Two-Phase Hybrid Cryptography Algorithm For Virtual Private Networks

B.Ramasubba Reddy[1], A.Saritha[2], B.BalaKonda Reddy[3]

[1] Professor, Dept of CSE, SV College of Engineering
Tirupati, India, Email:rsreddyphd@gmail.com

[2]Asst Professor, Dept of CSE, SV Engineering College for Women
Tirupati, India, Email:sarithaanchuri@gmail.com

[3]Asst Professor, Dept of CSE, SV College of Engineering
Tirupati, India, Email:balakondareddyb@gmail.com

Abstract— *With the advent of Internet and Virtual Private Network (VPN) technologies, data transmission has become a challenging task. In every organization, the flow of different kind of information is increasing from one organization to other as well as to its clients roaming in different areas. Ensuring security in VPN is a major task since it is subject to several attacks along with the security criteria such as authentication, access control, confidentiality and data integrity. While several different key protocols and methods to ensure security subsist, these existing systems have their limitations. In this a framework is proposed for secure data transmission in VPNs using a new security algorithm, which uses both symmetric and asymmetric cryptographic techniques to provide high security with minimized key maintenance. It guarantees three cryptographic primitives, integrity, confidentiality and authentication. Advanced Encryption Standard(AES) to provide encryption, XOR-DUAL RSA algorithm for authentication, and Message Digest-5(MD5) for integrity***.**

Keywords- Security, Key length, Integrity, confidentiality, Authentication

I Introduction

A Virtual Private Network (VPN) is a general network mechanism to offer a secure end-to-end network connection. The design is to first negotiate and setup a network tunnel among the two communication nodes. Generally a VPN server also connects to a RADIUS server to permit only authorized users have the privilege to establish such tunnels. The data will then be encrypted before it is transmitted over the network and will then be decrypted on the receiver side. Compare to dedicated private leased lines, VPNs are much cheaper and are ideal to many companies.

VPN is the network which offers security to the sensitive traffic while traversing networks like Internet , a network with VPN is depicted in the figure 1.2 [5]. A VPN is a communications environment in which access is controlled to permit peer connections only within a defined community of interest, and is constructed through some form of partitioning of a common underlying communications medium, where this underlying communication medium provides services to the network on a non-exclusive basis.

The main objective of VPN is to prevent outsiders (hackers) from interfering with messages sent among hosts in the network, and to protect the privacy and integrity of messages going through un trusted networks [3]. From the user's perspective, a VPN connection is a point-to-point connection between the user's computer and the company's server. The nature of the intermediate inter network is irrelevant to the user because it appears as if the data is being sent over a dedicated private link VPN has been adopted by many organizations looking to expand their networking capabilities while reducing their costs. The key feature of a VPN is its ability to use public networks like the Internet rather than private leased lines in order to allow remote users to access the corporate network.

II SECURITY APPROACHES IN VPNS

Confidentiality and data integrity plays an important role in the security of innovative Internet based applications. Confidentiality and data integrity is essential in all data communication networks like Virtual private networks. And can achieve more security with several kinds of symmetric and asymmetric key cryptosystem algorithms. A major part of the proposed work is about confidentiality and data integrity and we present a subset of the latest research relating to its chapter. Current research on VPNs to achieve secure data transmission through public network is presented along the lines of TCP-IPSec based, TCP-AES based, mTCP-IPsec based, SCTP single path-multihoming-based, WiMP-SCTP based, CMP SCTP-CMT based, SCTP-CMT based, mobile VPN, wireless VPN, TCP/IP based VPN, VPN shield, and hybrid encryption protocol based VPN.

1. If you are going to connect to a remote host computer using public-key authentication, you will have to generate your key pair before connecting. Public-key authentication is based on the use of digital signatures. Each user creates a pair of 'key' files. One of these key files is the user's public key, and the other is the user's private key. The server knows the user's public key, and only the user has the private key. When the user

tries to authenticate herself, the server checks for matching public keys and sends a challenge to the user end. The user is authenticated by signing the challenge using her private key.

2. Remember that your private key file is used to authenticate you. Never expose your private keys. If anyone else can access your private key file, they can attempt to login to the remote host computer as you, and claim to be you. Therefore it is extremely important that you keep your private key file in a secure place and make sure that no one else has access to it.
3. Do not use public-key authentication on a computer that is shared with other users. Generate keys only on your personal computer that no one else can access!
4. Also note that if you are using the Windows roaming profiles functionality, your personal settings will be replicated with the roaming profile server. If you store your private keys in the default location (under the profile folder of your Windows user account) your private keys may be suspected to a malicious user listening to the network traffic. Therefore the User Settings folder should not be a directory that will be used in profile roaming.
5. In order to use public-key authentication, you must first generate your own key pair. You can generate your own key files with the help of a built-in key generation wizard. On the Key Generation - Generation page the computer will generate your key files. This can take several minutes, depending on the chosen key length and the processor speed of the computer.
6. During the key generation phase an animation of random bits is displayed. When the process is ready, the Next button is ungraded and you can proceed to the next phase by clicking it. On the **Key Properties** page, select the type of the key to be generated. You can select to generate an RSA or a DSA key, as well as the key length.

Key Length:

Select the length (complexity) of the key to be generated. Available options are 768, 1024, 2048 or 3072 bits. Larger keys are more secured, but also slower to use. The recommended key length for most occasions is 2048 bits.

III Implementation of algorithms

ECC algorithm[13]: Elliptical curve cryptography (ECC) is a public key encryption technique based on *elliptic curve theory* that can be used to create faster, smaller, and more efficient cryptographic keys. ECC generates keys through the properties of the elliptic curve equation instead of the traditional method of generation as the product of very large prime numbers. The technology can be used in conjunction with most public key encryption methods, such as RSA, and Diffie-Hellman. According to some researchers, ECC can yield a level of security with a 164-bit key that other systems require a 1,024-bit key to achieve. Because ECC helps to establish equivalent security with lower computing power and battery resource usage, it is becoming widely used for mobile applications. ECC was developed by Certicom, a mobile e-business security provider, and was recently licensed by Hifn, a manufacturer of integrated circuitry (IC) and network security products. RSA has been developing its own version of ECC. Many manufacturers, including 3COM, Cylink, Motorola, Pitney Bowes, Siemens, TRW, and VeriFone have included support for ECC in their products.

AES Algorithm:

1. In cryptography, the **Advanced Encryption Standard** (**AES**), also known as **Rijndael**, is a block cipher adopted as an encryption standard by the U.S. government. It has been analyzed extensively and is now used worldwide, as was the case with its predecessor, the Data Encryption Standard (DES). AES was announced by National Institute of Standards and Technology (NIST) as U.S. FIPS PUB 197 (FIPS 197) on November 26, 2001 after a 5-year standardization process in which fifteen competing designs were presented and evaluated before Rijndael was selected as the most suitable (see Advanced Encryption Standard process for more details). It became effective as a standard May 26, 2002. As of 2006, AES is one of the most popular algorithms used in symmetric key cryptography. It is available by choice in many different encryption packages. AES is the first publicly accessible and open cipher approved by the NSA for top secret information (see Security of AES, below).

The cipher was developed by two Belgian cryptographers, Joan Daemen and Vincent Rijmen, and submitted to the AES selection process under the name "Rijndael", a portmanteau of the names of the inventors. (Rijndael is pronounced [r inda l]).

Unlike DES (the predecessor of AES), AES is a substitution-permutation network, not a Feistel network. AES is fast in both software and hardware, is relatively easy to implement, and requires little memory. As a new encryption standard, it is currently being deployed on a large scale.

TABLE 1 Table 1 Comparative execution times (in seconds) of encryption algorithms in ECB mode on a P-II 266 MHz machine

Input Size (bytes)	DES	3DES	AES	BF
20,527	2	7	4	2
36,002	4	13	6	3
45,911	5	17	8	4
59,852	7	23	11	6
69,545	9	26	13	7

Input Size (bytes)	DES	3DES	AES	BF
137,325	17	51	26	14
158,959	20	60	30	16
166,364	21	62	31	17
191,383	24	72	36	19
232,398	30	87	44	24
Average Time	14	42	21	11
Bytes/sec	7,988	2,663	5,320	10,167

Table 2 Comparative execution times (in seconds) of encryption algorithms in ECB mode on a P-4 2.4 GHz machine

Factors	AES	3DES
Key length	128, 192 or 256 bits	(k1, k2 are same) 112 bits k2 are same) 112 bits
Cipher type	Symmetric block cipher	Symmetric block cipher
Block size	128, 192, or 256 bits	64 bits
Developed	2000	1978
Cryptanalysis resistance	Strong against differential, truncated differential, linear, interpolation and square attacks	Vulnerable to Attacker could analyze plain text using differential cryptanalysis
Security	Considered secure	One only weakness, which exists in DES
Possible keys	2^{128}, 2^{192}, or 2^{256}	2^{112} or 2^{168}
Possible ASCII printable character keys	95^{16}, 95^{24}, or 95^{32}	95^{14} or 95^{21}
Time required to check all possible keys at 50 billion keys per second**	For a 128-bit key: 5 x 10^{21} years	For a 112-bit key: 800 days

RSA Algorithm[13]: In cryptography, **RSA** is an algorithm for public-key cryptography. It is the first algorithm known to be suitable for signing as well as encryption, and one of the first great advances in public key cryptography. RSA is widely used in electronic commerce protocols, and is believed to be secure given sufficiently long keys and the use of up-to-date implementations.

RSA involves a public key and a private key. The public key can be known to everyone and is used for encrypting messages. Messages encrypted with the public key can only be decrypted using the private key.

MD5 (Message-Digest algorithm 5)[13]: In cryptography, MD5 (Message-Digest algorithm 5) is a widely used, partially insecure cryptographic hash function with a 128-bit hash value. As an Internet standard (RFC 1321), MD5 has been employed in a wide variety of security applications, and is also commonly used to check the integrity of files. An MD5 hash is typically expressed as a 32 digit hexadecimal number.

MD5 was designed by Ron Rivest in 1991 to replace an earlier hash function, MD4. In 1996, a flaw was found with the design of MD5. While it was not a clearly fatal weakness, cryptographers began recommending the use of other algorithms, such as SHA-1 (which has since been found vulnerable itself). In 2004, more serious flaws were discovered making further use of the algorithm for security purposes questionable. In 2007 a group of researchers including Arjen Lenstra described how to create a pair of files that share the same MD5 checksum. In an attack on MD5 published in December 2008, a group of researchers used this technique to fake SSL certificate validity.

IV Conclusion

In this paper, a hybrid security algorithm for VPNs is proposed. It is designed to solve several problems as practical implementation, short response time, efficient computation and strength of cryptosystem. The proposed HCA tries to trap the attacker by splitting the plain text and then applies two different techniques. First it takes the advantages of the combination of both symmetric and asymmetric cryptographic techniques using Aes algorithm. Second, XOR-DUAL-RSA is used since it is more robust and cannot be easily attacked. In addition, Hashing is also used for data integrity using MD5 to be ensured that original text is not being altered in the communication medium. The performance is compared with other existing security algorithms.

REFERENCES

[1] El. A, T. Abd El Al, T. N. Saadawi, and M. J. Lee (2004), "LS-SCTP: A bandwidth aggregation technique for stream control transmission protocol," *Comput. Commun.* vol. 27, no. 10, pp. 1012–1024, Jun. 2004.

[2] Alamgir, R., AT iquzzaman, M. and Ivancic, W. (2002). *Effect of Congestion Control on the Performance of TCP and SCTP over Satellite Networks*: proceedings of the NASA Earth Science Technology Conference, Pasadena.

[3] Alwin Thomas and George Kelley (2002), "Cost-Effective VPN-Based Remote Network Connectivity Over the Internet", 2002

[4] Arjen Lenstra (2001), "AES in security protocols", available at http://people.epfl.ch/arjen.lebstra , 2001

[5] Arno Wagner, Thomas Dubendorfer, Roman Hiestand, Christoph Goldi and Bernhard Plattner (2006), "A Fast Worm Scan Detection Tool for VPN Congestion Avoidance", DIMVA, 2006.

[6] Atkinson.R, (1998a).IP authentication header. RFC 2402. Available at http://www.ietf.org/rfc/rfc2402.txt.

[7] Atkinson.R, (1998b).IP authentication header. RFC 2406. Available at http://www.ietf.org/rfc/rfc2406.txt.

[8] D. Boneh, G. Durfee, "Cryptanalysis of RSA with private key d less than N (2000)**",** IEEE Trans. Inf. Theory, 46 (4), pp. 1339–1349

[9] W. Burr, "Selecting the advanced encryption standard (2003)", IEEE Secur. Priv., 1 (2), pp. 43–52

[10] M.J. Dubal, T.R. Mahesh, P.A. Ghosh (2011), "Design of a new security protocol using hybrid cryptography architecture", Proceedings of 3rd International Conference on Electronics Computer Technology (ICECT), vol. 5, India

[11] M. Frunza, Gh. Asachi(2007), "Improved RSA encryption algorithm for increased security of wireless networks", ISSCS International Symposium, vol. 2

[12] Md.A. Hossain, Md.K. Islam, S.K. Das, Md.A. Nashiry (2005), "Cryptanalyzing of message digest algorithms MD4 and MD5".

[13] Int. J. Cryptogr. Inf. Secur. (IJCIS), 2 (1) (2012), "A study of encryption algorithms (RSA, DES, 3DES and AES) for information security", Int. J. Comput. Appl., 67 (19), pp. 33–38,

[14] S. Subasree, N.K. Sakthivel (2010), "Design of a new security protocol using hybrid cryptography algorithms", IJRRAS, 2 (2), pp. 95–103.