Available online www.jsaer.com

***Journal of Scientific and Engineering Research*, 2015, 2(2):94-98**

Research Article

ISSN: 2394-2630
CODEN(USA): JSERBR

Network Performance of different Encryption and Authentication Algorithm

Jitendra Kumawat

Department of Computer Science, Amity University Rajasthan

Abstract The previously used IPv4 does not deal with the issue of IPsec. It does not inherently provide any security for data transmitted across networks. Even not any integrity and encryption algorithms were used. Presently, IPsec is used widely by nearly all security vendors. It is the primary security protocol used in Virtual Private Networks; IPsec was defined in RFC 2401. The objectives are to analyze whether the IPsec VPNs configure with variety of encryption (3DES, Blowfish and AES) and authentication (HMAC-MD5, HAMC-SHA1) algorithms and to compare their TCP and UDP throughput and request/response time on the network and find out the optimal solution among these algorithm based on their performance in IPsec enable network traffic. The tests have been done with two x86 based hosts in Red Hat Enterprise 2.6.9 kernel and for configure IPsec using ipsec-tools-0.6.6 tool.The measurements are taken by the Netperf version 2.4.1 tools. This work investigates the various encryption and authentication algorithms and foreseeing the effect of these algorithms over network performance. HMAC-MD5 and AES (authentication, encryption) gives the optimum network performance parameter.

Keywords Encryption, Algorithm, HMAC-MD5, AES.

Introduction

Virtual Private Network (VPN)

Beside Local Area Networks (LAN) or Wide Area Networks (WAN), networks can be generally cut into public and private. Examples for public networks are the Internet or telephone networks. Private networks consisting of networked devices of restricted private organizations, mainly communicating among each other. The crossover between private and public networks happens via gateway router. A configured firewall prevents attacks from outside and restricts the users' access to the public network. The VPN concept blurs the borders between public and private networks by offering the possibility to build up a safe, private network over public network(s) like the internet. A virtual private network is a method to simulate a private network in a public network. It is named "virtual", because of the virtual connections appearing to be within one private network – that means temporally connections that are not physical but consists of packages, transferred via public networking infrastructure (e.g. internet) without the notice of that by the user [1].

Thus VPNs use the internet as a WAN connection. An advantage of this method for an organization can be the use of only relatively short dedicated connection from the own location to the next Point of Presence (PoP) normally to the service provider. This connection could be a local leased line. The outcome of this is a lower-cost option for major organizations and scalability of the resources. VPN systems require an in-depth understanding of public network security issues. The availability and performance of an organization's wide-area VPN (over the Internet in particular) depends on factors largely outside of their control. Some VPN

technologies from different vendors do not work well together due to immature standards. VPNs need to accommodate protocols other than IP and existing ("legacy") internal network technology. Different types of technologies are used to protect the data transmissions. For data protection package tunnelling and firewalls are used. VPN protocols also support authentication and encryption to keep the tunnels secure. VPN supports two types of tunneling [2], voluntary and compulsory tunnelling. In voluntary tunnelling, the VPN client manages connection setup. The client first makes a connection to the carrier network provider (an ISP in the case of Internet VPNs). In compulsory tunnelling, the carrier network provider manages VPN connection setup. When the client first makes an ordinary connection to the carrier, the carrier in turn immediately brokers a VPN connection between that client and a VPN server. Compulsory VPN tunnelling authenticates clients and associates them with specific VPN servers using logic built into the broker device. Compulsory tunnelling hides the details of VPN server connectivity from the VPN clients and effectively moves control over the tunnels from clients to the ISP.

IPsec Overview

IPsec is an internet engineering task force standard suite of protocol developed that provides data authentication, integrity and confidentiality as data is transferred between Communication points across input networks. IPsec provides data security at the packet level. It aids in having private data transmitted over public insecure networks without being interrupted in any sense. IPsec contains ESP (Encapsulating Security Payload) that provides confidentiality, authentication, and integrity. ESP provides all encryption services. IPsec also contains AH (Authentication Header) that provides authentication and integrity, which protect against data tampering and unauthorized retransmission of packets. The last component it has IKE (Internet Key Exchange) that provides key management and security association management. IPsec has introduced the concept of SA (security association). A SA is a logical connection between two devices transferring data. A SA provides data protection for unidirectional traffic by using defined IPsec protocol.

IPsec Services

IPsec is designed to provide the following services at Network layer.

- Access control
- Connectionless integrity
- Origin authentication
- Replay protection
- Privacy/confidentiality

Of course the quality of these services depends upon the decision of the security administrator. IPsec is a tool, a powerful tool, but its effectiveness depends upon how it was implemented.

IPsec Protocol Suite

The IPsec services are provided by two traffic security protocols, the Authentication Header and the ESP (Encapsulation Security Payload). Additional other protocols are employed such as Key Management Protocol, which are not defined in the IPsec specification. AH and ESP are part of IPsec.

IPsec Authentication Header (AH)

IPsec AH provides connectionless integrity, data origin Authentication and anti-replay integrity. The later is optional and not enforced at the receiver's end. Figure 1.1 depicts the IPsec AH header format. The "Next Header" field is of 8 bit size and specifies the type of the Transport protocol used in the upper layer. The "Payload Length" field is also an 8-bit size, and contains the IPsec Header length in words (32-bit) minus 2 words, e.g. 3+3-2= 4, if authentication data is 3 words (96-bits). The sender always transmits the "Sequence Number" field (32-bits), but the receiver might optionally act on it. Finally, the "Authentication Data" field, variable size, multiple of 32-bits, ICV for the attached packet (Including the AH header itself). "Reserved" bits Must Be Zero (MBZ). Other fields are Next Header Payload Length Reserved (32-bits) (MBZ), Security Parameter Index (SPI) (32-bits), Sequence Number field (32-bits) and Authentication Data [3]. The ICV is

computed first at the transmitter by the use of a common authentication algorithm that is also known to the receiver. Then ICV is recomputed at the receiver and compared to match the received value for authentication integrity. ICV computation excludes non-predictable IP Header (IPH) fields like Time to Live (TTL), Flags, Type of Service (TOS), Fragment offset, Checksum, etc. If IP fragmentation occurs at the sender, it should be performed after AH processing. The IP reassembly should then be performed before AH processing at the receiver.

Next Header	Payload Length	Reserved(32)
Security Parameter Index(32)		
Sequence Number Field(32)		
Authentication Data		

***Figure 1**: Authentication Header*

IPsec Encapsulating Security Payload (ESP)

Provides confidentiality (encryption), connectionless integrity (optional, not enforced at receiver end), data origin authentication (optional, not enforced at receiver end), and anti -replay integrity. Figure 1.2 depicts the ESP header format. The "Next Header" field is exactly as in IPsec AH. The "Pad Length" contains the number of pad bytes inserted by the encryption algorithm. The "Sequence Number" field is used same way as in IPsec AH. Finally, the "Authentication Data" field (variable size, multiple of 32 bits) contains ICV for the encapsulated packet and the ESP header/trailer (not including the authentication data itself) .The ICV computation steps are the same as in IPsec AH.

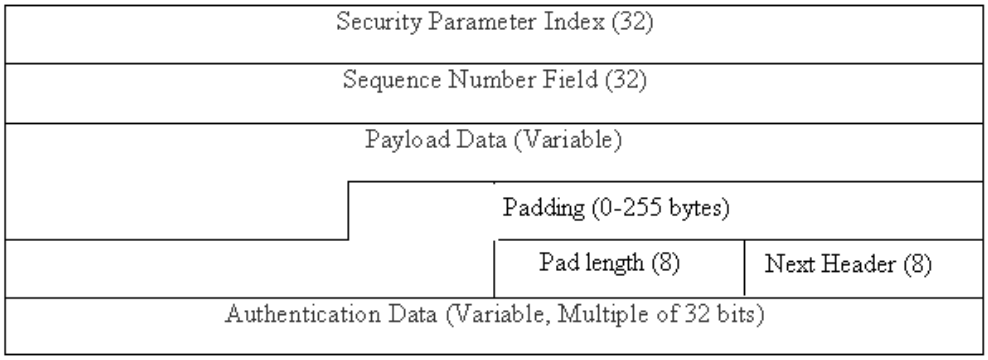

***Figure 2**: IPsec ESP Header Format.*

IPsec Technologies

IPSec combines several different security technologies into a complete system to provide confidentiality, integrity, and authenticity [5]. In particular, IPsec uses:

- Diffie-Hellman key exchange for deriving key material between peers on a public network
- Public key cryptography for signing the Diffie-Hellman exchanges to guarantee the identity of the two parties and avoid man-in-the-middle attacks
- Encryption algorithms, such as DES,3DES for encrypting the data
- Keyed hash algorithms, such as HMAC, combined with traditional hash algorithms such as MD5 or SHA for providing packet authentication.
- Digital certificates signed by a certificate authority to act as digital ID cards.

IPsec Operation

The purpose of IPsec is to provide various services to traffic traveling between a source and a destination. The destination/source may be a router or a host. The services may be provided to all traffic or only to specific types of traffic [6].

There are different types of protection provided by IPsec and there are also different modes for IPsec to operate upon. IPsec may operate upon certain types of data while other data is transmitted on an unprotected path.

In terms of packet construction and TCP/IP stack IPsec is implemented at the network layer. The diagram below shows the location of the IPsec protocol in the stack. The arrows show the path of a packet traveling from Host A to Host B. Notice that Host B implements IPsec as a separate layer, whereas Host A and the routers include IPsec as part of the network layer. These are two different types of host implementation known as OS integrated or bump in the stack (BITS). There are drawbacks and advantages for both types of implementation; OS Integration can be difficult for external companies providing solutions to existing networks, however, OS integration can make use of services in an existing network layer. IPsec physically interacts with the stack by modifying, encapsulating or inserting data into the IP Packet before it is passed to the data link layer on the way out and again modifying the packet before it is passed up to the network or transport layer.

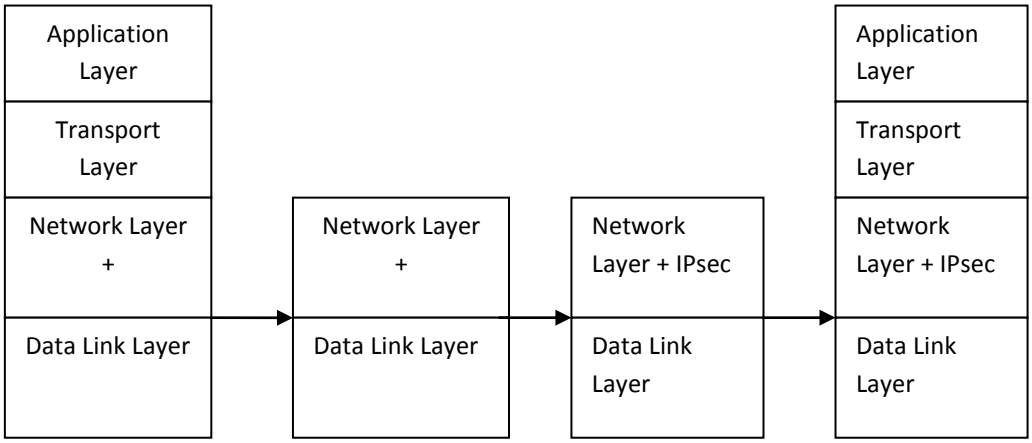

***Figure 1.3**: TCP/IP stack*

Conclusions

This work investigates the various encryption and authentication algorithms and foreseeing the effect of these algorithms over network performance. HMAC-MD5 and AES (authentication, encryption) gives the optimum network performance parameter.

3DES takes much time to authenticate at number of rounds are higher while AES takes lesser round thus leading to lesser time interval for execution yet randomness is maintained.

HMAC-SHA1 has much more complexity than HMAC-MD5. Present work recommends the use of HMAC-MD5 and AES, providing lesser complexity, much faster execution time, yet random and not attacks negotiable.

Future prospectus

IPV6 has been designed with IPSec at its center. Hopefully, this will create a more secure protocol by engineering IPV6 with IPSec built-in. Research work related to IPSec has been around and is providing secure IPSec-VPN solutions, but the future demands much more flexibility, scalability, and compatibility like with NAT from this security protocol. New implementation should have inbuilt intrusion detection and prevention capability also, so that a single secure centralized system can provide the entire feature to secure a network from any sort of attacks. There should also be an efficient compression technique to be used with encryption techniques so as to improve throughput, transaction rate and path MTU of IPSec protocols.

Since IPSec depends upon some other protocols like key management protocols for implementing security associations (SA), encryption algorithms like 3DES, AES for encrypting IP traffic etc. So to avoid any sort of weaknesses in IPSec, the performance analysis of these algorithms is a must, so as to implement flexible IPSec product with the highest level of protection. There are further recommendations for implementing IPV6-IPSec while concerning things like IPSec/QoSS (Quality of Security Service), data compression with IPSec encryption and authentication for fast secure network transactions.

In IPsec we have used various types of security algorithms to provide privacy, authentication etc., but due to extra processing of security algorithms in IP packets the performance of network degrade and more CPU consumptions. To improve performance of network with IPsec efficient algorithms must be used.

Impact of DoS attacks on IPsec capacity and demonstrate that a single attacker can degrade throughput as much as 50%. So for that problem we plan to explore security parameter index (SPI) spinning using pseudorandom sequences and explore the use of layer nonces for addition protection to check the valid incoming packet before processing on IPsec packet on NIC.

References

1. Simpson, W. (1995). "IP in IP Tunneling," RFC 1853.
2. [Hamzeh, K., Pall, G., Verthein, W., Taarud, J., Little, W., & Zorn, G. (1999). Point-to-point tunneling protocol.
3. Atkinson, R., & Kent, S. (1998). IP authentication header. IETF RFC 2402.
4. Kent, S. (2005). IP encapsulating security payload (ESP). IETF RFC 2406..
5. Elkeelany, O., Matalgah, M. M., Sheikh, K. P., Thaker, M., Chaudhry, G., Medhi, D., & Qaddour, J. (2002). Performance analysis of IPSec protocol: encryption and authentication. In *Communications, 2002. ICC 2002. IEEE International Conference on* (Vol. 2, pp. 1164-1168). IEEE.
6. Uyles, B. (2001). "Internet Security Protocols: Protecting IP traffic," Pearson Education Asia, 1st Edition