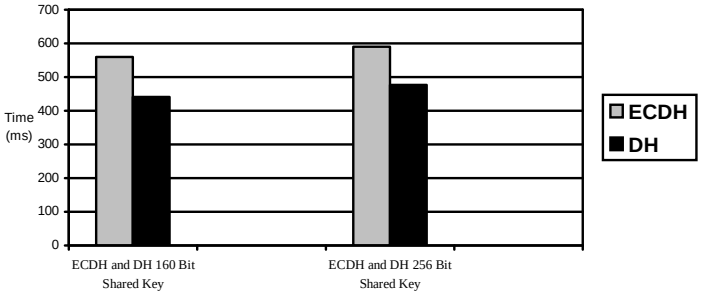

Fig. 6 Comparison of computation time for generating 160 bit and 256 bit ECDH and DH key

6.1 Comparison of Computation time for AES Encryption (or) Decryption of Voice Packet with 256 bit Hashed ECDH and DH keys.

This figure 7 shows that for the packet size of 300 bytes DH based encryption (or) decryption takes 0.054ms time duration but the hashed ECDH encryption (or) decryption takes 0.058ms time duration.Though the ECDH encryption (or) decryption computation time is slightly high in µsec compared to DH but the VoIP performance is not much affected because any delay less than 125msec for VoIP is acceptable. From the figure it is seen that as the packet size is increasing the encryption (or) decryption time is also increasing.

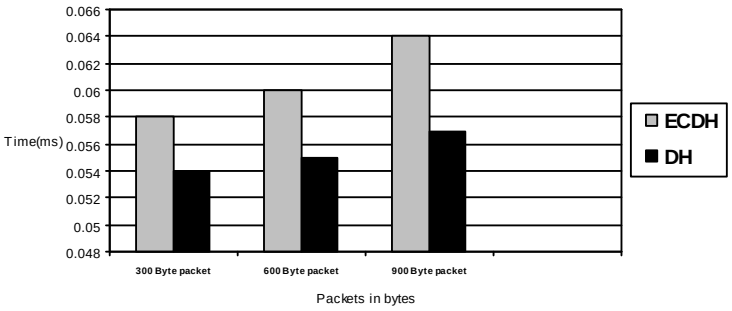

Fig.7 Comparison of computation time for AES encryption or decryption for different packet sizes using ECDH and DH keys.

7. CONCLUSION AND FUTURE WORK

Existing public key crypto systems for VoIP such as RSA and DH can be easily attacked by the hackers. So to increase the confidentiality of VoIP packet, an approach for strengthening AES encryption algorithm is developed by integrating Elliptic Curve Diffie Hellman key exchanging mechanism with SHA-256 hashing algorithm. So, this approach makes it difficult for the hacker to estimate the encryption key values compared to usual methods of AES encryption. The security for VoIP data can be further increased by applying dynamic key changing scheme, where each packet is encrypted by different hashed ECDH keys. This approach makes each key exponentially growing in complexity and making the hacker difficult to estimate the key for each packet.

REFERENCES

[1] A.Arul Lawrence Selvakumar,C.Suresh Ganandhas,"The Evaluation Report of SHA-256 Crypt Analysis Hash Function",IEEE Computer Society, International Conference On Communication Software And Networks 2009.

[2] Chia-Hui Wang, Mei-Wen Li, and Wanjiun Lian,"A Distributed Key Changing M- echanism For Secure Voice Over IP (VOIP) Services",IEEE 2007 International Conference On Multimedia And Expo(ICME 2007),July 2-5,2007 Beijing China.

[3] David Butcher, Xiangyang Li, and Jinhua Guo,"Security Challenge And Defense In VoIP Infrastructures", IEEE Transaction On Systems, an And Cybernetics,PART C:Applications and Review, Vol. 37, NO. 6 ,November 2007.

[4] D.Richard Kuhn, Thomas J. Walsh, Steffen Fries,"Security Considerations For Voice Over IP Systems",NIST Special Publication ,January 2005.

[5] Elaine Barker, William Barker, William Burr,William Polk, and Miles Smid, "Recommendation For Key Management",NIST Special Publication 800-57, May 2006.

[6] Feng Cao and Saadat Malik,"Vulnerability Analysis And Best Practices For Adopting IP Telephony In Critical Infrastructure Sectors",IEEE Communications Magazine,pp138-145, April 2006.

[7] FIPS(Federal information processing standards),"Advanced Encryption Standard",issued by NIST, November 26,2001.

[8] Gary S. Miliefsky,"Securing your Voip",Net clarity ACVE white paper October 20, 2005.

[9] N.koblitz,"Elliptical Curve Cryptosystems",Mathematics of Computation,Vol. 48, . Published By American Mathematical Society, pp. 203-209.January 1987.

[10] Prateek Gupta, V.M.Ware and Vitaly Shmatikov ,"Security Analysis Of Voice-over-IP Protocols",20th IEEE Computer Security Foundations Symposium(CSF'07) 2007.

[11] Tim Grance, Rick Kuhn, Susan Landau,"Cryptographic Hash Standards", Published By The IEEE Computer Society. IEEE Security & Privacy,pp88-91, 2006.

[12] Victor S.Miller,"Use of Elliptic Curve In Cryptography",Advances In Cryptography Springler-Verlag,pp417-426, 1998.

[13] W.Diffie,M.Hellman,"New Directions In Cryptography",IEEE Transaction On Information Theory, VOL. IT-22, NO. 6,November 1976.

.