Learning Tool for IPSEC with Emphasis on the Use of MGRE in Corporate Networks

Herramienta para el Aprendizaje de IPSEC con Énfasis en el Uso de MGRE en Redes Corporativas

ANDRÉS MAURICIO RAMÍREZ
Electronic Engineering
ZTE Corporation
andresxbsb@yahoo.com.ar
Bogotá, Colombia

OSCAR POLANCO SARMIENTO
Specialist in Computers and Digital Systems
Universidad del Valle
oscar.polanco@correounivalle.edu.co
Cali, Colombia

FABIO GERMÁN GUERRERO
Master in Electronic Engineering
Universidad del Valle
fabio.guerrero@correounivalle.edu.co
Cali, Colombia

Fecha de recepción: 09/08/2012
Fecha de aprobación: 11/05/2013

ABSTRACT

This paper presents a tool named "UV IPsec Tools", developed to understand and interact in a didactic way with the transformations performed by IPsec when using the MD5, SHA-1 and 3DES algorithms for the encryption and integrity check of an IPv4 datagram. As an example, we present the implementation of a corporate network using Dynamic Multipoint Virtual Private Networks, which are based on the establishment of dynamic tunnels protected by IPSec. The tool was developed in Java and with the help of another program we developed, it was possible to validate the code for the MD5 and SHA-1 algorithms with 14 test vectors as specified in RFC 2202. Also, to show an application on IPsec, the design, configuration, emulation and validation of three private networks connected via the public Internet using GNS3 was made.

KEYWORDS: IP security, DMVPN, mGRE, ESP, AH, 3DES, SHA-1.

RESUMEN

Este artículo presenta la herramienta "IPsec Tools UV", desarrollada para entender e interactuar de una manera didáctica con las transformaciones que realiza IPsec cuando usa los algoritmos MD5, SHA-1 y 3DES durante la verificación de integridad y cifrado de un datagrama IPv4. Como ejemplo se presenta la implementación de una red corporativa usando Redes Privadas Virtuales Dinámicas Multipunto, las cuales se basan en el establecimiento de túneles dinámicos protegidos por IPsec. La herramienta fue desarrollada en Java y con el apoyo de otro programa desarrollado fue posible validar el código de los algoritmos MD5 y SHA-1 con 14 vectores de prueba especificados en la RFC 2202. Además, para mostrar una aplicación de IPsec, se hizo el diseño, configuración, emulación y validación de tres redes privadas conectadas a través de la Internet pública utilizando el software de emulación GNS3.

PALABRAS CLAVE: IP security, DMVPN, mGRE, ESP, AH, 3DES, SHA-1.

1. INTRODUCTION

When IPsec (Internet Protocol Security) is configured to provide integrity checks using either the AH (Authentication Header) or ESP (Encapsulating Security Payload) protocol [1], the HMAC (Hashed Message Authentication Code) algorithms that are commonly available in most computer networks are MD5 (Message-Digest algorithm 5) and SHA-1 (Secure Hash Standard version 1). Despite the superiority of SHA-1 over MD5, recent research suggests that it will require only 2^{52} operations to undermine the resistance to collisions of SHA-1 [2]. This suggests that in the short or medium term a transition will be necessary from SHA-1 to an algorithm more resistant to collisions, such as SHA-2. Currently, there are several applications based on SHA-1 signatures that enjoy widespread popularity and acceptance: the Digital Signature Algorithm, the message format OpenPGP (Open Pretty Good Privacy) defined in RFC 4880 [3], the concept of Trust in the Web in systems compatible with OpenPGP, and the IPsec protocol. Additionally, in the router configuration, the options for encryption algorithms that can be used for the ESP protocol are 3DES (Triple Data Encryption Standard) and AES (Advanced Encryption Standard). Similarly, the authentication between two routers in phase 1 of IKE (Internet Key Exchange) can be configured so that they make use of shared keys or so that it is based on RSA´s (Rivest, Shamir and Adleman) public key algorithm.

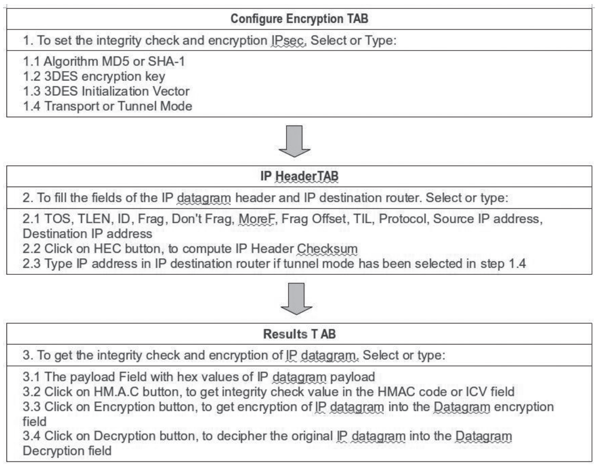
When trying to observe the IP datagrams protected by IPsec with a packet sniffer tool such as Wireshark, it is only possible to interpret the datagram fields that have not been encrypted [4]. To understand and interact with the IPsec processing performed by the MD5, SHA-1 and 3DES algorithms, a tool called “IPsec Tools UV” was developed. With this tool, it is possible to type in the header fields in the original IP datagram, define integrity checking algorithms with their respective HMAC keys, specify the key and initialization vector for the 3DES algorithm, define the operation mode of IPsec as tunnel or transport, specify the destination IP address to the IPsec tunnel, complete the IP datagram payload field, obtain the hexadecimal data for integrity checking and encryption of the original datagram and retrieve clear text (as a hexadecimal string) of the original IP datagram with the information added by IPsec before encryption. The “IPsec Tools UV” tool was developed in the absence of any tool that provides the above functions. It requires no prior knowledge of the keys to decipher the fields of the IP datagrams, and also it is of public use and portable. The tool was developed in Java and the following aspects were considered in the design of it: ease of use, portability, provides default values in user fields, and the ability to validate MD5 and SHA-1 algorithms. Tools like NIIST (NIST IPsec and IKE Simulation Tool) [5] have a different scope because they are designed mainly to evaluate and investigate IPsec performance in large-scale virtual private network environments, with emphasis on IKE

As an IPsec application, we test the emulated company’s private networks interconnected via the Internet with proper protection provided by IPsec [6]. The most commonly used topology is called Hub-Spoke, which uses a tunnel to connect each remote router to the central router. One disadvantage of this configuration is that when the communication takes place between two remote offices, information must pass through the central site, precluding the use of the best available route on the Internet between the two remote sites, which may be critical for delay-sensitive applications such as VoIP (Voice over IP). Another disadvantage is related to configuration management: for each new remote router, some additional lines in the central router must be configured. To overcome these restrictions and provide a solution to the problem of scaling, a design concept known as DMVPN (Dynamic Multipoint Virtual Private Network) can be exploited, using a single multipoint tunnel called mGRE (Multipoint Generic Routing Encapsulation) [7; 8] superimposed over the Internet and with their end points protected by IPsec. The configuration of the tunnel makes use of NHRP (Next Hop Resolution Protocol) [9]. Of course, when attempting to deploy this technology directly in the field without the necessary experience and control logistics, too much time can be wasted before success. For this reason, it is desirable to emulate in a controlled environment the network setup, validate and tune the design and identify the tasks to be carried out in the field. This can be accomplished using physical routers or emulation tools such as Dynamics under the GUI provided by GNS3 [10]; We choose the latter option. This allows considering the GNS3 emulation as a useful option for ISPs when they require exploring prior to actual IPsec Implementation.

2. METHODOLOGY

2.1 Basic IPSEC algorithms: integrity verification and encryption

The development of the “IPsec Tools UV” tool was done using the Java programming language because it provides high-level programming and has libraries and APIs that incorporate security algorithms such as MD5, SHA-1 and 3DES. This tool allows to analyze the transforms that occur in an IP datagram when this is processed at the end of an IPsec tunnel, it provides a basic interactivity interface with an integrity verification function for SHA-1 or MD5 algorithms and encryption function for the 3DES algorithm; such algorithms are used for the protection of IP datagrams. Figure 1 shows a block diagram representing the logic structure of the "IPsec Tools UV" tool. A user can use the tool in three steps. In the first step, the user manages the configuration information related with the integrity verification algorithm and encryption algorithm on the "Configure Encryption" Tab. In the second step, the user fills in 11 fields of the IP datagram header and the "IP destination router" field on the "Header IP" Tab. In the third step, the user can type a string of hexadecimal values representing the payload of the IP datagram and display the results of the integrity check and encryption of IPsec on the "Results" Tab. Using this Tab, the user can also decrypt the previously encrypted IP datagram.



Configure Encryption TAB

1. To set the integrity check and encryption IPsec. Select or Type:

1.1 Algorithm MD5 or SHA-1
1.2 3DES encryption key
1.3 3DES Initialization Vector
1.4 Transport or Tunnel Mode

IP HeaderTAB

2. To fill the fields of the IP datagram header and IP destination router. Select or type:

2.1 TOS, TLEN, ID, Frag, Don't Frag, MoreF, Frag Offset, TIL, Protocol, Source IP address, Destination IP address
2.2 Click on HEC button, to compute IP Header Checksum
2.3 Type IP address in IP destination router if tunnel mode has been selected in step 1.4

Results T AB

3. To get the integrity check and encryption of IP datagram. Select or type:

3.1 The payload Field with hex values of IP datagram payload
3.2 Click on HM.A.C button, to get integrity check value in the HMAC code or ICV field
3.3 Click on Encryption button, to get encryption of IP datagram into the Datagram encryption field
3.4 Click on Decryption button, to decipher the original IP datagram into the Datagram Decryption field

Figure 1. *Structure logic of "IPsec Tools UV" tool*

2.2 Design of a dynamic multipoint virtual private network

The strategy for validating a network's ability to establish dynamic tunnels on the Internet under DMVPN was conducted in three steps. The first step was to undertake a network design taking into account the user needs in terms of requirements for public and private IP addresses. The second step was to connect and configure four routers that represent a sample of the user´s network, including a router that represented the Internet. Finally, the results were observed and documented in order to adjust them and apply them in practice.

Figure 2 shows the design of a network that uses DMVPN as a direct application of IPsec. The network is made up of four routers, the router whose name is R4-Internet emulates the Internet, its functions can be performed by any Layer 3 switch. The R4-Internet router knows only about the existence of three public IP networks directly connected to it whose addresses are: 12.34.56.0/24, 23.45.67.0/24 and 34.56.78.0./24. The R1 router assumes the role referred to as "Hub router", this is connected to the LAN1 private network (192.168.1.0/24) and has a connection to the Internet. The R2 and R3 routers have a role referred to as "Spoke router", these are connected to the LAN2 private network (192.168.2.0/24) and LAN3 private network (192.168.3.0/24), respectively. Both have Internet connections. Also, in relation to routers R1, R2 and R3, it is important to verify first if their operating systems have DMVPN operation capabilities. In practice, the LAN1 network could represent the main headquarters network of a corporation while the LAN2 network and LAN3 network could represent two branches of the same corporation.

In a conventional topology of type "Hub-spoke", the connection of each remote network with the central network is done by setting a static tunnel between the central router and each of the remote routers. Accordingly, each new remote network will require additional configuration lines in the central router. Additionally, the voice and data traffic between two remote sites must go through the first tunnel between one of the remote sites and the central router, and immediately such traffic should enter into a second tunnel that will lead to the network of the destination remote site. Although the Hub-spoke topology is an acceptable solution which allows internetworking of private networks via the Internet, it can have drawbacks with scaling in more complex situations or when it is used for applications between two remote sites which demand the lowest possible delay.

Figure 3 shows a mGRE tunnel overlaying the Internet, as if it were a new IP logic multipoint network. In this network there are three interfaces that receive the assignment of IP addresses within the 192.168.0.0/24 range. To differentiate the IP addresses assigned to the logical interfaces that belong to the multipoint tunnel (192.168.0.1/24, 192.168.0.2/24 and 192.168.0.3/24) from the IP addresses assigned to physical interfaces connected to the Internet, the latter are called "physical addresses" since they correspond to physical interfaces in the routers. As can be appreciated, a mGRE tunnel allows to have more than two network interfaces and it can be treated primarily as a multi-access network without broadcast support. Such networks are also called type NBMA networks (non-broadcast multi-access).

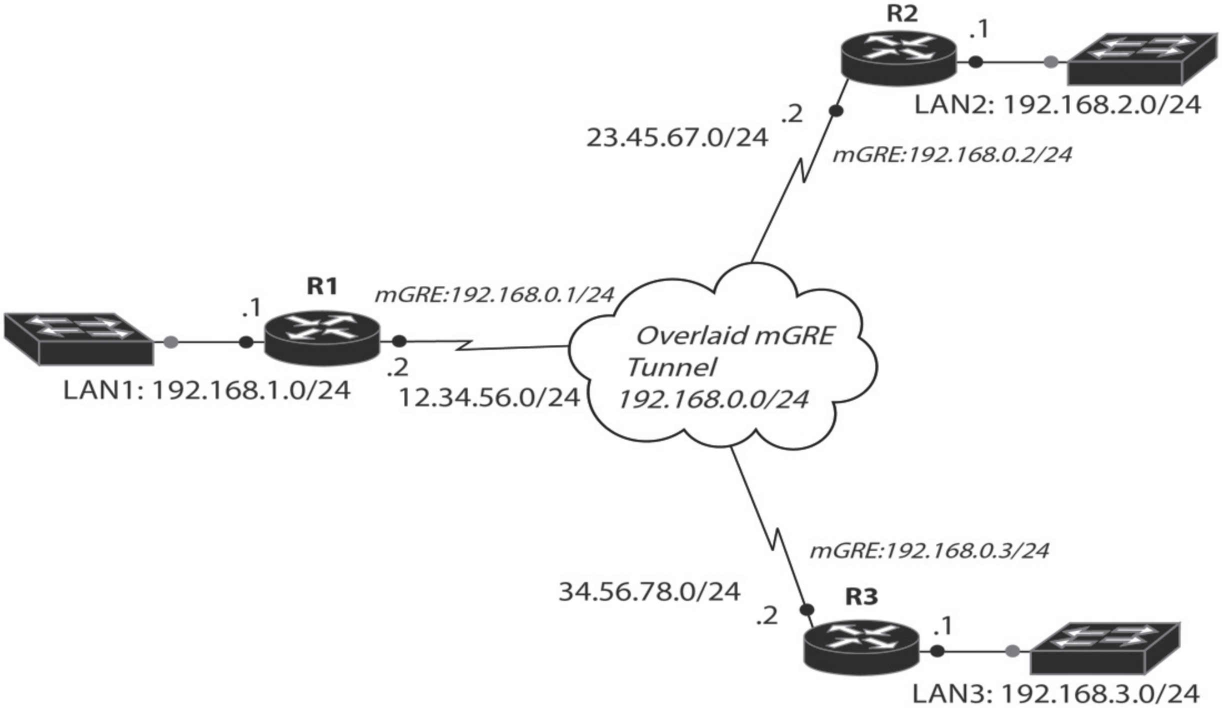


Figure 2. *Three Local Area Networks with connection to Internet*

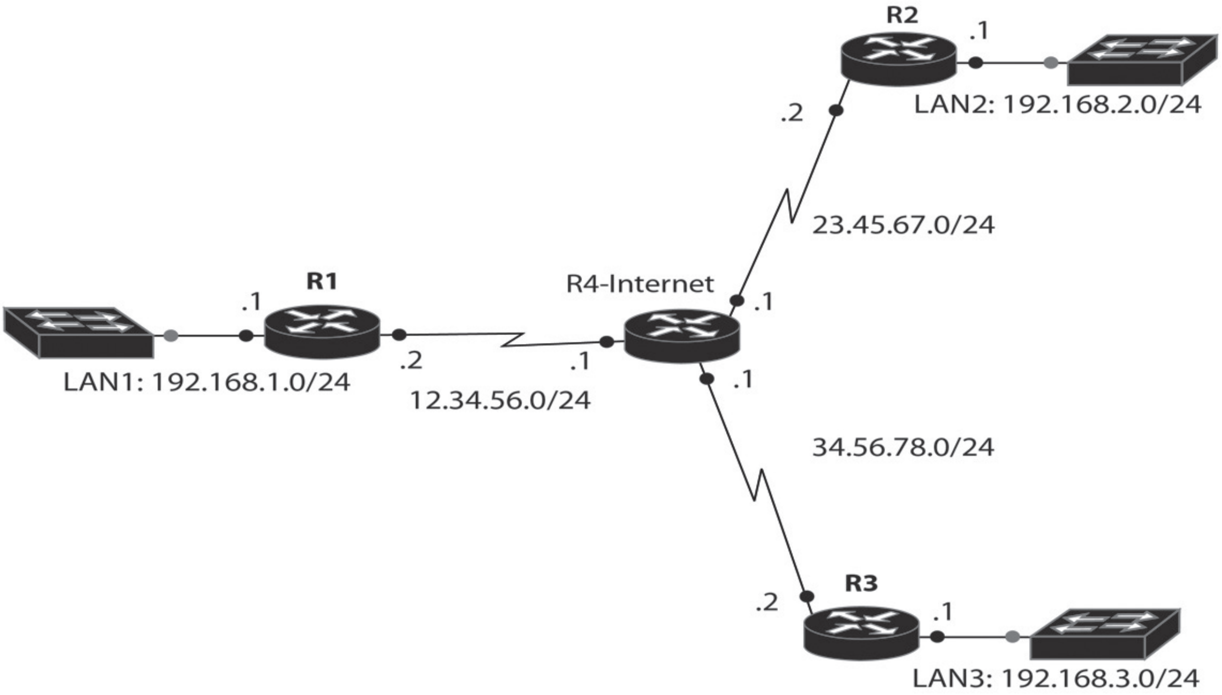


Figure 3. *A mGRE tunnel overlaying the Internet*

2.3 Dynamic multipoint virtual private network configuration

The R4-Internet router in this example represents the Internet. The R1, R2 and R3 routers have some of their interfaces configured with public IP addresses, as if they were connected to the Internet. Other interfaces of the R1, R2 and R3 routers are configured with the private IP addresses of their respective local area subnetworks. Each of these routers has the IP address of the next hop that allows an Internet connection as their default gateway (the nearest IP address to the R4-Internet router). For example, R1 has as default gateway 12.34.56.1.

In the operation of DMVPN, R1 has the role of NHS (Next Hop Server). The following command lines allow to configure DMVPN [11] at R1:

```
1. interface Tunnel0
2. ip address 192.168.0.1 255.255.255.0
3. ip nhrp map multicast dynamic
4. ip nhrp network-id 1
5. tunnel source 12.34.56.2
6. tunnel mode gre multipoint
```

In the above lines, it can be seen that the tunnel, configured to operate in multipoint GRE mode, does not have an explicit destination IP address. This is because the multipoint tunnels are created in a dynamic way, as initiated from the remote routers to the central router, thereby avoiding the need to configure the addresses of the remote routers in the central router. The line 4 “ip nhrp network-id 1” uniquely identifies the DMVPN network and avoids the formation of tunnels with routers that have different identifiers. The line 3 “ip nhrp map multicast dynamic” allows forwarding of multicast traffic through the tunnel to the remote routers, which is required by most routing protocols. Configuration of remote routers is very similar to that of R1. In the configuration of R2 that is presented below, there are two new commands: line 12 “ip nhrp nhs 192.168.0.1” designating the IP address of the interface tunnel of R1 as the next hop server and line 9 “ip nhrp map 192.168 .0.1 12.34.56.2 “ making a static association of the IP address of the next hop server with the IP address of the physical interface of R1. Finally, line 10 “ip nhrp map multicast 12.34.56.2” allows multicast traffic only from the remote router to the central router and not between remote routers.

```
7. interface Tunnel0
8. ip address 192.168.0.2 255.255.255.0
9. ip nhrp map 192.168.0.1 12.34.56.2
10. ip nhrp map multicast 12.34.56.2
11. ip nhrp network-id 1
12. ip nhrp nhs 192.168.0.1
13. tunnel source 23.45.67.2
14. tunnel mode gre multipoint
```

2.4 Routing protocols and security configuration

Since the mGRE tunnel behaves like an NBMA multipoint network which functions to interconnect private subnets LAN1, LAN2 and LAN3, a dynamic routing protocol must be enabled to allow automatic exchange of routing information to make each router known directly. In this case we have chosen the protocol OSPF (Open Shortest Path First) due to its high scalability. To ensure optimal operation such that traffic exchanged between routers R2 and R3 does not have to go through R1, the DMVPN cloud should be treated as if it were a broadcast network like Ethernet. In this way, when the central router reflects the routes, the next hop IP address value obtained by the remote routers is the address best suited for communication between them. Therefore, the R1 tunnel interface must be configured in broadcast mode (line 18 “ip ospf network broadcast”).

The OSPF priorities are set to ensure that the central router is always the DR (Designated Router) and that the remote routers are not elected as DR or BDRS (Backup Designated Router). This means that only the central router should be able to generate and replicate multicast IP datagrams to all remote routers. The only difference between configuring OSPF on R2 and R3 compared to configuring OSPF on R1, is that for R2 and R3 the OSPF priority is set to zero (with “ip ospf priority 0”). The configuration lines for R1 are shown below.

```
15. router ospf 1
16. network 192.0.0.0 0.255.255.255 area 0
17. interface Tunnel0
18. ip ospf network broadcast
19. ip ospf priority 10
```

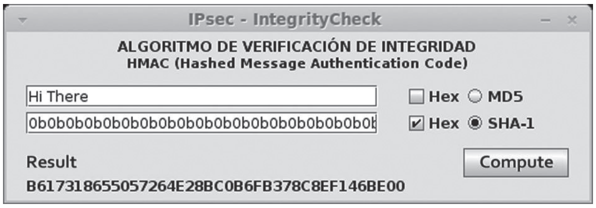
Since multipoint tunnels use an infrastructure without security guarantees like the Internet, their protection must be enabled through IPsec. In general, to activate IPsec protection four configuration steps that are related should be carried out as explained briefly in the following. The first step is to define an ISAKMP (Internet Security Association and Key Management Protocol) policy for authentication. This has the goal of selecting the authentication mode (shared key or public key), encryption algorithm, integrity check algorithm, with parties agreeing on the parameters to use in the authentication phase (lines 20 to 23). In the second step, a set of transforms is created which define the encryption protocol (ESP) and its associated algorithms (3DES, AES), as well as the integrity check protocol (ESP or AH) and its associated algorithms (SHA-1 , MD5) (line 25). In the third step, the set of transforms (defined above) is associated to a profile identified by a name (lines 27 to 28). Finally, the profile name is applied to the tunnel interface to be protected (lines 30 to 31). Below are the configuration lines that enable protection of the R1 tunnel interface using IPsec. Configuration of R2 and R3 is similar to R1, except for the physical interface addresses to which each configuration line (“crypto isakmp key Pa8sw0rd address”) must refer to according to the router which is to be configured.

```
20. crypto isakmp policy 10
21. authentication pre-share
22. crypto isakmp key Pa8sw0rd address 23.45.67.2 255.255.255.0
23. crypto isakmp key Pa8sw0rd address 34.56.78.2 255.255.255.0
24. !
25. crypto ipsec transform-set MisTransformadas esp-3des esp-sha-hmac
26. !
27. crypto ipsec profile MiPerfil
28. set transform-set MisTransformadas
29. !
30. interface Tunnel0
31. tunnel protection ipsec profile MiPerfil
```

3. RESULTS AND DISCUSSION

3.1 Integrity check

Figure 4 shows the validation program (IPsec IntegrityCheck) which has a similar code to “IPsec Tools UV” for the algorithms MD5 and SHA-1. IPsec IntegrityCheck allows to validate the MD5 and SHA-1 algorithms using the 14 test vectors specified by RFC 2202 [12]. These vectors cannot be introduced directly into the “IPsec Tools UV” tool because it has been assumed that the IP version and header length fields have fixed values and therefore by design are protected for editing with their default values . The graphical interface of the validation program allows to select the integrity algorithm using radial circles for MD5 or SHA-1. The selected integrity verification function is applied to the message entered in the upper field using the key that has been entered in the lower field. For the standard test number 1 SHA-1 enters the text “Hi There” in the upper field and the string “0x0b0b ... 0b0b” (20 times hex number 0b) in the lower field. Finally, after clicking the “Compute” button, the message verification code is obtained, which for the standard test for number 1 begins with “B617” and ends with “be00”. The resulting integrity check code (also called message digest or hash) has a length of 160 bits when using the SHA-1 algorithm and 128 bits when using the MD5 algorithm. The length of the code is independent of the length of the message to protect and the length of the key used.



IPsec - IntegrityCheck

ALGORITMO DE VERIFICACIÓN DE INTEGRIDAD
HMAC (Hashed Message Authentication Code)

Hi There — □ Hex ○ MD5

0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b0b — ☑ Hex ● SHA-1

Result

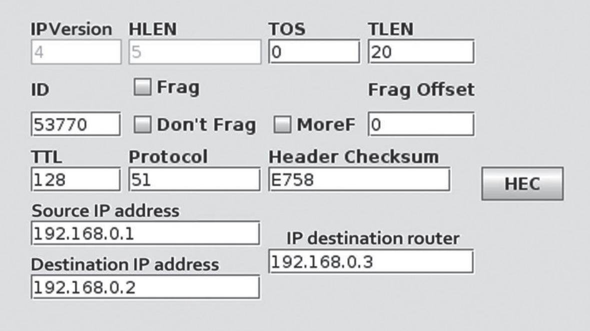
B617318655057264E28BC0B6FB378C8EF146BE00

Figure 4. *Validation program for the algorithms MD5 and SHA-1*

3.2 IPsec TOOLS UV TOOL

From the variety of configuration options for authentication, integrity and privacy available in IPsec, the subset MD5, SHA-1 and 3DES was chosen to be implemented in IPsec Tools UV.

Figure 5 shows the IP Header Tab used to enter values in all header fields of an IP datagram, except in the fields “IP version” (which defaults to 4) and HLEN (header length, default value is 5). All these fields are used to form both the outer header (tunnel mode) and the inner datagram header protected by IPsec. In general, the “Protocol” field identifies the upper level protocol payload that is carried by an IP datagram. In particular, when an IP datagram is protected using IPsec, the “Protocol” field codes AH with 51 and ESP with 50. Using the HEC button the verification of IP header (Header Checksum field) is obtained, which in this example is “E758”. The program verifies that the “IP destination router” field is activated only if the operation of IPsec in tunnel mode has been configured via the “Configure Encryption” Tab. When this option is activated, the source and destination IP addresses header for both ends of the tunnel are added. When forming the protected IPsec datagram, the program uses the value entered in the Source IP Address field (192.168.0.1) as the tunnel source IP address and takes the value of the address entered in the IP destination router field as the destination IP address of the tunnel (192.168.0.3).

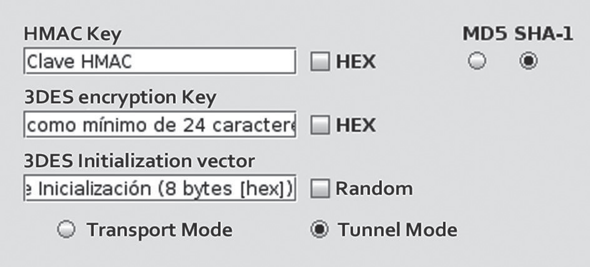


IPVersion 4
HLEN 5
TOS 0
TLEN 20
ID 53770
□ Frag
□ Don't Frag
□ MoreF
Frag Offset 0
TTL 128
Protocol 51
Header Checksum E758

Source IP address 192.168.0.1
IP destination router 192.168.0.3
Destination IP address 192.168.0.2

Figure 5. *IP Header Tab*

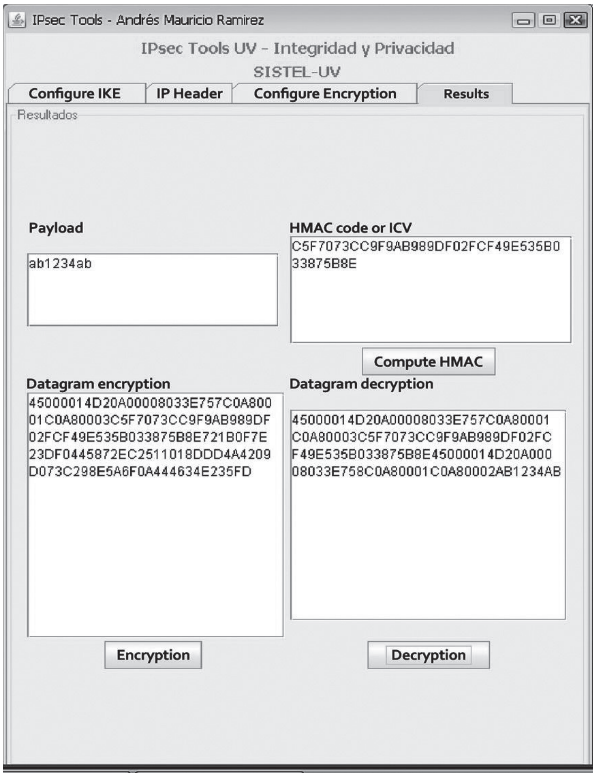
Figure 6 shows the "Configure Encryption" Tab to set up the encryption key that will be used by the encryption algorithm (3DES) used by "IPsec Tools UV". The minimum size of this key is 24 characters. The 64-bit initialization vector can be randomly generated or entered manually. Finally, the operation mode for IPsec "Transport" or "Tunnel" mode can be set.



HMAC Key: Clave HMAC □ HEX
MD5 ○ SHA-1 ●
3DES encryption Key: como mínimo de 24 caracter □ HEX
3DES Initialization vector: e Inicialización (8 bytes [hex]) □ Random
○ Transport Mode ● Tunnel Mode

Figure 6. *Configure Encryption Tab*

The "Payload" field (see Figure 7) allows the payload value of the plain IP datagram to be entered in hexadecimal. By clicking on the "Compute HMAC" button, the integrity check code covering the IP datagram payload and IP datagram header fields that do not change is obtained. The verification code has a size of 160 bits (20 bytes) for SHA-1 and 128 bits (16 bytes) for MD5. To encrypt and decrypt the IP datagram, the "Encryption" and "Decryption" buttons are used respectively. In the lower left box labeled "Datagram encryption", after the field that represents the destination address of the tunnel "C0A80003" (192.168.0.3) appears the code generated by the HMAC SHA-1 algorithm, which for this example is the hex string "C5F7073C C9F9AB98 9DF02FCF 49E535B0 33875B8E". Then there follows the string with a length of 32 bytes "47C33033 79CE944A E06296C1 DA8DF5F7 258C706D F7FF6B77 7322BCB8 22BCA205", which are the values generated by the 3DES encryption algorithm, these values represent the encryption of the 20 bytes of internal header from the IP datagram "45000014 D20A0000 8033E758 C0A80001 C0A80002" and of the four octets of payload carried by the datagram "AB1234AB" (these two strings of 24 bytes are displayed in plain text to the right, below the "Datagram decryption" heading). The above results demonstrated that each of the fields in the IP datagram are encrypted and decrypted, emulating the process that performs the IPsec protocol. For example, the inner header of the IP datagram is encrypted using the 3DES algorithm and the integrity of the datagram is achieved using either SHA-1 or MD5. With an upgrade of the tool, these transformations are feasible on protocols such as IPv6. Results on [13] indicate that IPsec performance can be improved to be used in smart grids through ESP+, in that sense, the tool "IPsec Tools UV" could be adapted to display the new transformations performed by the ESP + protocol.



IPsec Tools - Andrés Mauricio Ramirez
IPsec Tools UV - Integridad y Privacidad
SISTEL-UV
Configure IKE
IP Header
Configure Encryption
Results
Resultados

Payload
ab1234ab

HMAC code or ICV
C5F7073CC9F9AB989DF02FCF49E535B0
33875B8E

Datagram encryption
```
45000014D20A00008033E757C0A800
01C0A80003C5F7073CC9F9AB989DF
02FCF49E535B033875B8E721B0F7E
23DF0445872EC2511018DDD4A4209
D073C298E5A6F0A444634E235FD
```

Datagram decryption
```
45000014D20A00008033E757C0A80001
C0A80003C5F7073CC9F9AB989DF02FC
F49E535B033875B8E45000014D20A000
08033E758C0A80001C0A80002AB1234AB
```

Figure 7. *Tool "IPsec Tools UV" with some of the key functions of IPsec*

3.3 Virtual private network dynamic multipoint: verification of operation

One of the main advantages of designing a network infrastructure based on the DMVPN concept is the ability to establish tunnels between remote routers, both dynamically and directly. In our example, after establishing the tunnel configuration on each router, it can be verified that the R2 router is able to establish two DMVPN sessions: a static session with the R1 central router and a dynamic session with the R3 remote router which is activated when traffic is generated from R2 to R3. Table 1 shows the result when running the command "show dmvpn" in R2, which shows that a packet originating in LAN2 and destined for LAN3 does not have to go through R1 to reach R3 (i.e. it travels by the optimal path).

After applying IPsec protection to the mGRE tunnel, the command "show crypto isakmp sa" in R2 displays the IKE security associations that have been established and the command "show crypto ipsec sa" shows the number of packets encrypted and decrypted through each tunnel. The command "show ip route" in turn shows the routing table with the networks known by each router. Table 2 shows the R2 routing table. In Table 2, the penultimate entry indicates that the next hop to reach the 192.168.3.0/24 network has IP address 192.168.0.3, that is from R2 it is possible to go directly to LAN3 without any involvement of R1. These results have been obtained in a fully controlled environment.

Table 1. *DMVPN sessions provided by the R2 router*

Tunnel0, Type:Spoke, NHRP Peers:2					
# Entry	Peer NBMA Address	Peer Tunnel Address	State	UpDown Time	Attribute
1	12.34.56.2	192.168.0.1	Up	02:16:55	S
2	34.56.78.2	192.168.0.3	Up	Never	D

Table 2. *R2 routing table*

Protocol : C - connected, S* – Static, O – OSPF	
	23.0.0.0/24 is subnetted, 1 subnets
C	23.45.67.0 is directly connected, serial 1/0
C	192.168.0.0/24 is directly connected, Tunnel0
O	192.168.1.0/24 [110/11121] via 192.168.0.1, 00:18:55, Tunnel0
C	192.168.2.0/24 is directly connected, FastEthernet0/0
O	192.168.3.0/24 [110/11121] via 192.168.0.3, 00:17:59, Tunnel0
S*	0.0.0.0/0 24 [1/0] via 23.45.67.1

4. CONCLUSIONS

IPsec is a comprehensive security architecture [14] aimed at protecting IP datagrams across a public network. This architecture allows combining multiple options in terms of security: different levels of protection for IP datagrams using AH (integrity check) or ESP (integrity check and/or encryption), different modes of operation (transport or tunnel), and a set of algorithms to implement the respective transformations (MD5, SHA-1, 3DES, AES). The "IPsec Tools UV" tool facilitates the exploration of the main transformations as it allows to type data in the header fields and payload field of an IP datagram, choose the operation mode of IPsec, select the integrity check algorithms and perform transformations by MD5, SHA-1 and 3DES. By developing this kind of tool, we hope to have made a contribution to education on the understanding and best provisioning of data networks in our country. A future work could be to include IPv6 fields, newer security algorithms and higher level protocols; like Secure Socket Layer.

In this article, it has been shown that it is possible to interconnect private networks in a secure way over the Internet using the appropriate tools and protocols. The design approach, which uses dynamic multipoint tunnels based on mGRE protected by IPsec, offers the benefit of expedited communication through direct tunnels established between remote sites involving the exchange of IP datagrams. Using mGRE also eases the configuration of the central router when it is necessary to increase the number of remote sites as the design can incorporate the OSPF protocol as a routing protocol when it is desired to exploit its high scalability.

Before attempting a direct deployment of a relatively complex network based on mGRE and bringing it into production, the option of developing a prototype of the network using a few routers or using emulation software such as Dynamips or GNS3 should be considered. During the process of making the prototype operational, the protocols that are most suited in terms of operation, security and scalability can be identified. The critical parameters that must be taken into account for final deployment can also be defined. According to this approach, sufficient experience is gained by tackling the keys issues involved in the final deployment of the network.

5. REFERENCES

[1] Y. Bhaiji, "Network Security Technologies and Solutions (CCIE Professional. Development)", Indianapolis: Cisco Press, Inc., 2008, Chapter 15.

[2] C. McDonald, P. Hawkes, and J. Pieprzyk, "Differential Path for SHA-1 with complexity 2^{52}". (2009). Available: http://eprint.iacr.org/2009/259 [visited June 2011].

[3] J. Callas, L. Donnerhacke, H. Finney, D. Shaw, and R. Thayer, "OpenPGP Message Format", In IETF (The Internet Engineering Task Force) Request for Comments RFC 4880. Available: https://tools.ietf.org/html/rfc4880 [visited August 2011].

[4] L. Chappell, "Wireshark Network Analysis: The Official Wireshark Certified Network Analyst Study Guide", Laura Chappell University, San Jose, CA 95129 USA, 2010, pp. 341-342.

[5] Advanced Network Technologies Division, "NIST IKE (v1/v2) / IPsec Simulation Tool" Available: http://www.antd.nist.gov/niist/ [visited April 2011].

[6] S. Kent, K. Seo, "Security Architecture for the Internet Protocol", In IETF (The Internet Engineering Task Force) Request for Comments RFC 4301. Available: http://tools.ietf.org/html/rfc4301 [visited December 2010].

[7] D.Farinacci, T. Li, S. Hanks, D. Meyer, P. Traina, and R. Glenn, "Generic Routing Encapsulation", In IETF (The Internet Engineering Task Force) Request for Comments RFC 2784. Available: http://tools.ietf.org/html/rfc2784.html [visited January 2011].

[8] G. Dommety, "Key and Sequence Number Extensions to GRE", In IETF (The Internet Engineering Task Force) Request for Comments RFC 2890. Available: http://tools.ietf.org/html/rfc2890 [visited February 2011].

[9] J. Luciani, D. Katz, D. Piscitello, B. Cole, and N. Doraswamy, "NBMA Next Hop Resolution Protocol (NHRP)", In IETF (The Internet Engineering Task Force) Request for Comments RFC 2332. Available: http://tools.ietf.org/html/rfc2332 [visited June 2011].

[10] J. Grossmann, X. Alt, "Graphical Network Simulator (GNS3 0.8.2)". Available: http://www.gns3.net/download/ [visited August 2011]

[11] Cisco Systems, Inc. "Configuring Dynamic Multipoint VPN (DMVPN) using GRE over IPsec between Multiple Routers". Available: http://www.cisco.com/en/US/tech/tk583/tk372/technologies_configuration_example09186a008014bcd7.shtml [visited January 2012].

[12] P. Cheng and R. Glenn, "Test Cases for HMAC-MD5 and HMAC-SHA-1", In IETF (The Internet Engineering Task Force) Request for Comments RFC 2202. Available: http://xml2rfc.tools.ietf.org/html/rfc2202 [visited February 2011].

[13] B. Hirschler, A. Treytl, and W. Neustadt, "Internet Protocol Security and Power Line Communication", 16th IEEE International Symposium on Power Line Communications and Its Applications (ISPLC), date: 27-30 March 2012. Piscataway, N.J.: IEEE, 2012.

[14] S. Kent and K. Seo, "Security Architecture for the Internet Protocol", In IETF (The Internet Engineering Task Force) Request for Comments 4103. Avalilable: http://tools.ietf.org/html/rfc4301 [visited june 2012].

6. CURRICULUM

Andrés Mauricio Ramirez, received a B.Eng. degree in Electronic Engineering from Universidad del Valle, Cali, Colombia (South America), 2007. Currently, he works as support engineer at ZTE corporation.

Oscar Polanco Sarmiento, received a B.Eng. degree in Electrical Engineering from Universidad del Valle, Cali, Colombia (South America), 1986, and a Esp. degree in Computers and Digital Systems from Universidad del Valle, 1991. Currently, he works as telecommunications assistant lecturer in the Department of Electrical and Electronics Engineering of Universidad del Valle, Cali, Colombia (South America). His research interests include IP based internetworking, Security network, and data network modeling and simulation.

Fabio G. Guerrero, received a B.Eng. degree in telecommunications engineering from Universidad del Cauca, Popayan, Colombia (South America), 1992, and a M.Sc. degree in Electronic Engineering from Bradford University, UK, 1995. Currently, he works as telecommunications assistant lecturer in the Department of Electrical and Electronics Engineering of Universidad del Valle, Cali, Colombia (South America). His research interests include digital communications, telecommunication systems modeling, and ICT.