International Journal of Innovative Technology and Exploring Engineering (IJITEE)
ISSN: 2278-3075 (Online), Volume-9 Issue-4, February 2020

A Procedure to Prevent Confidential Information Leakage of Government Organizations in Bangladesh using Isakmp Cryptographic Technique

Tasniya Ahmed , Marjia Sultana, Md. Rakib Hasan , Mahmuda Khatun , Israt Jahan

Abstract— To ensure security for the transmission of confidential information, Cryptographic algorithms play an important role in providing security against malicious attacks. Confidential information is exchanged among different organizations of the government. If the necessary security is not involved there, the information will be leaked due to un-trusted transmission, unattended nature and get access easily which can cause a disaster in the government system. In this research, my centre of attention is to prevent confidential information leakage in government organization using ISAKMP cryptographic technique.

Keywords: Internet Security Association and Key Management Protocol (ISAKMP), Internet Key Exchange (IKE).

I. INTRODUCTION

In traditional government system, the letters are exchanged through post office which can be insecure. But sensitive data exchanged among government organizations need to be encrypted to prevent it from being disclosed or modified by unauthorized parties.

In today's world internet is available everywhere in our house, in my work place, mobiles, cars everything is connected to the internet and if an unauthorized person is able to get access to this network he can not only spy on us but he can easily mess up our lives. And it is more important for a government organization.

II. LITERATURE REVIEW

Now-a-days for secure communication, Cryptography has received an enormous attention. In Cryptography, ISAKMP Cryptography is more secure.

Therefore, research on ISAKMP has been carried out by researchers [1]-[7].

Revised Manuscript Received on February 28, 2020.

***** Correspondence Author

Tasniya Ahmed *, Institute of Information Technology, Noakhali Science & Technology University, Nokhali-3814, Bangladesh. E-mail: tasniya.iit@nstu.edu.bd

Marjia Sultana, Department of Computer Science & Engineering ,Begum Rokeya University, Rangpur-5404, Bangladesh. E-mail: marjia.cse@brur.ac.bd

Md. Rakib Hasan, Department of Information and Communication Technology, Comilla University, Cumilla - 3506, Bangladesh. E-mail: rakib@cou.ac.bd

Mahmuda Khatun, Department of Computer Science & Engineering, Comilla University, Cumilla - 3506, Bangladesh. E-mail: mahmuda@cou.ac.bd

Israt Jahan, Department of Computer Sciene & Engineering, Jahangirnagar University, Savar, Dhaka, Bangladesh. E-mail: isratju1@yahoo.com

Charles M Kozierok describes about IPsec and it's ability to encrypt any higher level messaging [1].

A researcher, Hani Alsharani describes how to provide a set of security services for traffic at the IP layer, in both the IPv4 and IPv6 environments [2].

A module describes how to configure the Internet Key Exchange (IKE) protocol for basic IP Security (IPsec) Virtual Private Networks (VPNs) [3].

A paper of Prof. Dr. P. Trommler describes the pros and cons of ISAKMP, Security Association and Management [4].

A module provides an overview of IP access lists [5]. There is a guide for network managers who perform any of the following tasks: Manage network security, Install and configure firewalls/security appliances, Configure VPNs, Configure intrusion detection software [6].

However, the final expression of the research work do not enough to implement ISAKMP Cryptography technique. Hence, I have proposed ISAKMP cryptography and configure for secure efficient communication management of government institution.

III. RESEARCH CONTRIBUTION

We develop an efficient algorithm with high accuracy and the system reduce time and cost.

If our proposed Methodology is applied to the government system of Bangladesh, then various file transfer like very confidential papers of government will be transferred in secure manner.

At last we also observe the capacity of the system and simplifies network design which saves bandwidth and control congestion.

A. Proposed Algorithm

Input: Data Packets

Output**:** Successfully sent the packet to destination.

1. Initialization
2. If ISAKMP Cryptographic Technique is enabled in the network, go to step 3 otherwise go to step 11.
3. Apply DES encryption algorithm and go to step 4.
4. Apply SHA hash algorithm.
5. If crypto map is enabled in the network, go to step 6 otherwise go to step 11.
6. Apply transform set and pfs protocol and go to step 7.
7. Set peers and go to step 7.
8. Set access list.
9. Sender sent the packet to the destination in the ISAKMP enabled network in the encrypted form.

10. Receiver received the packet and decrypted it.
11. End

B. Configuration of ISAKMP in phase 1

- In phase 1, There are five policy parameters to enable ISAKMP. These are:
- An encryption method with DES or AES, to ensure privacy.
- An authentication method with RSA public key or preshare, to ensure the identity of the peers.
- A Hashed Message Authentication Codes (HMAC) method with Secure Hash Standard-1(SHA-1) or Message Digest algorithm(MD5) to ensure the identity of the sender, and to ensure that the message has not been modified in transit.
- A Diffie-Hellman group is used to determine the strength of the encryption-key-determination algorithm. This algorithm is used to derive the encryption and hash keys.
- The encryption key use a time limit before replacing it.

C. ISAKMP in phase 2

In phase 2, Crypto map is used.Which traffic should be protected by IPSec, where IPSec-protected traffic should be sent, and what IPSec transform sets should be applied to this traffic, is specified by Crypto map [7].
Crypto map includes transform set , pfs protocol, peer, access list and life time.

IV. EXPERIMENTAL RESULTS

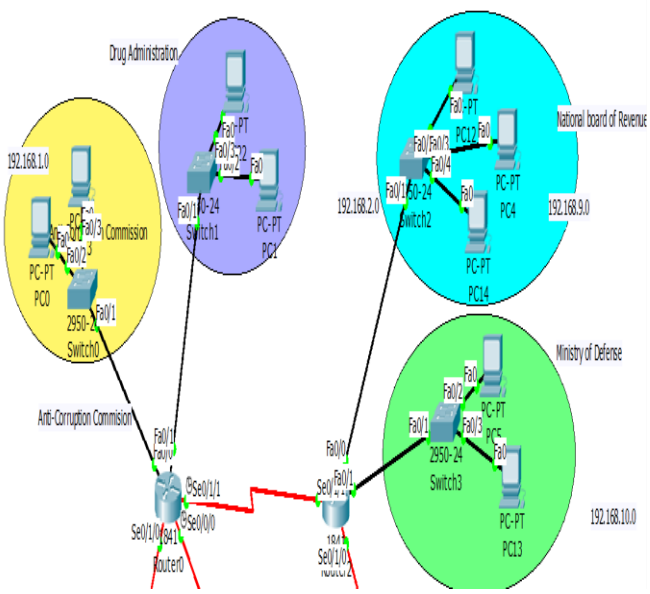

Fig.1. Network System with Anti-Corruption Commission, Drug Administration, National Board of Revenue and Ministry of Defense

Table I. Result Evaluation

Sourc-e	Destination	Encrypted packets	Decrypted Packets	Sent error	Received error
Natio-nal Broad of Reve-nue	Ministry of Defense	7	7	0	0
Anti-Corru-ption Com-missi-on	Drug Administration	14	14	0	0
Public Admi-nistr-ation	Health Ministry	6	5	1	0
National Broad of Reven-ue	Anti-Corruption Commission	10	10	0	0
Minis-try of Finan-ce	Department of Immigrati-on & Passport	5	5	0	0

V. CONCLUSION & FUTURE SCOPE

The implementation of ISAKMP Cryptography is quite complex but it shows optimum results in respect to the other cryptosystem.
We believe that with sufficient equipment in future we can implement our simulated work. We can bring the whole government system of Bangladesh within a secured network system in cost effective and efficient way ensuring the security issues.

REFERENCES

1. Charles M Kozierok, "*The TCP/IP guide: a comprehensive, illustrated internet protocols reference*," No Starch Press, Inc. 38 Ringold Street, San Francisco ,William Pollock, 2005.
2. Hani Alsharani ,"*Internet Protocol Security (IPSec) Mechanisms* " ,International Journal of Scientific & Engineering Research", Volume 5, 2014, ISSN 2229-5518 .
3. "*Internet Key Exchange Protocol*", (Cisco systems Inc ,2001)
4. Prof. Dr. P. Trommler, "*FWPF Internet Security(GSO FH Nurnberg, Fachrichtung Informatik,2004*)".
5. "*Security Configuration Guide: Access Control Lists, Cisco IOS XE Release 3S*," Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706.
6. "*Cisco Security Appliance Command Line Configuration Guide*" Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA.
7. "*VPN Availability Configuration Guide, Cisco IOS Release 12.4T*", Chapter: IPsec VPN High Availability Enhancements.

AUTHORS PROFILE

Tasniya Ahmed has completed her B.Sc. (Honors) in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh in 2016 and MSc. in 2018 from the same University. Currently, She is working as a Lecturer at Institute of Information Technology, Noakhali Science & Technology University, Noakhali. Previously She worked as a Lecturer at Department of Computer Science and Engineering, Daffodil International University, Dhaka from May 2017 to February 2019 and Gono University from June 2016 to April 2017. Her research interest includes Cyber Security, Machine Learning, Artificial Intelligence and Data mining.

Marjia Sultana, currently working as a Lecturer at the department of Computer Science and Engineering of Begum Rokeya University, Rangpur, Bangladesh. She received her B.Sc.(Hons) degree in Computer Science and Engineering from Jahangirnagar University, Savar, Dhaka in 2016 and M.Sc. degree from the same university in 2018. Her teaching experience includes taking different post graduate (M.Sc.) and under graduate (B.Sc.) courses. Her research interest focuses on Machine Learning, Data Mining, Artificial Intelligence, Image Processing and Computer Networking.

Md. Rakib Hasan has completed his B.Sc. (Honors) and M.Sc. in Computer Science and Engineering from Jahangirnagar University, Dhaka, Bangladesh in 2016 and 2018 respectively. He is now working as a Lecturer at Department of Information and Communication Technology, Comilla University, Cumilla. Previously he worked as a Lecturer at Department of Computer Science and Engineering, Daffodil International University, Dhaka from May 2016 to February 2019. He is currently working on Artificial Intelligence and Machine Learning. His research interest includes Natural Language Processing, Machine Learning, Cyber Security and Computer Vision. He is actively engaged in educational activities.

Mahmuda Khatun, a faculty member of the Faculty of Engineering, Comilla University, Bangladesh, is currently working as a Lecturer at the department of Computer Science and Engineering. She has completed her B.Sc. (Hons) in Computer Science and Engineering from Jahangirnagar University, Savar, Dhaka in 2016 and M.Sc. from the same university in 2018. Her teaching experience includes different graduate (M.Sc.) and under graduate courses. Her current research interest includes Wireless Communication, Machine Learning, Artificial Intelligence and Image Processing.

Israt Jahan, Professor, Department of Computer Science and Engineering, Jahangirnagar University ,Dhaka, has completed her B.Sc. and MSc from BUET. Her research interest includes E-Commerce, Computer Security, E-Governance, and Communication