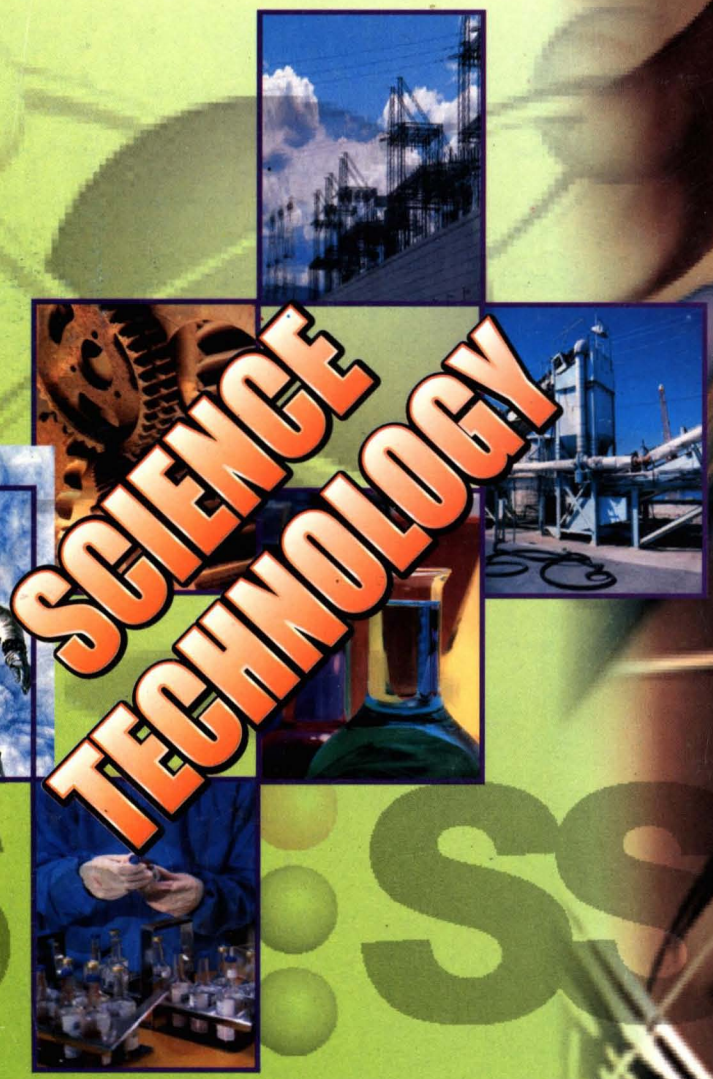
UNIVERSITI TEKNOLOGI MARA

ISO 9001:2000 No Sijil :0500132

Globalising Knowledge and Information



NATIONAL SEMINAR ON SCIENCE TECHNOLOGY & SOCIAL SCIENCES 2006

30-31 May 2006

Swiss Garden Resort & Spa

Kuantan, Pahang

Performance Analysis of AES (Advance Encryption Standard) in IPSec (Internet Protocol Security)

Nik Shahidah Afifi Md Taujuddin,
Abdul Hanan Abdullah
Mohd Aizaini Maarof

ABSTRACT

The Internet Protocol Security (IPSec) is a standard-based method that being used to protect the information that traverse in the Internet networking without expensive cost or complex modification on Internet application itself. But with the growth of the new technology, IPSec is subject to many treats. But the major treat of the IPSec is caused by the usage of the algorithm that has weak keys. The algorithms are DES, 3DES, Blowfish, Cast128 and RC5. These algorithms are being used as encryption algorithm in Encapsulated Security Payload (ESP) protocol. Besides, the encryption speed of these algorithms is too slow and it can only encrypt a small size data. So, to overcome these problems, this research is done to improve the security on IPSec. Throughout this research, a new algorithm from NIST that is Advance Encryption Standard (AES) is found can be used in IPSec to overcome these problems. But to make it happen, some work must be done. Initially, the framework of Internet Security Association Key Management Protocol (ISAKMP) is done. After that, the protocol is building to suite the AES in IPSec. It involve a process of initialize the ID transform value for AES and initialize the SA (Security Association) message. After that, a prototype is build to test the execution of the propose protocol. The research is then continued by doing some analysis to determine the propose protocol's performance.

Keywords: *Internet Protocol Security (IPSec), Advance Encryption Standard (AES), Internet Security Association Key Management Protocol (ISAKMP)*

Introduction

Internet is changing many ways of our life style. It change the way of communication, business, entertainment, learning and so on. The Internet users are increasing rapidly day after day makes it a popular medium to exchange document, selling product and services and also distributing information.

But, Internet is so vulnerable, it facing with so many treat such as packet spoofing, sniffers, password cracking and Denial of Service (DOS). Internet communities around the world are trying to solve this problem by providing alternative to solve the problem.

One of the most popular ways is by using Internet Protocol Security (IPSec). IPSec is an IP security protocol founded by researchers from IETF (Internet Engineering Task Force) (Atkinson, 1995 and Kent and Atkinson, 1998). IPSec is using some cryptographic algorithm to perform encryption and authentication process.

IPSec contains 3 major components that is AH (Authentication Header), ESP (Encapsulation Security Payload) and ISAKMP (Internet Security Association Key Management Protocol). AH provides authentication process for original packet data. ESP is giving encryption service to the packet data while ISAKMP is defining the procedures and packet format to negotiate, produce and modify the Security Association (SA). SA contains all the information of security mechanisms that will be used during the communication process.

Problem Background

Data security is a major concern in transaction of information in Internet. Thousand of researches have been done to find out the best way to solve this problem. A research from Matt Blaze show that the level of security will increase with the increasing of security technique implemented in network layer (Blaze, et al. (2001).

One of the main problems in IPSec is the use of weak encryption algorithm. Currently, it used DES, RC5, Blowfish, IDEA, CAST128 and 3DES (Bellovin, 1997 and Smith 1997). But all of them are labeled as not secured anymore.

For DES algorithm, it is found as weak because the key is already broken up by hackers (Blaze, et al. 1996, Smith 1997, Ferguson and Schneier 2001 and Chodowiec, et al. 2001). Hacker can only try any suitable key to break the system. This technique is called brute force.

A findings from a cryptographic group DESCHALL shows that the DES key can be cracked using brute force technique only just by 72 quadrillion of times trial (Curtin and Dolske 1998).

Blowfish algorithm is suitable for high speed hardware (Schneier 1994). But it is also defined as weak algorithm. So, Pereira suggests the use of RC5 algorithm. But from the research done by Biryukov and Kushilevitz they found that RC5 was already broken up and it won't be save anymore (Biryukov and Kushilevitz 1998).

IDEA is a block cipher using 8 times round to complete a process. IDEA is a fast algorithm and it commonly being used in hardware. But, the weaknesses of IDEA are it is expensive and the key is also had been cracked (Schneier and Whitting 2001 and Pereira and Adams 1998).

While for 3DES, it uses encryption 48 times round, 64 bit block and 48 sub-keys. But, a research from Pereira and Adams found that it already has 64 weak keys including 80 half-weak keys (Pereira and Adams 1998).

System Design

So, to overcome the problem, a new strong encryption algorithm must be implemented in IPSec to ensure the security. The National Institute of Science and Technology (NIST) have founded a new cryptographic algorithm name Advance Encryption Standard (AES). AES is currently has the highest level of security and its' characteristic is very efficient (Wright 2001).

So, AES is a very suitable algorithm to replace the recent algorithm that being used in IPSec. But some work must be done to ensure that AES can operate in IPSec environment.

A research is done to find out the Identification Transform value for AES in IPSec. Throughout the work that has been done, we found that the ID Transform value for AES is 12. Besides, data packet format for Security Association (SA) has been designed to make sure that communication can be done during data transferring.

Analysis

From the research that has been done, we found that AES can operate perfectly in IPSec environment. Besides, it shows a good performance compared to the recent algorithm used in IPSec. It shows the lowest round trip time, a high throughputs performance and ability of using a various and long size data and key.

Round Trip-Time Analysis

Round Trip-time analysis is proposed by Braun to examine the encryption impact on round trip data packet performance (Braun et al 2000). He said that encryption process during data transmission will bring a heavy load to the system. It is because the encryption process will increase the system activity and will boost up the round trip time.

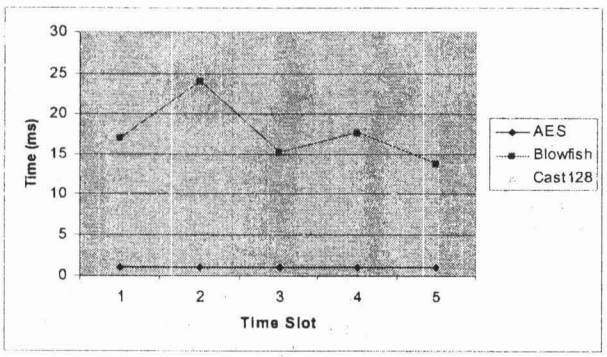


Fig. 1: Round Trip Time Analysis

Figure 1 shows the differences of the round trip time between AES, Blowfish and Cast128. From the chart, we found that the round trip time for Blowfish and Cast128 are high and not uniform. While the round trip time for AES is low and rather uniform.

Throughputs Performance Analysis

The analysis is done to measure throughputs performance of a system. That system is using encryption algorithm to make the data encryption process. For this analysis, a program called TTCP (Test TCP) is used to measure the performance.

TTCP is used to measure bit, data string or data block that traverse in a data communication system. It is also a measurement indicator for work load of a system for a certain time.

Referring to David G. Andersen (Andersen 2001) throughputs value from TTCP program is referring to system performance doing encryption and decryption process on data packet. The speed of encryption and decryption process will give an impact to the speed of process that can be done in a time.

Table 1: Average throughputs Value for Four Loader Size

	Throughputs value (KB/s)			
Algorithm/Loader	7000	8192	9000	10000
3DES	422.73	419.49	422.23	423.28
BLOWFISH	747.32	741.94	731.96	745.28
AES	**855.95**	**846.98**	**854.84**	**839.2**

The Table 1 shows the average throughputs value using some loader size. From the table, we can see that the AES shows the best performance for all experiment that has been done. AES also shows the highest throughputs value for all loader size. For this experiment, we used four loader size that is 7000, 8192, 9000 and 10 000 with default loader is 8192.

Discussion

There are some problems occurred when IPSec is used. But the main problems of IPSec is the usage of weak encryption algorithm. DES, 3DES, Blowfish, Cast128 and RC5 are some algorithm that have been used in IPSec. The use of weak algorithm will cause many problems in transmitting data.

From the research that have we done, AES is the suitable encryption algorithm to replace the recent algorithm in IPSec. It has no weak keys or even half-weak keys. It also allows the usage of big key size that is 92,128 and 192 and all the keys in 32 increments such as 32, 64 and 96. So, it will increase the security level of information hidden.

To make sure that AES can be implemented in IPSec, it must get it transform identification. Throughout research that has been done, we found that transform ID value for AES is 12. Some modification also will be done at ISAKMP protocol.

Conclusion

From the experiment, we found that AES functioning well with the protocol suggested. Besides, it shows the best performance overall compared to the recent encryption algorithm. AES shows a low round-trip time, the higher throughputs performance and allow multiple key size.

References

Atkinson, R. (1995c). *Security Architecture for the Internet Protocol.* RFC 1825, Internet Engineering Task Force.

Andersen, D.G. (2001). *Resilient Overlay Networks.* Master Thesis. Massachusetts Institute of Technology.

Bellovin, S.M. (1997). Probable Plaintext Cryptanalysis of the Security Protocols. *Proceeding of the 1997 Symposium on Network and Distributed System Security.*

Biryukov, A & Kushilevitz, E. (1998). *Improved Cryptanalysis of RC5.* Advance in Cryptology – EUROCRYPT'98 Proceedings, Springer-Verlag: pp. 85-99.

Blaze, M., Diffie, W., Rivest, R., Schneier, B., Shimomura, T., Thompson, E. & Weiner, M. (1996). *Minimal Key Lengths for Symmetric Ciphers to Provide Adequate Commercial Security.* Minneapolis, USA: Counterpane Internet Security, Inc.

Blaze, M., Ionnidis, J. & Keromytis, A. D. (2001). *Trust Management and Network Layer Security Protocol.* San Diego: NDSS.

Braun, T., Gunter, M., Khalil, I. & Liu, L. (2000). *Performance Evaluation for Virtual Private Network.* Institute for Informatics and Angewandte Mathematics (AIM), University Bern.

Chodowiec, P., Gaj, K., Bellows, P. & Scott, B. (2001). Experimental Testing of Gigabit IPSec-Compliant Implementation of Rijndael and Triple DES Using SLAAC-1V FPGA Accelerator Board. *Proceedings Information Security Conference*, Spain.

Curtin, M. and Dolske, J. (1998). *A Brute Force Search of DES Keyspace.* RSA Data Security Inc.

Ferguson, N., & Schneier, B. (2001). *A Cryptographic Evaluation of IPSec.* Minneapolis, USA: Counterpane Internet Security, Inc.

Kent, S. & Atkinson, R. (1998a). *Security Architecture for Internet Protocol.* Internet Engineering Task Force, RFC 2401.

Pereira, R. & Adams, R. (1998). *The ESP CBC-Mode Cipher Algorithm.* Internet Engineering Task Force, RFC 2451.

Schneier, B. (1994). Description of a New Variable-Length Key, 64-Bit Block Cipher (Blowfish). *Fast Software Encryption, Cambridge Security Workshop Proceeding*, Spinger-Verlag: pp. 191-204.

Schneier, B. & Whiting, D. (2001) *Fast Software Encryption: Designing Encryption Algorithms for Optimal Software Speed on the Intel Pentium Processor.* Minneapolis, USA: Counterpane Internet Security, Inc.

Smith, R.E. (1997). *Internet Cryptography.* Massachusetts: Addison Wesley Longman, Inc.

Wright, M.A (2001). The Advanced Encryption Standard. *Journal Network Security*: pp. 11-13.

NIK SHAHIDAH AFIFI MD. TAUJUDDIN, Kolej Univesiti Teknologi Tun Hussien Onn.

ABDUL HANAN ABDULLAH & MOHD AIZAINI MAAROF, Universiti Teknologi Malaysia.