ISSN: 2321-7782 (Online)
e-ISJN: A4372-3114
Impact Factor: 7.327

Volume 6, Issue 11, November 2018

International Journal of Advance Research in Computer Science and Management Studies

Research Article / Survey Paper / Case Study

Available online at: www.ijarcsms.com

Constraints of 3C Application for Packet Encryption

Prof. Harshika Rana[1]
Dept. BCA, PICA
Parul University
Vadodara – India.

Dr. Vishal Dahiya[2]
Dept. MCA, IICT
Indus University
Ahmedabad – India.

Abstract: ***Any innovative approach is end result of solving hurdles which were arising during research work. These hurdles are nothing but some limitations or constraints which indicate us for dead end and thus researcher will try to find new way to solve problem. For 3C: Customized Cascaded Cryptography application on packet in real mean will be very difficult. There were few constrains arise in terms of firewall policy, Commands and Encryption Policy. Finally it will conclude in own customized tool to be developed for application of 3C concepts for packet encryption.***

Keywords: Firewall policy, Encryption Policy, Commands, 3C, Customized, Cascaded, Cryptography, router, Ipsec, Security, SSL, IP, TCP, Header, Security Header.

I. INTRODUCTION

Network Encryption means encryption services which are provided in network layer. Packet security or packet encryption is one of the latest concepts in data security field. IPsec and SSL are two major services through which this security can be achieved.

But 3C is most efficient way to do packet encryption in terms of cost and usability.

In the network, packets have payload in plain text which can be easily monitor through network traffic monitoring systems(software). So now a day it is mandatory to encrypt packets, thus intruders (sniffers) will not be able to trace payload from the encrypted form.

II. OVERVIEW OF SYSTEM

Generally TCP IP packet has TCP header which determines which determines where packet should go within the network and IP header is used to determine where data should reach to get data from a to b within the network.

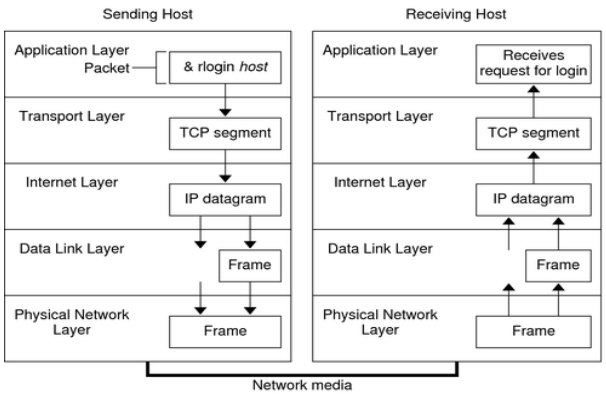


Fig. 1 General IP packet with ISO layer

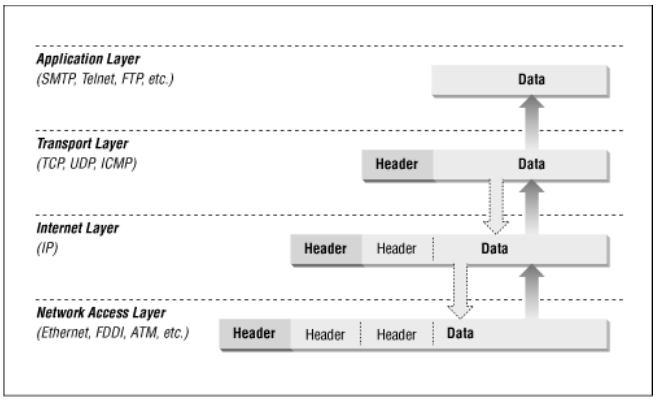


Fig. 2 General IP packet with header detail

1. ***IPsec:***

IPsec is one of the latest service which add one header to packet named as IPsec header which is determine only by the authentic nodes. There are two modes of Ipsec: Tunnel mode and Transport mode.

Transport Mode: This mode is basically use for giving security to end to end i.e node to node and in this mode packet has three headers: (a) IP header (b) IPsec header (c) TCP header in the sequence.

Tunnel Mode: This mode is basically use for giving security router to router and in this mode packet has four headers:

(a) Ip header- for identifying router's Ip and (b) Ipsec Header (c) Ipheader – to determine machine's ip and (d) TCP header.

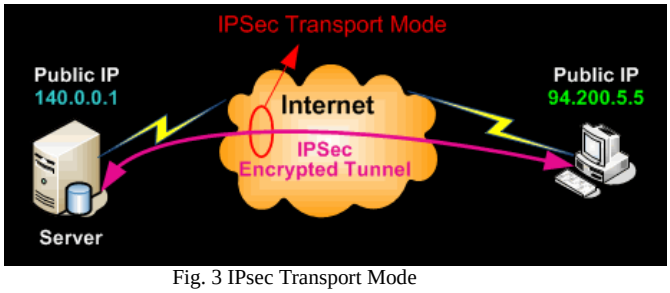


Fig. 3 IPsec Transport Mode

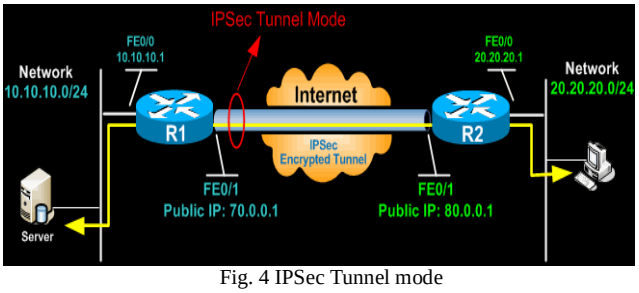


Fig. 4 IPSec Tunnel mode

2. ***3C: Customized Cascaded Cryptography flow chart:***

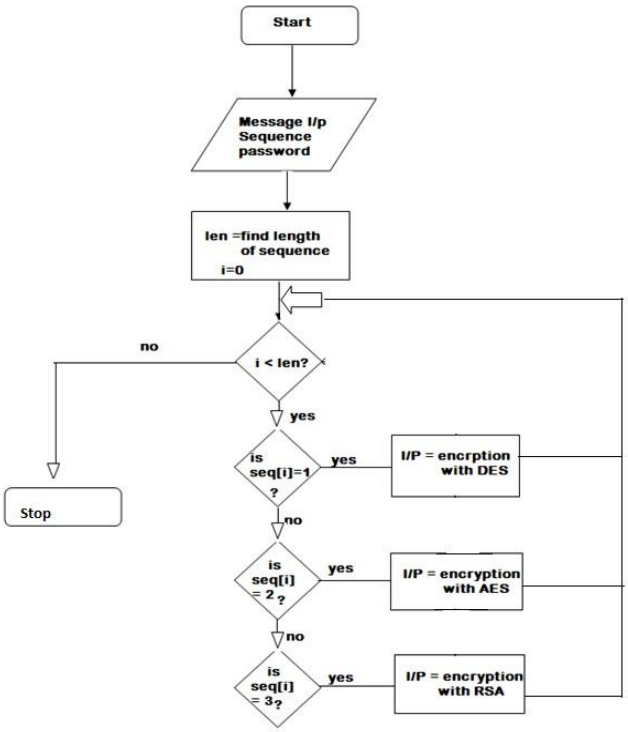


Fig. 5 Flow chart of 3C

III. Techniques and Constraints for 3C Application in Packet Encryption

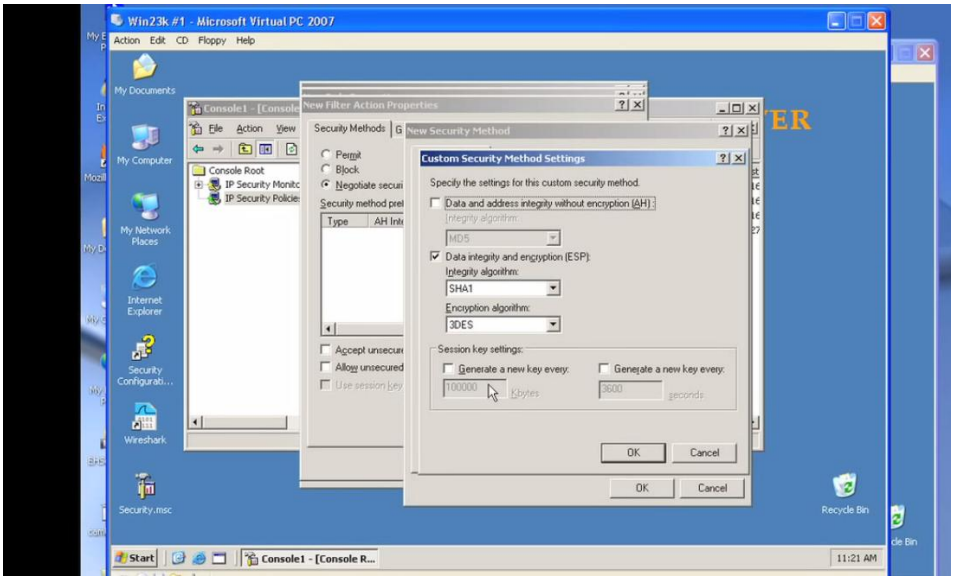
1. ***First Technique:***

By creating encryption policies between two nodes

Steps:

1. Create virtual pc
2. Create a policy between two node
3. Command for microsoft management console – run ->mmc and do further process

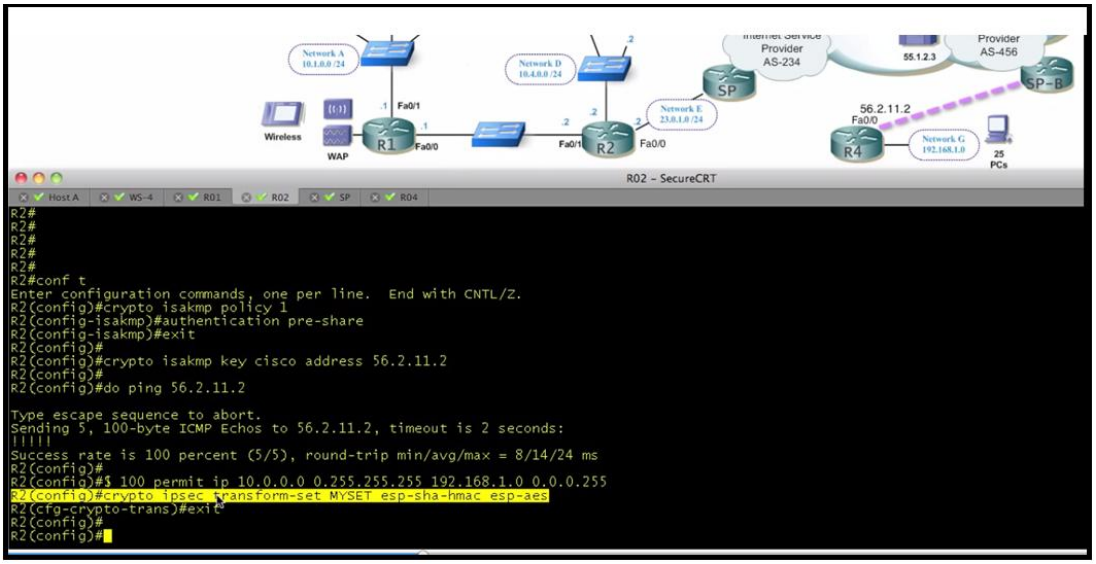
Constraint: we cannot run multiple policies at a same time thus we cannot implement 3C through this method.



2. Second Technique:

By configuring two routers/ two nodes through command prompt i.e transform set

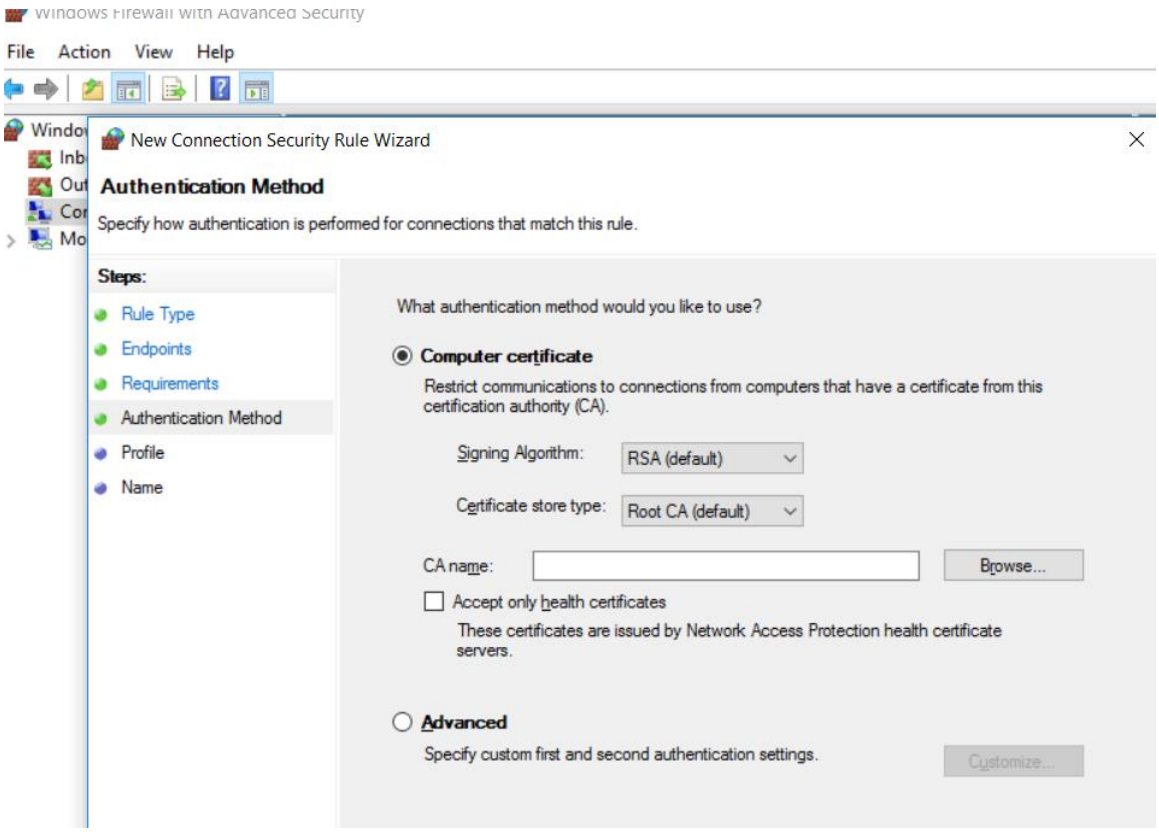
Command : #crypto transform-set esp-SHA-hmac esp-aes



Constraint: You can set multiple algorithm and policy but you can run one policy at a time.

3. Third Technique:

By setting firewall Policy: You can set a authentication method and algorithm through fire wall new rule connection authentication method.



Constraint: You can set only one algorithm at a time in customized rule.

IV. Conclusion

As we have discussed major three constraints arises when we tries to establish secure communication way between two router or two nodes through 3C algorithm thus we can conclude that we have to make a tool or an application which uses 3C algorithm and we can analyze packet through different packet analysis software like wireshark etc. As encrypted payload will be pass then it will be very difficult to crack plaintext from packet.

Acknowledgement

With a deep sense of gratitude, I express my sincere thanks to my esteemed and worthy Supervisor **Dr. Vishal Dahiya,** Director, Department of Computer IICT, Indus University, Ahmedabad for her immense help, valuable guidance, effective supervision, stimulating suggestions and encouragement at all times while carrying out this research work.

References

1. http://www.firewall.cx/networking-topics/protocols/870-ipsec-modes.html
2. https://docs.oracle.com/cd/E18752_01/html/816-4554/ipov-29.html
3. http://web.deu.edu.tr/doc/oreily/networking/firewall/ch06_03.htm
4. https://www.youtube.com/watch?v=gP1LtwqYYq4
5. https://en.wikipedia.org/wiki/IPsec
6. https://security.stackexchange.com/questions/34391/how-to-encrypt-packets-in-network
7. https://security.stackexchange.com/questions/18087/is-multiple-encryption-a-good-idea
8. https://ssl.trustwave.com/support/support-how-ssl-works.php
9. https://vpn-services.bestreviews.net › Articles
10. https://www.youtube.com/watch?v=CuxyZiSCSfc
11. https://codebeautify.org/hex-string-converter
12. https://www.httpwatch.com/
13. https://www.wireshark.org/
14. Lauren Darcey and Shane Conder, "Android Wireless Application Development" by, 2nd Edition, Pearson Education. [2011].

A Tanenbaum ," Computer Networks " ,5th ed., McGraw-Hill

15. Hashika Rana , Vishal Dahiya "Data Secrecy using 3C with Mobile Application and Packet Encryption", IEEE,International Conference on Networks & Advances in Computational Technologies on July 20-22, 2017ISBN No:978-1-5090-6590-5
16. Harshika Rana, Vishal Dahiya, "Value Addition in Cascaded Cryptography", NCEETM, ISSN 2349-4301, January 2015
17. Harshika Rana, Prashant Pittalia, "Advances in cryptography", IJARCSMS, ISSN print 23471778 ISSN Online 23217782, April 2015

AUTHOR(S) PROFILE

Harshika Rana, has received MCA degree from GTU, Gujarat, India. She has been working as an Assistant Professor at Parul University, vadodara since 4 years and 7 months. She has published 2 International and 2 National research papers.She has been doing research work in network security as a part of PhD curriculum since 3.5 years at Indus University, Ahmedabad, Gujrat, India.

Dr. Vishal Dahiya, has received her PhD degree in 2013. She is serving as a HOD of IICT department, Indus University, Ahmedabad, Gujrat, India. She has a vast experience of 14 years in academic field. She has published more than 12 National and 16 International research papers.