A NEW COMMUNICATION PLATFORM FOR DATA TRANSMISSION IN VIRTUAL PRIVATE NETWORK

Farhad Soleimanian Gharehchopogh[1], Ramin Aliverdiloo[2], and Vahid Banayi[3]

[1,2,3]Computer Engineering Department, Science and Research Branch, Islamic Azad University, West Azerbaijan, Iran

[1]Bonab.farhad@gmail.com, [1]farhad@hacettepe.edu.tr,
[2]ramin.aliverdiloo@gmail.com, [3]vbs.banayi@gmail.com

ABSTRACT

Nowadays security is an evident matter in designing networks and much research has been done in this field. The main purpose of the research is to provide an appropriate instruction for data transmission in a reliable platform. One of the instructions of transferring information is to use public networks like internet. The main purpose of the present paper is to introduce that enables the users to enter to a new security level. In this paper, VPN as one of the different instructions for establishing the security proposed to be examined. In this type, tunneling method of internet protocol security (IPsec) is used. Furthermore, the advanced method of scanning fingerprint is applied to establish authentication and Diffie-Hellman algorithm for coding and decoding data, of course with conversion in this algorithm.

KEYWORDS

Authentication, Diffie-Hellman Algorithm, Virtual Private Network (VPN)

1. INTRODUCTION

Recently secure access to the private sources is considered as of the essential needs. Thus, one of the most efficient and cost-effective ways for granting secure access needs from far path in the organizations is the use of VPN [1]. There are two types of VPN technology including: IPsec and SSL. That in this paper the IPsec method is applied. IPsec is one of the most complete, secure, and accessible standards based on developed protocols for data transportation. In this method, in order to connect the tunneling method will be used. The VPNs that use the IPsec method make a tunnel between the starting and destination points which through it different protocols move e.g. web, e-mail, file transfer, VoIP, etc.[2] Most private networks lack data security and allow hackers to have access to read and attack the data directly. A VPN shares a network that data can be passed through the private traffic in the way that only authorized users have access to it. IPsec-based VPN uses encryption method for data security. In order to make this process possible, VPNs connect and combine public and private networks to each other, encrypt packets that are transferred in the net, and increase the resistance of net in front of hackers attack, data retouch, and robbery [3]. The main purpose of VPNs is to prevent the sniff of data that are being sent in the connection platform and the other one is to maintain the integrity of untrusted networks[4].

The other purpose of VPNs is to get access to common sources. Because the connection between these sources is secure, organization can allow its customers and partners to have access to information. Considering VPNs from user's point of view, they can be noticed as a point to point connection between computers and servers[5].

IPsec-based VPNs can be established on different types of networks such as ATM, Frame Relay, MPLS, and internet. Since the internet is cheaper and accessible, however, users prefer to use it instead. There are different types of virtual private networks. whit due to operational requirements, however, several ways to create each of these VPNs are available[8]. In the method we present, at first, by using high-security devices like scanning fingerprint, an authentication is established between two organizations. After establishing connection, the data are coded by (modified) Diffie-Hellman algorithm. Then, these data are sent and after receiving data in the destination, they are decoded. Therefore, the connection among organizations is completely secure and the probability of attacking data by hackers decreases remarkably.

Ram raj [6] proposed a new encryption protocol for data in VPN and a management key that in this model VPN server is a trusted one. In this model VPN server is a trusted one. In this method, Customer presents his request to VPN server and it assigns a key value for customer. Thus, customer begins encrypting data by using this key and advanced encryption standard AES. In this method, the customer receives a public key and with this key the user is able to send data. There is a private key in VPN server that enables the customer to identify the value of the main key. And by RSA encryption algorithm can decode the coded information again, so we can say this method has high security. M.C.Nicalescu [7] has presented IP mobile security in VPNs. At first AH, ESP examined the defined protocols in IKE in IPsec-IETF architecture. Based on these protocols, protection against denial of viruses, sniff and the other active dangers was discussed. This paper developed this discussion to a large scope called “Internet”. In which the use of secure tunneling as a main protective mechanism was tested.

This paper organized as follows: in the next section the previous works that have been done in this case are discussed. In section 3 IPsec protocol is reviewed. In section 4 the peer authentication methods are surveyed. In section 5 the Diffie-Hellman algorithm which is a powerful algorithm for coding is surveyed. In section 6 the proposed method will be discussed which is done in two parts of authenticate: with applying the modified Diffie-Hellman algorithm until decreasing the fail our percentage of code, and the sample practical scenario will be shown. Section 7 is surveying and discussion. Section 8 presents the results and future works and finally section 9 is references.

2.OVERVIEW OF INTERNET PROTOCOL SECURITY (IPSEC)

The following formatting rules must be followed strictly. This (.doc) document may be used as a template for papers prepreferences. IPsec is a type of protocol which is used for funding, data integrity and confidential data. IPsec works in IP layer [9]. IPsec is the safest way to connect to available business network website.

2.1 IPC Security Features

There are some methods in IPsec which are used to present security features that definite the kind of security sending packages in the network. Here are some of them:

Authentication: Authentication or identification attaining means the two organizations can have authenticity with each other [9]. It is the first step in security, because first two organizations should know each other and then act to send information.

Data integrity: Data integrity guarantees that package contents have not changed during transportation process [9]. It checks whether a bit has been changed during path or not and this is done by its special algorithms.

Confidentiality: Confidentiality encrypts the package contents by coding method [9] and it is done after two organizations knew each other that with sniff on the path package don't be easily readable. Replay Detection: This has the capability of recognition [9]. If two organizations can connect with each other, someone may attack the package and take it. But if he cannot open and decrypt the package the router will find out that the package is not new. So replay detection supports this connection.

2.2 IPSEC Component

IPsec standard includes two following parts:

Encapsulation Security Payload (ESP): This protocol has 50 numbers which is allocated to it by (IANA) [10]. ESP is kind of protocol which is safely responsible to receive data from resource and send them to the destination [10]. To make this work possible, method like coding and decoding are used so that only sender and receiver can be allowed to read the data [8]. As you can see in figure (8:2-1) it is clear that ESP encrypts up to three layers and in order to preform routing operation, it adds an IP header to the package. ESP follows every four IPsec security features.

Authentication Header (AH): This protocol has number 51 which is allocated to it by (IANA) [11]. AH is devoted to authentication and never codes the data. This protocol is used only to authentication the data from sender. AH uses two of IPsec security features as follows: Authentication, Data integrity. As you can see, ESP has a remarkable security level; But AH has a high security level for authenticity, too. Thus, everywhere high security is proposed both of them and used simultaneously, but in this way devices suffer high overhead. SHA1 and MD5 are kinds of coding algorithms that are used in AH and ESP applied for authenticate and data integrity, And AES, 3DES, DES algorithms are ones that support confidentiality which only used in ESP. Internet Key Exchange (IKE): Internet key exchange is the contracted form of security association internet and the management of protocol key. And it is a protocol which is responsible for discussion [12]. This method in IPsec-based VPNs includes three phases. Which the first and the second phase are used in site to site VPNs as has explained below:
-Phase 1: This is called ISAKAMP phase and its duty is to establish authentication among neighbors. In this phase detection has been done between two organizations with the use of authentication methods supplying before like preshared keys. Common algorithm for two phases of 1 and 2 in the IPsec method is called Diffie-Hellman [8].
-Phase 2:This is called IPsec phase that is responsible for transmitting data encrypted. Diffie-Hellman [12] algorithm (fig. 1) is used for transmitting data [8]. As you can see in the reference figure [9:6-11], IKE model has two phases: The first phase is called ISAKAMP which itself has six main states and the second one which is called IPsec has three fast states.

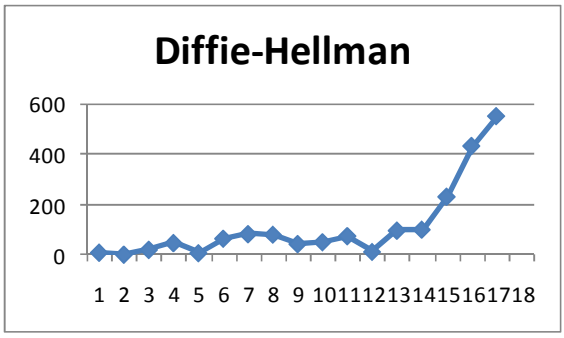

Fig 1: Diffie-Hellman algorithm analyze

3. Peer authentication methods

As mentioned before, one of the important principles in establishing security through VPNs is authentication. In order to perform this work we can make use of following methods:

Username and Password: "Username and Password" is one of the common ways in easy VPNs or the same client to site VPN. In this method there is a VPN server [9] that clients are authenticated by "Username and Password". This server provides a secure place in internet.
OTP (PIN/TAN): In this method, a special code is created by using a special calculator, but this code has authenticity constraint. This method is used to establish authentication [9].

Preshared keys: This is another method for authentication. Through this method a common code is used to connect among organizations.

Digital certificate: This is another suitable instruction that makes use of digital signatures to establish authentication.

Biometric: Using hardware machines is a suitable instruction to increase the security level. Biometric device provides secure availability to network using hardware's [9]. There are different types of biometrics:

Bertillon age: This is the first type of biometric which was created by allfonce in 1980 [15]. This method is based on measuring human anatomy that includes measuring different parts of human body such as height, arm length, finger length, etc. [15]. But this method has a problem: There is the possibility of people with the same profile and because of this reason the above method wasn't used anymore.

Fingerprint Recognition: That is to take a photo from the tip of finger includes features such as grooves, loops, and arches [15]. There are another biometric devices, but in this paper we use the fingerprint recognition.

4. Data Encryption

After establishing authentication, it is time to send data. Diffie-Hellman algorithm is one of proper algorithms which uses the encryption method to perform this process. There are large numbers of these algorithms (about six) and this algorithm was employed in cisco device [9]. The procedure of Diffie-Hellman algorithm allows two organizations to produce a common key. After producing this key, they should send data by symmetric key encryption [16].

5. Case Study

As mentioned above, in order to send information in internet using VPNs, we employ two consecutive methods to provide security. One of these methods is in authentication section and the others are in coding section. And here are presented new instructions that include:

5-1: As stated before use IKE method who's the first phase is associated with authentication argument. Although nowadays "Username and Password" and preshared key methods are very common in most of the VPNs. The problem, however, is that probably the third person may sniff the content of packages in the path and decode and abuse "Username and Password" or preshared methods. It causes low security level percentage. Thus, here must be an instruction which cannot

be easily discovered. To do so biometric method is offered in this paper. As mentioned before, among different types of biometric devices, fingerprinting scan is used here to establish authentication among organizations. Since everybody has a unique fingerprint, it probability decreases to use it again event if attackers sniff it in the path they cannot use it because of its uniqueness. There are two ways to use fingerprinting: One of them is using its own fingerprinting scan device directly, and the other is using code intellectual devices USB that is done easily with any program. Code intellectual USBs have three models among which esign BTO is used for fingerprinting. Esign BTO: This program has basic capacities for an intellectual code to make authentication. This USB is a developed copy of STD model with Biometric increased module fingerprint that is used to enter [14]. Because every human begin has a unique fingerprinting, the abuse of this method will be decreased remarkably. Even if attackers can find out the authentication method they cannot use it.

5-2: As mentioned before, after authentication the discussion is related to data coding. In this paper some changes are done Diffie-Hellman algorithm [16] in order to reduce coding failure extremely. One way to work with Diffie algorithm is first to define to same p, g amounts in two destinations and then to produce the same key mathematical and start to send data according to that key. Here a numerical sample of Diffie-Hellman is shown and the next section deals with proving that the modified algorithm is the best. The following algorithm is a sample of Diffie-Hellman algorithm [16].

1. Alice and Bob agree to use a prime number p=23 and base g=5.
2. Alice chooses a secret integer a=**4** and, then sends Bob A = g^a mod p
   - A = 5^6mod 23
   - A = **625** mod 23
   - A = 4
3. Bob chooses a secret integer b=**10**, and then sends Alice B = g^b mod p
   - B = 5^{10} mod 23
   - B = **9765625** mod 23
   - B = 9
4. Alice computes **s** = B^a mod p
   - **s** = 9^4 mod 23
   - **s** = **6561** mod 23
   - **s** = **6**
5. Bob computes **s** = A^bmod$p$
   - **s** = 4^{10} mod 23
   - **s** = **1048576** mod 23
   - **s** = **6**
6. Alice and Bob now share a secret: **s** = **6**. This is because 4*10 is the same as 10*4. So somebody who had known both these private integers might also have calculated s as follows:
   - **s** = 5^{4*10}mod23
   - **s** = 5^{10*4} mod 23
   - **s** = 5^{40} mod 23
   - **s** = **909494701772928237915039062 5**
   - **s**= **6**

Now by performing following modifications in Diffie-Hellman algorithm [16] and checking the numbers above, following result will be gained.

P1=2*g+1, P2=2*p+1, a and b plus v

1. Alice and Bob agree to use a prime number p=23 and base g=5, v=2.
2. $P1=2*q+1$, $p2=2*p+1$
3. Alice chooses a secret integer ***a*=4** and **t1=a+v**, then sends Bob A = $p1^{t1}$ mod $p2$
   - A = 11^{6}mod 47
   - A = **1771561** mod 47
   - A = 37
4. Bob chooses a secret integer ***b*=10**, and **t2=b+v** then sends Alice B = $p1^{t2}$ mod $p2$
   - B = 11^{12} mod 47
   - B = **3138428376721** mod 47
   - B = 6
5. Alice computes **s** = B^{t1} mod $p2$
   - **s** = 6^{6} mod 47
   - **s** = **46656** mod 47
   - **s** = **32**
6. Bob computes **s** = A^{t2} mod $p2$
   - **s** = 37^{12} mod 47
   - **s** = **6582952005840035281** mod 47
   - **s** = **32**
7. Alice and Bob now share a secret: **s** = **32**. This is because 6*12 is the same as 12*6. So somebody who had known both these private integers might also have calculated s as follows:
   - **s** = 11^{6*12} mod 47
   - **s** = 11^{12*6} mod 47
   - **s** = 11^{72} mod 47
   - **s= 90555938177273214530938076429508e+74**
   - **s** = **32**

As you see, because of modifications performed on the algorithm, the created numbers grow and these numbers will have a less defeat possibility. So, sniffer must analyse more in order to be able to obtain a public key.

5-3: Partial Scenario Sample:

(1. R1(config) #ip route 192.168.24.0 255.255.255.0 1.1.46.4

2. R1 (config) #crypto isakmp policy 10

3. R1 (config-isakmp) #authentication Biometric

4. R1 (config-isakmp) #enc 3des

5. R1 (config-isakmp) #hash md5

6. R1 (config-isakmp) #group 1

7. R1 (config) #crypto isakmp policy 20

8. R1 (config-isakmp) #authentication Biometric

9. R1 (config-isakmp) #encaes 128

10. R1 (config-isakmp) #hash sha

11. R1 (config-isakmp) #group 2

12. R1 (config-isakmp) #ex

13. We can choice biometric device

14. R1 (config) #crypto ipsec transform-set TS1 esp-des esp-md5

15. R1 (cfg-crypto-trans) #mode tunnel

16. R1 (cfg-crypto-trans) #ex

17. R1 (config) #ip access extended INT_TRAFFIC

18. R1 (config-ext-nacl) #permitsip 192.168.13.0 0.0.0.255 192.168.24.0 0.0.0.255

19. R1 (config-ext-nacl) #ex

20. R1 (config) #crypto map R1 10 ipsec-isakmp

21. R1 (config-crypto-map) #match address INT_TRAFFIC

22. R1 (config-crypto-map) #set transform-set TS1

23. R1 (config-crypto-map) #set peer 1.1.46.4

24. R1 (config-crypto-map) #ex

25. R1 (config) #int f0/1

26. R1 (config-if) #crypto map R1)

Above command line reference is [13]

In order to connect with other organizations, IP route is written in the first line. Then the possibility of connection with other organizations by tunnelling method will be demonstrated. The lines 2 to 6 show the policies by which data encryption and authentication are performed. These policies are defined by authorities, but these policies must be equal in both sides. In the case, there are a lot of policies; the priority is from top to bottom. For example number 10 policy is compared orderly with the policies in the other side of the router have been set and synchronized with considered policy. The line 3 shows the authentication and the type of device can be chosen in line 13 after defining policies. In line 6, the authorities are allowed to choose the type of decrypt and decryption of data. As mentioned before, a group of Diffie-Hellman algorithms were implemented on cisco routers which are used in policy 10 from group 1 and in policy 20 from group 2. The line 14 to 26 is used for setting. The router R2 must be set, too(fig .2).

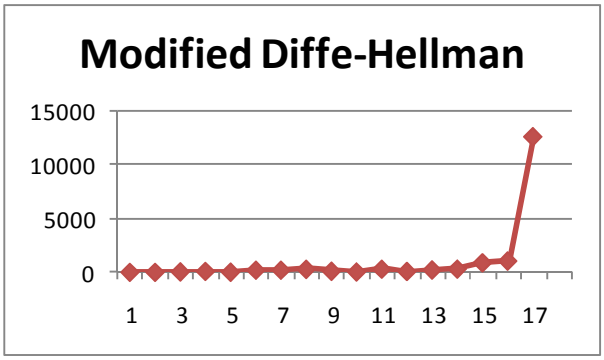

Fig 2: Both of them analyze

6- Discussion

As stated before, security is one of the most attractive discussions of the world, since increasing number of data transportation is done from the platforms like internet. Thus all of organization is looking for some ways to send their data safely without hackers, accessibility to their information. One of the security software instructions is to use VPNs. The focal point of this paper is about authentication and data encryption which are discussed, here. The first step in security is authentication, therefore, the organizations should truly connect together in order to start sending data.

In modern VPNs are used two methods: preshared key and "Username and Password". But there is a problem in both methods. There may be a third person that may use them too and break the first step of security. Also there is much software that can easily take hacked account and change their real account. So when the two above methods are used to be decoded and used the possibility of using it by the third person exists. Using fingerprinting scan increases the security level in authentication because every person's fingerprinting is unique. Even by sniffing they are not easily decoded and reused. But there's a problem in this method, too; in this method it should be applied a hardware machine that gets to cost. But due to less possibility to decode, it is an appropriative instruction for organizations that security level is very important for.

The second part in security discussion is data encrypt. After presenting the suitable authentication it is turn to send information. Despite the fact that the route has become secured, the data should be coded, again, to increase the security.

Used algorithm in site to site VPN is Diffie-Hellman algorithm that sample of it illustrated in the previous part and some modifications were done in order to increase the common number that is produced to make it greater and respectively to reduce the failure possibility. And here for comparing two algorithm Matlab software is used and for different several repetition of each following results are gained as you see in the second method produced numbers got 10 ^27 and in the first method 10^9. Produced numbers in modified diffie-hellman algorithm have been made larger over 18 times and this needs many times to be decoded and so increases the security level so much (fig.3).

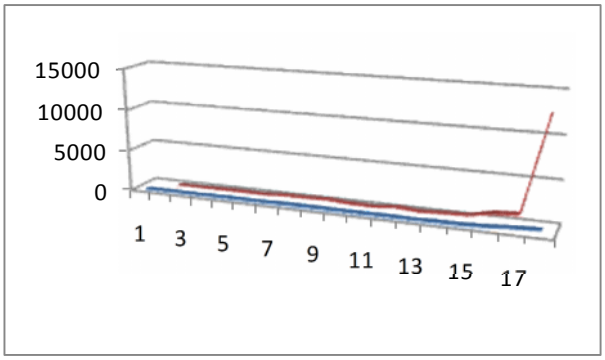

Fig 3: Modified Diffie-Hellman analyze

8 CONCLUSION

Security is essential requirement in network-based connection especially in unsecure platforms. Among enormous offers have been made, VPN is an example of them. Authentication establishment by the means of biometrics leads to increasing the security of them. Therefore for maximizing security using these devices are highly recommended. Also by using the secure encryption algorithms such as modified Diffie-Hellman [16] the safety of information from hacker attacks will increase.

By more frequent and easier access to biometric devices, the possibility for comfortable and safe use of information will increase, in the future.

REFERENCES

[1] A.Thomas, G.Kelley," Cost-Effective VPN-Based Remote Network Connectivity over the Internet", Department of Computer Science,University of Massachusetts,100 Morrissey Boulevard,Boston, MA 02125-3393,2002.

[2] S.Kadry, W.Hassan, "Design and implementation of system and network security for an enterprise with worldwide branches", *Journal of Theoretical and Applied Information Technology*, *School of Engineering*, LIU, Beirut, Lebanon ,2008

[3] "Security & Savings with Virtual Private Networks", available:http://tools.netgear.com/media/whitepapers/VPN_Security.pdf. Last Available 02,08,2012.

[4] E. Ramaraj and S. Karthikeyan,"A New Type of Network Security Protocol Using Hybrid Encryption in Virtual Private Networking", *Journal of Computer Science*, Vol: 2, No: 9, pp: 672-675, 2006.

[5] M. C. Niculescu, Elena Niculescu,and I. Resceanu, "Mobile IP Security in VPNs", 5th WSEAS Int. Conf. on Data Networks, Communications & Computers, Bucharest, Romania, October 16-17, pp:119-124, 2006.

[6] Netgear, Virtual Private networking,24,santacalara, 4500 Great America Parkway Santa Clara, CA 95054 USA, Available: http://documentation.netgear.com/reference/nld/vpn/pdfs/FullManual.pdf. Last Available: 02.08.2012.

[7] G. Bastian, E.Carter, C.Degu, "CCSP Cisco Secure PIX Firewall Advanced Exam Certification Guide", Cisco Press, 808, Indianpolis, IN 46240 USA, 2005.

[8] IP Encapsulating Security Payload, Network Working Group, Request for Comments: 2406, Obsoletes: 1827, Category: Standards Track, @Home Network November 1998

[9] IP Authentication Header. Network Working Group, Request for Comments: 2402, Obsoletes: 1826, Category: Standards Track, @Home Network November 1998

[10] Internet Key Exchange protocol , Copyright Ó 2001, Cisco Systems, Inc., Acces VPN v1.0

[11] Cisco IOS VPN Configuration Guide, Site-to-Site and Extranet VPN Business Scenarios, OL-8336-01

[12] Softlock Secure VPN Access Solution, Availabel: www.softlock.net/Softlock-Secure-VPN-Access-Solution-Document.pdf. Last Available: 02.08.2102

[13] S. Angle, R. Bhagtani, H.Chheda,"Biometrics: A Further Echelon of Security", Department of Biomedical Engineering, ThadomalShahani Engineering College, T.P.S III, Bandra, Mumbai-50. Pp.1. Jan.2005.

[14] Diffie–Hellman key exchange, Wikipedia, http://en.wikipedia.org/wiki/Diffie-Hellman_key_exchange. Last Available: 02.08.2012.