Journal of Computer Science 2 (9): 672-675, 2006
ISSN 1549-3636

A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking

[1]E. Ramaraj and [2]S. Karthikeyan
[1]Computer Centre, Alagappa University, Karaikudi, Tamilnadu, India
[2]Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu, India

Abstract: Today wireless communications is acting as a major role in networks. Through year-end 2006, the employee's ability to install unmanaged access points will result is more than 50% of enterprises exposing sensitive information through the wireless virtual private networks (VPN). It enables you to send the data between two computers across a shared or public network in a manner that emulates the properties of a private link. The basic requirements for VPN are User Authentication, Address Management, Data Compression, Data Encryption and Key Management. The private links are established in VPN using Point-to-Point Tunneling Protocol (PPTP) and Layer-Two-Tunneling Protocol (L2TP). These protocols are satisfies VPN requirements in five layers. In user authentication layer, multiple trusted authorities using Extensible Authentication Protocol (EAP) do the authentication process. In fourth layer the data encryption part using RC4 called Microsoft-Point-to-Point Encryption (MPPE) method. The aim of this paper, instead of multiple trusted authorities we focus single trusted authority using public key cryptography RSA in EAP and also we include AES-Rijndael stream cipher algorithm instead of RC4 for MPPE. We propose new type of hybrid encryption technique using AES-Rijndael for encryption and decryption and RSA used for key management.

Key words: Wireless communication, security, and authentication

INTRODUCTION

Over recent years, the market for wireless communications has enjoyed tremendous growth. Wireless technology now reaches or is capable of reaching virtually every location on the face of the earth. Hundreds of millions of people exchange information every day using pagers, cellular telephones and other wireless communication products. With tremendous success of wireless telephony and messaging services, it is hardly surprising that wireless communication is beginning to be applied to the realm of personal and business computing. No longer bound by the harnesses of wired networks, people will be able to access and share information on a global scale nearly anywhere they venture. The security of the communication is mainly based on the cryptographic algorithms. The VPN is the major role for secure communication in an insecure network. The portion of the connection in which the data is encapsulated is known as the tunnel and some portion of the connection is encrypted this data known as VPN connection. In an Internet solution, few Internet connections through Internet service providers and VPN server computers can serve the remote networking needs of hundreds or thousands of remote clients. By using VPN server, the network administrator can ensure that only those users on the organization network who have appropriate permissions can establish the VPN connection with the VPN server and gain access to the protected resources of the computer. All the VPN connections can make sure the data confidentiality.

In VPN, generally two types of protocols are mainly used for secure transmission. The PPTP allows multi protocol traffic to be encrypted and then encapsulated in an IP header to be sent across an IP inter network. In L2TP allows multi protocol traffic to be encrypted and then sent over any medium that supports datagram delivery.

Basic VPN requirements: The four basic requirements are mainly focused in VPN. In the User authentication requirement is to identify the user. The address management is mainly used for the addresses of the client machine will keep secret.

The data compression mainly used for when the data is large. The data encryption management is used for secure data exchange. The key management effectively manages the key used for encryption and decryption. In user authentication part EAP protocol followed for user identity checking. In data encryption part MPPE algorithm mainly used RC4 stream cipher[1,2].

AES-Algorithm

Overview of AES Cipher: The Advanced Encryption Standard (AES) is a computer security standard that became effective on May 26, 2002 by NIST to replace

Corresponding Author: S. Karthikeyan, Part-Time Ph.D Scholar, Department of Computer Science and Engineering, Alagappa University, Karaikudi, Tamilnadu, India

DES. The cryptography scheme is a symmetric block cipher that encrypts and decrypts 128-bit blocks of data. Lengths of 128, 192 and 256 bits are standard key lengths used by AES[2-4].

The algorithm consists of four stages that make up a round, which is iterated 10 times for a 128-bit length key, 12 times for a 192-bit key and 14 times for a 256-bit key. The first stage "SubBytes" transformation is a non-linear byte substitution for each byte of the block. The second stage "ShiftRows" transformation cyclically shifts (permutes) the bytes within the block. The third stage "MixColumns" transformation groups 4-bytes together forming 4-term polynomials and multiplies the polynomials with a fixed polynomial mod (x^4+1). The fourth stage "AddRoundKey" transformation adds the round key with the block of data.

In most ciphers, the iterated transform (or round) usually has a Feistel Structure. Typically in this structure, some of the bits of the intermediate state are transposed unchanged to another position (permutation). AES does not have a Feistel structure but is composed of three distinct invertible transforms based on the Wide Trial Strategy design method.

The Wide Trial Strategy design method provides resistance against linear and differential cryptanalysis. In the Wide Trail Strategy, every layer has its own function:

* The linear mixing layer: guarantees high diffusion over multiply rounds
* The non-linear layer: parallel application of S-boxes that have the optimum worst-case non-linearity properties.
* The key addition layer: a simple XOR of the round key to the intermediate state

The Rijndael proposal for AES defined a cipher in which the block length and the key length can be independently specified to be 128, 192 and 256 bits. A use of three key size alternatives but limits the block length to 128 bits.

The algorithm was designed to have the following characteristics:

* Resistance against all known attacks
* Speed and code compactness on a wide range of platforms
* Design simplicity
* Input to the encryption algorithm, decryption algorithm in a single 128 bit block

In AES, four different stages are used

i. Substitution bytes

Use S-box to perform byte-to-byte substitution of the block

ii. Shift rows

A simple permutation

iii. Mix columns

A substitution that makes use of arithmetic

iv. Add round key

A simple bit wise XOR of the current block with the portion of the expanded key

In add round key stage makes use of the key. Any other stage applied at the beginning or end is reversible without knowledge of the key, this scheme is more efficient and secure. Each stage is easily reversible. For the substitute byte, shift row, mix column stages, as inverse function used in the decryption algorithm. For add round key stage, the inverse is achieved by XOR the same round key to the block.

The decryption algorithm is not identical for the encryption algorithm. This is a consequence of the particular structure of the AES.

AES-Rijindael: We analyze various AES-standard algorithms like MARS, RC6, Rijndael, Serpent, Twofish for encryption and decryption performance, key scheduling performance and overall performance. An enormous amount of information has been gathered on the speed of the AES- algorithms on a variety of software platforms. The Table 1 summarizes the overall performance of the finalists on the various platforms when using 128-keys. Additionally, an overall performance table is also included. The following Table 1 shows the overall performance of various AES algorithms and the graph-1 represents diagrammatic representation.

In this overall performance the MARS provides average performance for encryption, decryption and key setup. RC6 provides average to high-end performance for encryption and decryption and average performance for key setup. Rijndael provides consistently high-end performance for encryption, decryption and key setup, although performance decreases for the 192 and 256-bit key sizes. Serpent provides consistently low-end performance for encryption and decryption and platform-dependent performance for key setup. Twofish provides platform-dependent performance for encryption and decryption and consistently low-end performance for key setup.

Table 1: Overall performance of various AES standard algorithms

	Encryption / Decryption	Key Setup
MARS	II	II
RC6	I	II
Rijndael	I	I
Serpent	III	II
Twofish	II	III

Overview of RSA: In this Hybrid Encryption technique, we take the data to encrypt by AES-Rijndael using a key. The key should be received as an encrypted form using RSA from user. The RSA scheme is a block cipher in which the plain text and cipher texts are integers between 0 and n-1 for some n. We examine RSA in this section in some detail, beginning with an explanation of the algorithm. Then we examine some of the computational and cryptanalytical of RSA.

Description of the algorithm: Plain text is encrypted in blocks, with each block having a binary value less

than some number n. That is, the block size must be less than or equal to $\log_2(n)$; in practice, the block size is 2^k bits, where $2^k<n<=2^k+1$. Encryption and decryption are of the following form, for some plaintext block M and ciphertext block C:

$C = M^e \bmod n$

$M = C^d \bmod n = (M^e)^d \bmod n = M^{ed} \bmod n$

Both sender and receiver must know the value of n. The sender knows the value of e and only the receiver knows the value of d. Thus, the public key encryption algorithm with a public key of KU = {e, n} and private key of KR = {d, n}. For this algorithm to be satisfactory for public key encryption, the following requirements must be met:

* It is possible to find values of e,d, n such that $M^{ed} = M \bmod n$ for all M<n.
* It is relatively easy to calculate M^e and C^d for all values of M<n.
* It is infeasible to determine d given e and n.

For now, we focus on the first question, we need to find a relationship of the form

$M^{ed} = M \bmod n$

According to the Euler's theorem, given two prime numbers, p and q and two integers, n and m, such that n = pq and 0<m<n and arbitrary integer k, the following relationship holds:

$m^{k\varphi(n)+1} = m^{k(p-1)(q-1)+1} \equiv m \bmod n$

where φ(n) is the Euler function, which is the number of positive integers less than n and relatively prime to n. Suppose p, q prime, φ(pq) = (p-1)(q-1). Thus, we can achieve the desired relationship if

$ed \equiv k\varphi(n) + 1$

This is equivalent to saying:

$ed \equiv 1 \bmod \varphi(n)$

$d \equiv e^{-1} \bmod \varphi(n)$

That is, e and d are multiplicative inverses mod φ(n). Note that, according to the rules of modular arithmetic, this is true only if d (and therefore e) is relatively prime to φ(n).

Equivalently, gcd(φ(n),d) = 1.

We are now ready to state the RSA scheme. The ingredients are the following:

p, q, two prime numbers (private, chosen)

n=pq (public, calculated)

e, with gcd(φ(n),e)=1; 1<e< φ(n) (public, chosen)

$d = e^{-1} \bmod \varphi(n)$ (private, calculated)

The private key consists of {d, n} and the public key consists of {e, n}. Suppose that user A has published its public key and that user B wishes to send the message M to A. Then B calculates $C = M^e \pmod n$ and transmits C. On receipt of this ciphertext, user A decrypts by calculating $M = C^d \pmod n$.

So, $M^{ed} \equiv M \bmod n$. Now,

$C = M^e \bmod n$

$M = C^d \bmod n \equiv (M^e)^d \bmod n \equiv M^{ed} \bmod n \equiv M \bmod n$

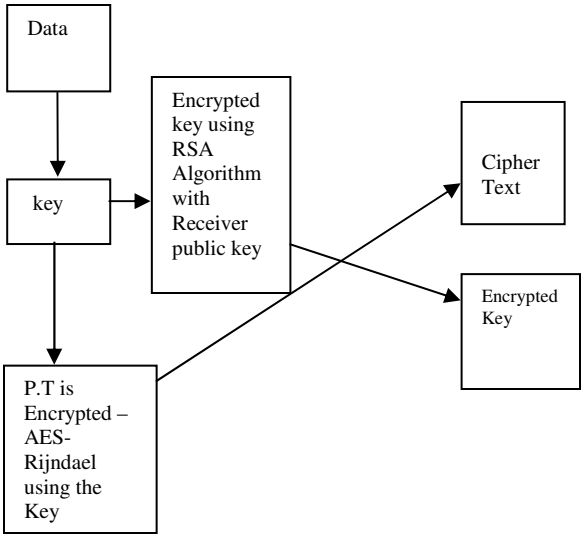

Fig. 1a: Sender side encryption process (Ex. VPN Server)

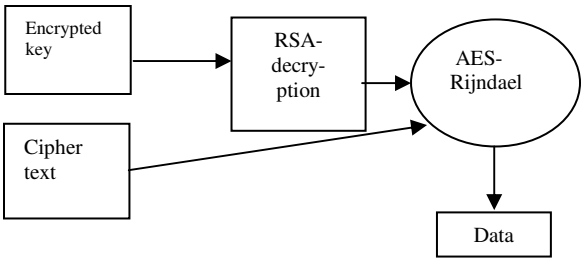

Fig. 1b: Sender side encryption process (Ex. VPN client)

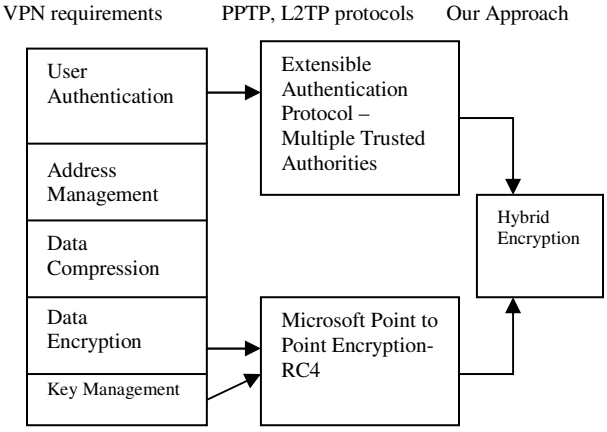

Fig. 2: Our new proposed hybrid encryption protocol

Overview of proposed system: In this paper we are going to perform new type of encryption technique in EAP and MPPE. In Hybrid Encryption, a key is agreed between the VPN client and the VPN server. This key can be dynamic or can even be static. A key of length says, 128 bits are chosen.

This is used to encrypt the plain text using AES-Rijndael steam cipher algorithm. The key is encrypted using the RSA algorithm with receiver's public key. Both are attached and sent. Now, the VPN client can apply its private key to decipher the key and using the key with AES-Rijndael can decrypt the Cipher text to get back the plain text. The main advantage of this method is that it takes much lesser time when compared to normal encryption with secure key transformation process. The design of our system shown in Fig. 1a and b.

This proposed hybrid encryption method is used instead of RC4 in MPPE. This will be illustrated in Fig. 2.

The above protocol is only our view of to implement hybrid encryption technique in data encryption and user authentication part. This protocol to reduce the user authentication and data encryption layers into a single protocol layer.

DISCUSSION

Let us discuss the security of the proposed schemes. Basically, the security of the proposed schemes is based on the difficulty of cryptographic assumptions as follows.

1. The security part of the AES-Rijndael algorithm is very high than other stream ciphers like RC4, RC5, RC6 and so on.
2. The RSA is very high secure than other public key cryptographic algorithms. But the RSA is very slow when we try to convert large number of data. To avoid this in our proposal RSA used to convert only the key values.

CONCLUSION

In this study we presented a new type of hybrid encryption protocol for VPN data encryption and key management. In this approach the VPN server is the trusted authority. The VPN client initiates the request; the VPN server gives the key value. Using the key value VPN client securely encrypt data with the help of AES-Rijndael. Then the key value encrypted using receivers public key with the help of RSA. Then these encrypted values integrated together and send to the receiver. The receiver using its private key and RSA identify the original key value. Using the key to decrypt the encrypted data with the help of AES-Rijndael. The proposed approach is more secure compare than the previous approach.

REFERENCES

1. James, N., E. Barker, L. Bassham, W. Burr, M. Dworkin, J. Foti and E. Roback, 2000. Report on the development of the advanced encryption standard (AES). Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce.
2. Srdjan, C., L. Buttyan and J.-P. Hubaux, 2003. Self-organized public-key management for mobile ad hoc Networks. IEEE Trans. Mobile Computing: pp: 52-64.
3. Philip, R., M. Bellare and J. Black OCB, 2003. A block-cipher mode of operation for efficient authenticated encryption. ACM Trans. Information System and Security, pp: 365-403.
4. Mary, R.T., A. Essiari and S. Mudumbai, 2003. Certificate-based authorization policy in a PKI environment. ACM Trans. Information System and Security, pp: 566-588.