Asian Journal of Information Technology 16 (1): 125-130, 2017
ISSN: 1682-3915

Performance Analysis of Various Encryption Techniques in Communication Network

Elvis Ximenes, Kheng Cher Yeo, Sami Azam and Bharanidharan Shanmugam
School of Engineering and Information Technology, Charles Darwin University,
NT Casuarina, Australia

Abstract: Cryptography is used in almost in every application to provide strong security to sensitive data during the communication across the public network. In this study, a performance analysis is conducted to find the optimal encryption cipher to provide a better performance during encryption process in the IPSec tunnel mode. The analysis is based on the comparison of number of delay and jitter between block cipher (DES-56 bits, 3DES-168 bits and AES-256 bits) and stream cipher (SEAL) used in IPSec encryption security payload. The result shows that 160 bits SEAL cipher has the least latency in encrypting the TCP and UDP traffic in both single and multi uses compared to other ciphers.

Key words: IPSec, DES, AES, SEAL, encryption

INTRODUCTION

Ensuring a secure communication between private networks in the Internet becomes the crucial part in the modern computer network. Securing the communication in the Internet Protocol (IP) network is the efficient way to protect the data that is being transferred over the public network. The IP packets are easy to forge because it does not inherit the security features. As a result, if the IP packets have been modified there is no guarantee that the source address in the IP datagram is from the original sender and contains the original data (Doraswamy and Harkins, 2003).

Network performance also plays important roles in determining the reliability and connectivity of the communications in the network. In the low bandwidth network situation, implementing the highly secured data encryption with large number of bits keys can have a high impact on the network performances and not cost effective for long term run because it will require expensive high performance network devices to overcome the network performance bottleneck. The optimized point between network security encryption and network performance for low bandwidth networks will be in selecting the encryption security that is faster in encryption and decryption process and also capable to provide a maximum security to the data communication process.

This study investigates the performance of block ciphers and stream ciphers encryption algorithms used in IPSec tunnel mode to encrypt the data communication between two private networks.

IPSec encryption overview: There are several methods have been used to protect internet communication data including the encryptions. The IPSec is one such method that is used to protect the network layer protocols such as TCP/IP. The main objective of the IPSec is to provide data authentication integrity and confidentiality between two communication points across IP network. For data integrity, the IPSec first establish the secure connection by authenticating with the peer device with key exchange (IKE). Once the connection is authenticated, the two networks can start to communicate in secured connection where the communication is encrypted under data packet encoding which are the Authentication Header and Encapsulated Security Payload (ESP) to provide confidentiality for data communication. The algorithm used in the IPSec encryption process mainly the block ciphers such as Data Encryption Standard (DES) Triple Data Encryption Standard (3DES) and Advanced Encryption Standard (AES). Alternatively, the stream ciphers such as Software-Based Encryption Algorithm (SEAL) also used for resources optimization encryption. IPSec is mostly used to provide a Virtual Private Network (VPN) and data security between two private (Frankel, 2011). IPSec has two modes in transferring the data. The transport mode is used to provide direct authentication between client and server and the tunnel mode is use for end to end communication (Sharma and Kalra, 2009). Both ESP and AH can provide a secure mechanism to transport and tunnel mode of the IPSec. The process of IPSec is properly managed by the security association key which

Corresponding Author: Elvis Ximenes, School of Engineering and Information Technology, Charles Darwin University, NT Casuarina, Australia

exists in the IPSec headers to define the unidirectional security service for inbound or outbound packets that are sent or received by the entity. IPSec requires encryption algorithm and hash functions to provide a highly protected data during the communication between two private networks. The hash functions such SH-1 and Message Digest 5 (MD5) are used in the authentication harder to digest the authentication password and convert it to scrambled values in order to protect password from being forged and also to ensure that the communication is originally from the trusted peer router or gateway. The encapsulated security payload uses the encryptions algorithm to encrypt the data communication. The encryption algorithm in IPSec consists of which is discussed.

Data Encryption Standard (DES): DES is a feistel type symmetric block cipher that uses 56 bits keys to encrypt and decrypt the data. The DES operation has 16 cycles where each cycle consists of four important operations:

- Expand the 32 bits into 48 bits vector
- Perform XOR operation to combine with the 48 bit round key
- Mapping the 48 bit results onto 32 bit vector using non-linear S-boxes
- Perform bit permutation where the 32 bits vectors are transposed

The 8 bit of the 64 bits length is used for the parity, check therefore DES key is effectively 56 bits (Daemen and Rijmen, 2013).

Tripe Data Encryption Standard (3DES): 3DES is the extended version of DES that uses 168 bits of keys to encrypt the data three times. 3DES uses 56 key bundles that can be describe as K1-K3 where the K1 is used to encrypt, K2 is used to decrypt and the K3 is used to encrypt. The decryption process will be the reverse order of the keys used (FIPS, 1999).

Advance Encryption Standard (AES): AES uses rijndael algorithm to encrypt the data. AES contains variable block length and variable key length which can be independently applied to any multiple of 32 bits with minimum of 128 bits and maximum 256 bits. Rijndael is a key, iterated block cipher where the process of converting the input into cipher text will go thru number of repetitions of transformation rounds. The round transformation started with adding the round key (AddRoundKey), followed by Substitute Byte (SubByte), Shift Rows (ShiftRows), Mix Columns (MixColumns) and Add Round Key (AddRoundKey) and in the final round it will perform the same step again however this time there is no Mix Column (MixColumns) in the final round (Daemen and Rijmen, 2013).

Software-optimized Encryption Algorithm (SEAL): SEAL is a length-increasing Pseudorandom Function family (PRF) stream cipher that performs CPU optimization during encryption process (Schneier and Whiting, 1997) and used as an alternative algorithm to DES, 3DES and AES. SEAL uses 160 bit keys to map a 32 bit string n to L-bit string, where the L number can be as large and as small depend on the target application requirements. The message encryption process depends on the key a, message x and the message position n in the data stream (Rogaway and Coppersmith, 1998).

Literature review: The encryption process can be done symmetrically and asymmetrically. In symmetric process, the sender and receiver using one key to encrypt and decrypt the message where as in asymmetric process the sender and receiver use two different keys to encrypt and decrypt the message. The symmetric ciphers can be the block ciphers and stream ciphers. The block cipher breaks the block of characters into 8 bit long blocks and applies the key to each block and encrypts each block while Stream cipher breaks the block of characters into small bits and encrypts each bit individually. Stream cipher encrypts each message with a time-varying function.

In the performance analysis between stream ciphers and block ciphers, Sharif and Mansoor (2010) concludes that the stream ciphers perform better than block ciphers in regards to the CPU time requirement for encryption. Performance analysis conducted by Kumar and Kumar (2012) compares execution time and resource utilization between RC6, Twofish and Rijndael block cipher algorithms. The results conclude that the performance of the three encryption algorithm is based on the key size used in the encryption process where the performance will decrease due to increasing number of keys and the average CPU utilization is the same among three encryptions algorithm. They also recommend the using the RC6 is ideal for high encryption rate situation while Rijndael is ideal for situation where memory is much concern.

In the comparison of DES performance with other encryption algorithm (Aggarwal *et al*., 2013) found that DES seems to be the slowest in the execution time in encryption process and the throughput in decryption is less compared to other ciphers. In contrast, A performance analysis of SEAL algorithm on Field Programmable Gate Arrays Accelerator (FPGA) by

Kumar *et al.* (2013) shows that mapping and optimization of SEAL on FPGA are able to exploit the thread level and achieve the high performance especially in the table generation module and the speed of SEAL algorithm is potentially fast by the support of the GPUs.

MATERIALS AND METHODS

This study covers the network topology used in the experiment to compare the different encryption techniques and the tools used to simulate the traffic.

Network topology model: In this experiment, four Cisco C2600 series routers has been used for the public network connection using star topology and two Cisco C2800 series for each private network gateways. The Open Shortest Routing Protocol (OSPF) was used in this experiment as the main protocol used for traffic forwarding and packet switching (Fig. 1).

IPSec configuration: We started with phase 1 configuration which is setting up the Internet Security Association and Key Management Protocol (ISAKMP) policy in the gateway of the network A and B in this case the LAB-G and LAB-H. The ISAKMP configured using DES encryption, Message Digest 5 (MD5) hashing algorithms, Diffie-Hellman 768 bit modulus size (group1), pre shared authentication method and the ISAKMP key. This policy is applied to the gateway interface to be used for peer negotiation.

In the IPSec phase 2 configuration, we first create the Access Control List (ACL) of two private networks, create the IPSec transform which contains the combination of ESP and AH for IPSec SA negotiation. We then associate the IPSec and the ISAKMP policy by creating the crypto map. We only use single crypto map for this experiment. Next, we map the crypto map to the gateway interface. Finally, we test the configuration by ping from the 172.16.0.0-172.16.1.0 network and verifying it by execute this command show crypto IPSec SA and show crypto ISAKMP SA in network a gateway.

Network synchronization and traffic generator: Since, our simulated network is a standalone network, load balancing and time synchronization is important to get the accurate results. We configure the OSPF network to perform in load balancing state so that the traffic can be separated equal through two network path. We also configure the router LAB-F to be the Network Time Protocol (NTP) master to provide clock synchronization to the rest of the network. For the client computer we also implement time synchronization with the NTP server by

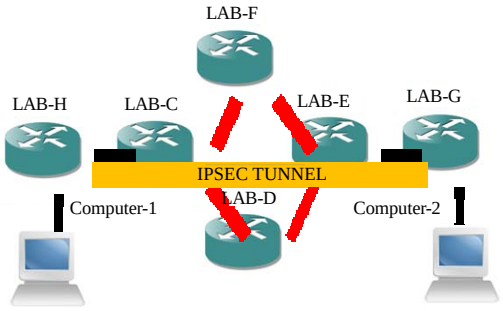

Fig. 1: Network topology

using third party software the network time. We use the Distributed Internet Traffic Generator (DIT-G) to generate traffic at transport, network and application layer. This traffic generator is a software based generator written in JAVA platform by Volker Semken from the University of Naples Federico II (Botta *et al*., 2012).

RESULTS AND DISCUSSION

TCP traffic in IPSec single user: In IPSec tunnel single user environment, the latency in TCP traffic has increased slightly from 27.70 up to 37.41 msec as the various encryptions is applied (Fig. 2). It can be seen from the graph 1 that the AES 256 bits gained the highest average delay at 37.41 msec compared to other three encryptions followed by 3DES 160 bits at 32.58 msec. Interestingly, the SEAL 160 bits cipher has slightly equal amount of delay with the 56 bits of DES.

With the 2.8 times bit different from 56 bits DES, SEAL-160 reached only 2% increase in total average delay while 168 bit of 3DES is 3 times bit of 56 bit DES and the percentage delay increase reached up to 18%. Finally, with the increase number of bit by 4.5 times, the 256 bit AES has 35% increases in delay (Table 1).

UDP traffic in IPSec single user: In UDP traffic the number of jitters increased slightly in smaller number from 0.172 up to 0.185 msec as the various encryptions is applied (Fig. 3). AES cipher has the highest jitter at 0.185 msec and followed by 3DES at 0.177 and DES at 0.172 msec while SEAL has the lowest jitter at 0.121 msec.

With the 2.8 times bit different from 56 bits DES, the average jitter is decreased by-30% in SEAL-160 bit while average jitter in 168 bit of 3DES is increased by 3% with 3 times bits different from 56 bit DES. Finally with the increase number of bit by 4.5 times the 256 bit AES has 7% increases in jitter (Table 2).

TCP traffic in IPSec multi user: In multi user environment the delay in TCP traffic has increased from

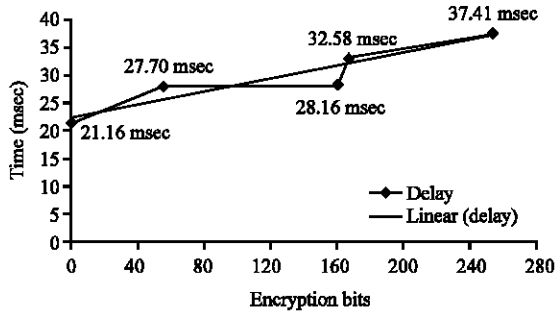

Fig. 2: Average delays in TCP traffic-single users

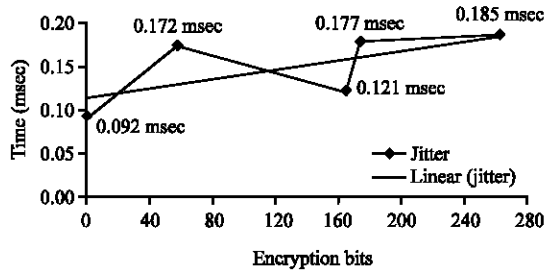

Fig. 3: Average jitters in UDP traffic-single users

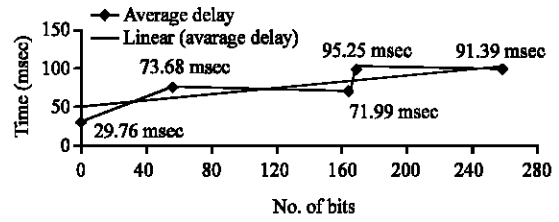

Fig. 4: Average delays in TCP traffic-multi users

71.99 up to 95.25 msec as the various encryptions is applied (Fig. 4). The highest delay recorded is in 168 bits 3DES cipher at 95.25 msec and the lowest delay is in 160 bit SEAL cipher at 71.99 msec. The second highest delay is in 256 bit AES cipher at 91.39 msec followed by 56 bit DES cipher at 73.68 msec.

With the 160-bits increase from 2.8 times higher than 56 bits, SEAL has 2% decreases in percentage while 168 bit which is 3 times greater than 56 bit has increase by 29% in delay and 24% increase in 256 bit AES which is 4.5 times >56 bit DES (Table 3).

UDP Traffic in IPSec multi user: In multi user UDP traffic the average jitter created between 2.73 and 3.81 msec (Fig. 5 and Table 4). The highest jitter is 3.81 msec in 256 bit AES cipher and the lowest jitter is 3.17 msec in 56 bit DES cipher while 168 bit 3DES is the second highest that has 3.51 msec of delay and followed by 160 bit SEAL at 3.22 msec.

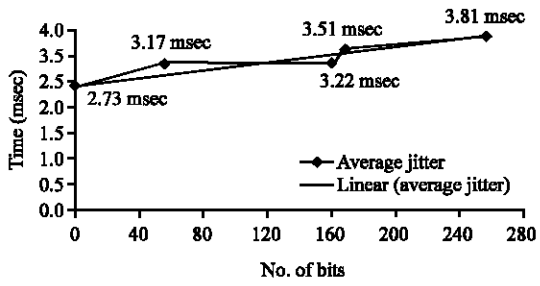

Fig. 5: Average jitter in UDP traffic-multi users

Table 1: Percentage delays increases in TCP traffic-single users

Percentage increase in delay-single user			
56 bits (DES)	160 bits (SEAL)	168 bits (3DES)	256 bits (AES)
-	2%	18%	0000.35%

Table 2: Percentage Jitter increases in UDP traffic-single users

Percentage increase in delay-single user			
56 bits (DES)	160 bits (SEAL)	168 bits (3DES)	256 bits (AES)
-	-30%	3%	7%

Table 3: Percentage delay increases in TCP traffic-multi users

Percentage increase in delay-single user			
56 bits (DES)	160 bits (SEAL)	168 bits (3DES)	256 bits (AES)
-	-2%	29%	24%

Table 4: Percentage jitter increases in UDP traffic-multi users

Percentage increase in delay-single user			
56 bits (DES)	160 bits (SEAL)	168 bits (3DES)	256 bits (AES)
-	2%	11%	20%

The highest percentage increase in jitter is at 256 bit AES with 20% increase from 56 bit DES, followed by 168 bit 3DES with 11% increase and 160 bit SEAL with only 2% increase in jitter. With the 2.8 times bit different from 56 bits DES, SEAL-160 reached only 2% increase in total average jitter while 168 bit of 3DES is 3 times bit of 56 bit DES and the percentage delay increase reached up-11%. Finally with the increase number of bit by 4.5 times the 256 bit AES has 20% increases in jitter.

"Quality of service is the ability to provide different priority to different applications, users or data flows or to guarantee a certain level of performance to a data flow" (Malik and Syal, 2010). To ensure the quality of service during IPSec remote communication between two sites, the performance of the connection need to meet the minimum requirement in latency, packet loss, jitter, Mean Opinion Score (MOS), R-factor. In this project we have used the latency and jitter as the main parameter to measure the performance of IPSec communication with various encryptions is applied. The avoid large latency/delay of the TCP packets in IPSec communication, the latency should not exceed 150 msec and to avoid such

under run of streaming video and audio the variation latency of receiving packets for UDP packets should not exceed 20-50 msec (Malik and Syal, 2010).

The overall results from Fig. 2 and 3 show that the highest delay and jitter created in single user environment is 37.41 msec for TCP data and 0.185 msec in UDP data. In multi-user environment (Fig. 4 and 5) the highest delay is 91.39 msec for TCP data and jitter is 3.81 msec for UDP data. This indicates that for the traffic size range from 128 bytes up to 4096 bytes the average delay and jitter are less than standard delay and jitter in IPSec communication. However, since the overhead is added in packet headers during the encryption process the average delay and jitter will be increased if the packet sizes are greater (Hattingh and Szigeti, 2004).

In single and multi-users environment the results have shown that SEAL 160 bit has outperform 3DES and AES in latency and jitter during encryption and decryption process in IPSec secured tunnel for single user. With eight bits different from 3DES, SEAL able to perform 9 times faster than 3DES-168 bits and 17 times faster than AES-256 bits. According to Saxena and Shibhu (2013) the quantity of time take by an encryption algorithm to produce a cipher text is considered as the encryption speed. This indicates that the algorithm and number of bits used in the encryption cipher determine the performance of its encryption and decryption process. The higher the number of bits, the greater is the latency in the encryption process. It can be prove by observing the AES bits allocation and the algorithm operation in the encryption and decryption process. A performance analysis conducted by Kumar and Kumar (2012) shows that the AES 128 bits key is claimed to the fastest block cipher compared to DES and 3DES. However, when the number of bits is increased to 198 and 256 bits the performance will also be affected because the number of rounds will increase from 12-14 rounds (Daemen and Rijmen, 2013). Therefore, in this experiment the AES-256 bit produces the highest number of delay at 37.41 msec during data transfer between two private networks. Similarly, 3DES uses 56 key bundles to encrypt the block of data three times using three different keys known as K2, K2 and K3 which will output 168bits block of data (FIPS, 1999). Three times iteration will cost the hardware resources to do its algorithm calculation during the encryption which is shown in Fig. 4 that 3DES delay 32.58 msec. SEAL-160 bits however, still perform as fast as the DES-56 bits at 28.16 msec which is 2% increase from DES-56 bits, despite the bits number is 104 bits higher than DES56 bits.

According to Schneier and Whiting (1997) SEAL is one of the stream ciphers that research at software basis that perform CPU optimization during the encryption and decryption process. In addition, stream ciphers operate on small unit of plain text where each unit input is continuously outputted one at a time. In contrast, the block ciphers break the input into blocks and perform encryption independently to each block.

CONCLUSION

The IPSec is the IETF standard suit of protocols that provides data authentication integrity and confidentiality between two communication points across IP network. It requires encryption mechanism in order to achieve the maximum protection that is offered. In this study, we have done a performance analysis to various encryption ciphers that is commonly used in the IPSec encapsulation security payload alongside with authentication header. Our aim is to conduct a performance evaluation is to find the optimal encryption cipher for fast encryption and decryption in IPSec tunnel mode. We have analysed the performance of four encryptions (DES, 3DES, AES and SEAL) and selected the best encryption cipher based on less delay and jitter produced during the data transmission between two sites using the IPSec tunnel mode. The experiment process consists of generating traffic with different sizes from private network A to B. During the generation process the data was monitored, captured and analysed. The result shows that for each pre-shared encryption used in the IPSec encapsulation, the SEAL cipher is proven to be the fastest cipher in encrypting the TCP and UDP packets through IPSec tunnel mode in single and multi-user environment. Finally, the significant of this study provide us with another alternative to make use of IPSec features in providing a high secured communication path without affecting the performance of the network.

ACKNOWLEDGEMENT

Researchers are thankful to Charles Darwin University for providing the funding support and necessary facilities for the preparation of the research.

REFERENCES

Aggarwal, K., J.K. Saini and H.K. Verma, 2013. Performance evaluation of rc6, blowfish, des, idea, cast-128 block ciphers. Intl. J. Comput. Appl., 68: 10-16.

Botta, A., A. Dainotti and A. Pescape, 2012. A tool for the generation of realistic network workload for emerging networking scenarios. Comput. Netw., 56: 3531-3547.

Daemen, J. and V. Rijmen, 2013. The Design of Rijndael: AES-the Advanced Encryption Standard. Springer, Berlin, Germany, ISBN:978-3-642-07646-6, Pages: 237.

Doraswamy, N. and D. Harkins, 2003. IPSec: The New Security Standard for the Internet, Intranets and Virtual Private Networks. 2nd Edn., Prentice Hall, Upper Saddle River, New Jersey, ISBN:0-13-046189X, Pages: 139.

FIPS., 1999. Data Encryptions Standard (DES). National Institute of Standards and Technology, Gaithersburg, Maryland.

Frankel, S., 2011. Demistifying the IPsec Puzzle. Artech House, Norwood, Massachusetts,.

Hattingh, C. and T. Szigeti, 2004. End-to-End Qos Network Design: Quality of Service in Lans WANs and VPNs. 1st Edn., Cisco Press, Indianapolis, Indiana,.

Kumar, A., S. Sinha and R. Chaudhary, 2013. A comparative analysis of encryption algorithms for better utilization. Intl. J. Comput. Appl., 71: 19-23.

Kumar, V.H. and S.R. Kumar, 2012. Performance analysis of rc6, twofish and RIJNDAEL block cipher algorithms. Intl. J. Comput. Appl., 42: 1-7.

Malik, R. and R. Syal, 2010. Performance analysis of IP security VPN. Intl. J. Comput. Appl., 8: 5-9.

Rogaway, P. and D. Coppersmith, 1998. A software-optimized encryption algorithm. J. Cryptology, 11: 273-287.

Saxena, P. and S. Shibhu, 2013. Performance analysis of best and njjsaa. Intl. J. Comput. Appl., 72: 33-37.

Schneier, B. and D. Whiting, 1997. Fast software encryption: Designing encryption algorithms for optimal software speed on the Intel Pentium processor. Proceedings of the International Workshop on Fast Software Encryption, January 20-22, 1997, Springer, Berlin, Germany, ISBN:978-3-540-63247-4, pp: 242-259.

Sharif, S.O. and S.P. Mansoor, 2010. Performance analysis of stream and block cipher algorithms. Proceedings of the 2010 3rd International Conference on Advanced Computer Theory and Engineering (ICACTE), August 20-22, 2010, IEEE, Bangor, Maine, ISBN:978-1-4244-6539-2, pp: V1-522-V1-525.

Sharma, V. and M. Kalra, 2009. Performance analysis and enhancement in IPSEC VPN to reduce connection establishment overhead and transmission delay: Part 1. Intl. J. Adv. Sci. Technol., 8: 422-430.