Impact of MD5 Authentication in secured and non-secured traffic routing for the case of EIGRP, RIPv2 and OSPF routing protocols

KHALID AHMED ABU AL-SAUD

THESIS SUBMITTED IN FULFILMENT FOR THE DEGREE OF MASTER OF PHILOSOPHY

COLLEGE OF ARTS AND SCIENCE UNIVERSITY UTARA MALAYSIA

2009
KOLEJ SASTERA DAN SAINS
(COLLEGE OF ARTS AND SCIENCES)
UNIVERSITI UTARA MALAYSIA

PERAKUAN KERJA/TESIS'
(Certification of Thesis Work)

Kami, yang bertandatangan, memperakukan bahawa
(We, the undersigned, certify that)

KHALID AHMED ABU AL-SAUD

calon untuk Ijazah
(candidate for the degree of) SARJANA SAINS [TEKNOLOGI MAKLUMAT]

teiah mengemukakan tesis/disertasinya yang bertajuk
(has presented his/her thesis work of the following title)

IMPACT OF MD5 AUTHENTICATION IN SECURED AND NON-SECURED TRAFFIC ROUTING FOR THE CASE OF EIGRP, RIPV2 AND OSPF ROUTING PROTOCOLS

seperti yang tercatat di muka surat tajuk dan kulit tesis/disertasi
(as it appears on the title page and front cover of thesis work)

bahawa tesis/disertasi tersebut boleh diterima dari segi bentuk serta kandungan, dan
liputan bidang ilmu yang memuaskan, sebagaimana yang ditunjukkan oleh calon dalam
ujian ihsan yang diadakan pada: 02 Ogos 2009

(that the thesis/dissertation is acceptable in form and content, and that a satisfactory
knowledge of the field covered by the thesis was demonstrated by the candidate through an
oral examination held on

Pengerusi Viva
(Chairman for Viva) : Dr. Fauziah Baharom

Pemeriksa Luar
(External Examiner) : Prof. Madya Dr. Hj. Mazani Hj. Manaf

Pemeriksa Dalam
(Internal Examiner) : Encik Fazii Azzali

Penyelia Utama
(Principal Supervisor) : Prof. Madya Hatim Mohamed Tahir

Setiausaha Panel
(Panal Secretariat) : Dr. Mohd Syazwan Abdullah

Tandatangan:
(Signature)

Tandatangan:
(Signature)

Tandatangan:
(Signature)

Tandatangan:
(Signature)

Tandatangan:
(Signature)

Tandatangan:
(Signature)

Tarikh
(Date) : 02 Ogos 2009
PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a postgraduate degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree that permission for copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor(s) or, in their absence by the Dean of Academic, College of Arts and Sciences. It is understood that any copying or publication or use of this thesis or parts thereof for financial gain shall not be allowed without my written permission. It is also understood that due recognition shall be given to me and to Universiti Utara Malaysia for any scholarly use which may be made of any material from my thesis.

Requests for permission to copy or to make other use of materials in this thesis, in whole or in part, should be addressed to

Dean of Academic
College of Arts and Sciences
University Utara Malaysia
06010 UUt sintok
Kedah Darul Aman
Abstract

Routing is the process of forwarding data across an inter-network from a designated source to a final destination. Along the way from source to destination, at least one intermediate node is considered. Due to the major role that routing protocols play in computer network infrastructures, special cares have been given to routing protocols with built-in security constraints. In this thesis, we evaluate the impact of MD5 Authentication on routing traffic for the case of EIGRP, RIPv2 and OSPF routing protocols in case of secured and non-secured routing traffic. A network model of four Cisco routers has been employed and a traffic generation and analysis tools have been developed and used to generate traffic data and measure delay time, jitter and overhead. The results show that the average delay time and jitter in the secured MD5 case can become significantly larger when compared to the unsecured case even in steady state conditions. Also, the EIGRP protocol shows the minimum overhead even when the system is extremely overloaded.
Acknowledgments

This thesis concludes my Master’s Degree in Computer Network and Security submitted to the Applied Science Division, College of Arts and Science at University Utara Malaysia.

I would like to thank my supervisor Dr. Hatim Tahir for his excellent guidance, helpful advice and deeply support, my extend thanks also for the Associate Professor Dr. Suhaidí Hassan, Associate Professor and Assistant Vice Chancellor College of Arts and Sciences, at UUM.

I would like also to thank Dr. Moutaz Saleh and Dr. Mohamed Saleh for their support and enthusiasm. Dr. Moutaz has enhanced my knowledge and understanding for the art of thesis writing. Indeed, whenever I lost the sight of my thesis objectives, he proficiently led me back on the track.

My thanks to Dr. Adel El-Zoghbi for his initial support and guidance, and also, many thanks for Prof. Qutaibah Malluhi the Head of Dept. of Computer Science & Eng., College of Engineering Qatar University for his support and help.

Finally, my sincere thanks to my wife and kids, family and friends for their patience and encouragement, for them I dedicate this thesis.
Thesis list of tables:

Table. No.                                               Page
2.1: EIGRP Metrics                                           13
2.2: Summary of Common Routing Protocol Features                 22
2.3: Steps for Generating an Authenticated RIP Message   30
2.4: Steps for Retrieving MD5 Digest                          30
4.1: Key Features of Cisco Routers 1721                         50
4.2: Cisco Routers 1721 Front Panel LEDs Description           51
4.3: Cisco Routers 1721 Back Panel Ports Description           53
4.4: Cisco Routers 1721 Back Panel LEDs Description           53
4.5: Straight-through Ethernet Cable Pin-outs                    57
4.6: Cross-over Ethernet Cable Pin-outs                        57
4.7: Ethernet Cabling Guidelines                                58
4.8: Console Cable and Adapter Pin-outs                        59
4.9: Client/server personal computer specifications              65
### Thesis list of figures

<table>
<thead>
<tr>
<th>Fig. No.</th>
<th>Description</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>2.1:</td>
<td>IGRP Protocol Structure</td>
<td>11</td>
</tr>
<tr>
<td>2.2:</td>
<td>EIGRP Protocol Structure</td>
<td>12</td>
</tr>
<tr>
<td>2.3:</td>
<td>RIP Protocol Structure</td>
<td>16</td>
</tr>
<tr>
<td>2.4:</td>
<td>OSPF Protocol Structure</td>
<td>19</td>
</tr>
<tr>
<td>2.5:</td>
<td>Plaintext Neighbor Authentication</td>
<td>23</td>
</tr>
<tr>
<td>2.6:</td>
<td>MD5 Neighbor Authentication: Originating Router</td>
<td>24</td>
</tr>
<tr>
<td>2.7:</td>
<td>MD5 Neighbor Authentication: Destination Router</td>
<td>25</td>
</tr>
<tr>
<td>2.8:</td>
<td>EIGRP MD5 Authentications</td>
<td>27</td>
</tr>
<tr>
<td>2.9:</td>
<td>RIPv2 Packet Format Using MD5 Authentication</td>
<td>28</td>
</tr>
<tr>
<td>2.10:</td>
<td>RIPv2 MD5 Trailer</td>
<td>29</td>
</tr>
<tr>
<td>2.11:</td>
<td>OSPF Packet Header</td>
<td>32</td>
</tr>
<tr>
<td>3.1:</td>
<td>Research Method</td>
<td>37</td>
</tr>
<tr>
<td>3.2:</td>
<td>Ways of Studying Systems</td>
<td>41</td>
</tr>
<tr>
<td>4.1:</td>
<td>Test-bed Network Model</td>
<td>49</td>
</tr>
<tr>
<td>4.2:</td>
<td>Cisco Routers 1721 Modular Access Router</td>
<td>50</td>
</tr>
<tr>
<td>4.3:</td>
<td>Front panel of Router 1721</td>
<td>51</td>
</tr>
<tr>
<td>4.4:</td>
<td>Back panel of Router 1721</td>
<td>52</td>
</tr>
<tr>
<td>4.5:</td>
<td>WAN Serial Cable Sockets</td>
<td>58</td>
</tr>
<tr>
<td>4.6:</td>
<td>One MD5 operation</td>
<td>61</td>
</tr>
<tr>
<td>4.7:</td>
<td>MD5 Neighbor Authentication at the Originating Router</td>
<td>63</td>
</tr>
<tr>
<td>4.8:</td>
<td>The Sequence of Events at the Destination Router</td>
<td>64</td>
</tr>
<tr>
<td>4.9:</td>
<td>Client Logic</td>
<td>68</td>
</tr>
<tr>
<td>4.10:</td>
<td>Client Java program after compilation</td>
<td>69</td>
</tr>
<tr>
<td>4.11:</td>
<td>Server Logic</td>
<td>70</td>
</tr>
<tr>
<td>4.12:</td>
<td>Server Waiting for Connections</td>
<td>71</td>
</tr>
<tr>
<td>4.13:</td>
<td>Server Java program after compilation</td>
<td>71</td>
</tr>
<tr>
<td>4.14:</td>
<td>Five-Step Model Traffic Pseudo Code</td>
<td>73</td>
</tr>
<tr>
<td>4.15:</td>
<td>Model Traffic Pattern</td>
<td>74</td>
</tr>
</tbody>
</table>
4.16: Start Hyperterminal Connection
75
4.17: Start Hyperterminal Connection
75
4.18: EIGRP Configuration in Secured MD5 Authentication
77
4.19: Non-Secured EIGRP Configuration
78
4.20: RIPv2 Configuration in Secured MD5 Authentication
79
4.21: Non-Secured RIPv2 Configuration
80
4.22: OSPF Configuration in Secured MD5 Authentication
81
4.23: Non-Secured OSPF Configuration
82
5.1: Average Delay Time of Secured / No-secured EIGRP
85
5.2: Jitter of Secured / Non-secured EIGRP
86
5.3: EIGRP Overhead
86
5.4: Average Delay Time of Secured / Non-secured RIPv2
87
5.5: Jitter of Secured / Non-secured RIPv2
88
5.6: RIPv2 Overhead
89
5.7: Average Delay Time of Secured / Non-secured OSPF
90
5.8: Jitter of Secured / non-secured OSPF
90
5.9: OSPF Overhead
91
5.10: Average Delay Time in Non-secured mode
93
5.11: Average Delay Time in Secured MD5 Authentication
93
5.12: Jitter in Unsecured Mode
94
5.13: Jitter in Secured MD5 Authentication Mode
95
5.14: Overhead of EIGRP, RIPv2, OSPF Routing Protocols
96
List of Abbreviations

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>TCP</td>
<td>Transfer Control Protocol</td>
</tr>
<tr>
<td>MPP</td>
<td>Markov Poisson Process</td>
</tr>
<tr>
<td>HMM</td>
<td>Hidden Markov Model</td>
</tr>
<tr>
<td>DCE</td>
<td>Data Communication Equipment</td>
</tr>
<tr>
<td>DTE</td>
<td>Data Terminal Equipment</td>
</tr>
<tr>
<td>IGRP</td>
<td>Interior Gateways Routing Protocol</td>
</tr>
<tr>
<td>EIGRP</td>
<td>Enhanced Interior Gateways Routing Protocol</td>
</tr>
<tr>
<td>RIP</td>
<td>Routing Information Protocol</td>
</tr>
<tr>
<td>RIPv2</td>
<td>Routing Information Protocol version 2</td>
</tr>
<tr>
<td>OSPF</td>
<td>Open Shortest Pass First</td>
</tr>
<tr>
<td>MD5</td>
<td>Message Digest 5</td>
</tr>
<tr>
<td>IPX</td>
<td>Internet Packet eXchange</td>
</tr>
<tr>
<td>IP</td>
<td>Internet Protocol</td>
</tr>
<tr>
<td>NLSP</td>
<td>NetWare Link State Protocol</td>
</tr>
<tr>
<td>LSA</td>
<td>Link State Advertisement</td>
</tr>
<tr>
<td>OSI</td>
<td>Open Systems Interconnection</td>
</tr>
<tr>
<td>AS</td>
<td>Autonomous System</td>
</tr>
<tr>
<td>DV</td>
<td>Distance Vector</td>
</tr>
<tr>
<td>LS</td>
<td>Link State routing protocols</td>
</tr>
<tr>
<td>VLSM</td>
<td>Variable Length Subnet Masks</td>
</tr>
<tr>
<td>IGP</td>
<td>Interior Gateway Protocol</td>
</tr>
<tr>
<td>EGP</td>
<td>Exterior Gateway Protocol</td>
</tr>
<tr>
<td>UDP</td>
<td>User Datagram Protocol</td>
</tr>
<tr>
<td>CIDR</td>
<td>Classless Inter-Domain Routing</td>
</tr>
<tr>
<td>IS-IS</td>
<td>Intermediate System - Intermediate System</td>
</tr>
<tr>
<td>BGP</td>
<td>Border Gateway Protocol</td>
</tr>
<tr>
<td>LED</td>
<td>Led Emitting Diode</td>
</tr>
<tr>
<td>LAN</td>
<td>Local Area Network</td>
</tr>
<tr>
<td>WAN</td>
<td>Wide Area Network</td>
</tr>
<tr>
<td>Acronym</td>
<td>Description</td>
</tr>
<tr>
<td>---------</td>
<td>------------------------------------</td>
</tr>
<tr>
<td>QoS</td>
<td>Quality of Service</td>
</tr>
<tr>
<td>VPN</td>
<td>Virtual Private Networks</td>
</tr>
<tr>
<td>DSU/CSU</td>
<td>Channel Service Unit/Data Service Unit</td>
</tr>
<tr>
<td>SNMP</td>
<td>Simple Network Management Protocol</td>
</tr>
<tr>
<td>NLSP</td>
<td>NetWare Link Services Protocol</td>
</tr>
<tr>
<td>RSVP</td>
<td>Resource Reservation Protocol</td>
</tr>
<tr>
<td>UTP</td>
<td>Unshielded Twisted-Pair</td>
</tr>
<tr>
<td>STP</td>
<td>Shielded Twisted-Pair</td>
</tr>
<tr>
<td>WIC</td>
<td>WAN Interface Card</td>
</tr>
<tr>
<td>DUAL</td>
<td>Diffusing Update Algorithm</td>
</tr>
<tr>
<td>CPU</td>
<td>Central Processing Unit</td>
</tr>
<tr>
<td>BSize</td>
<td>Bulk Size</td>
</tr>
<tr>
<td>FP</td>
<td>First Packet</td>
</tr>
<tr>
<td>SP</td>
<td>Step Packet</td>
</tr>
<tr>
<td>MP</td>
<td>Maximum packet</td>
</tr>
<tr>
<td>S-RIP</td>
<td>Secured-Routing Information Protocol</td>
</tr>
</tbody>
</table>
List of publications


Table of Contents

PERMISSIONE TO USE ii
ABSTRACT (ENGLISH) iii
ACKNOWLEDGMENTS iv
LIST OF TABLES v
LIST OF FIGURES vi
ABBREVIATIONS vii
LIST OF PUBLICATIONS x

Chapter 1
1. Introduction
  1.1 Overview 1
  1.2 Problem Statement 2
  1.3 Research Objective 4
  1.4 Research Scope 4
  1.5 Thesis outline 5

Chapter 2
2. Literature Review
  2.1 Introduction 7
  2.2 Routing Protocols 9
    2.2.1 Interior Gateways Routing Protocol (IGRP) 10
    2.2.2 Enhanced Interior Gateways Routing Protocol (EIGRP) 12
    2.2.3 Routing Information Protocol (RIP) 15
    2.2.4 Open Shortest Path First (OSPF) 18
    2.2.5 Comparison of Routing Protocols 22
  2.3 Routing Protocol Authentication 22
    2.3.1 Plaintext Authentication 23
    2.3.2 MD5 Authentication 24
  2.4 MD5 Authentication for EIGRP 26
  2.5 MD5 Authentication for RIPv2 28
2.6 MD5 Authentication for OSPF
2.7 Research Works on Routing Authentication
2.8 Conclusion

Chapter 3
3. Research Methodology
3.1 Introduction
3.2 Identifying Research Problem
3.3 Designing the Experimental Model
3.4 Selecting Evaluation Technique
3.5 Modeling Arrival Process
3.6 Measuring System Performance
3.7 Conclusion

Chapter 4
4. Test-bed Network Model Details
4.1 Introduction
4.2 Test-Bed Network Model (Cisco Routers)
   4.2.1 Cisco Routers 1721 Modular Access Router
   4.2.2 Cisco Router 1721 Key Feature
   4.2.3 Front Panel LED's
   4.2.4 Back Panel Ports and LED's
   4.2.5 Physical Interfaces
   4.2.6 LAN Adapter
   4.2.7 WAN Adapters
4.3 Network Transmission Media
   4.3.1 Ethernet Cable
   4.3.2 Ethernet Network Cabling Guidelines
   4.3.3 DCE/DTE DB60 Cable
   4.3.4 Console Cable and Adapter
4.4 The Test-Bed Network Model

XII
4.4.1 Message-Digest 5 (MD5) Authentication  60
4.4.2 MD5 Algorithm  60
4.4.3 MD5 Applications  61
4.4.4 MD5 hashes  62
4.4.5 End – to – End, Client / Server  64
4.4.6 The Client/Server Simulation  65
4.4.7 The Client Side  67
4.4.8 The Server Side  69
4.4.9 Model Traffic Pseudo Code  72
4.4.10 Traffic Pattern Model  74
4.4.11 Routing Protocols Configurations  75
4.5 Conclusion  82

Chapter 5

5. Results and Discussion

5.1 Introduction  84
5.2 Enhanced Interior Gateway Routing Protocol (EIGRP)  84
   5.2.1 Average Delay Time of EIGRP in both Secured/Unsecured  85
   5.2.2 Jitter of EIGRP in both Secured/Unsecured  85
   5.2.3 Overhead of EIGRP  86
5.3 Routing Information Protocol version 2 (RIPv2)  87
   5.3.1 Average Delay Time of RIPv2 in both Secured & Unsecured  87
   5.3.2 Jitter of RIPv2 in both Secured/Unsecured  88
   5.3.3 Overhead of RIPv2  88
5.4 Open Shortest Path First (OSPF)  89
   5.4.1 Average Delay Time of OSPF in both Secured & Unsecured  89
   5.4.2 Jitter of OSPF in both Secured/Unsecured  90
   5.4.3 Overhead of OSPF  91
5.5 Total Analysis  92
   5.5.1 Unsecured Average Delay Time  92
   5.5.2 Secured MD5 Average Delay Time  93
5.5.3 Unsecured of Jitter  
5.5.4 Secured MD5 Jitter  
5.5.5 Overhead of EIGRP, RIPv2 and OSPF  
5.6 Conclusions

Chapter 6  
6. Research Conclusions  
6.1 Conclusions  
6.2 Additional remarks  
6.3 Future work

REFERENCES
Chapter 1

Introduction

1.1 Overview

The past few years have witnessed an ever-growing reliance on computer networks for business transactions where routing plays an extensive role in these network communications. Routing is then an essential part in keeping networking infrastructures running. It is the method by which a router decides where to send a datagram. Routers are devices that direct traffic between hosts by collecting information about all the paths between a source and a destination. Based on this information, a router builds a routing table. A router may be able to send the datagram directly to the destination, if it is on one of the networks that are directly connected to the router. However, the interesting case is when the destination is not reachable directly. In this case, the router attempts to send the datagram to another router which is nearer to the destination. Thus, the goal of a routing protocol is to supply the information needed to do routing. [1], [3].

As our economy and massive infrastructure increasingly rely on the Internet, such routing protocols become of critical importance. Routing protocols, however, are difficult to efficiently secure; since an attacker attempt to inject forged routing messages into the system or may modify legitimate routing messages sent by other sources. Routing protocols are, thus, subject to threats and attacks that can harm individual users or the network operations as a whole. For instance, an attacker may attack messages that carry control information in a routing protocol to break a routers' neighboring relationship. This type of attack can impact the network routing behavior in the affected routers and likely the surrounding neighborhood as well. An attacker may also attack messages that carry data information in order to break a database exchange between two routers or to affect the database maintenance functionality where the information in the database must be authentic and authorized. Attackers can also send forged protocol packets to a router with the intent of changing or corrupting the contents of its routing table or other databases, which in turn could degrade the functionality of the router. [2], [4], [5].
The contents of the thesis is for internal user only
References


[38] Ronald L. Rivest, Massachusetts Institute of Technology, MD5 Message-Digest Algorithm, RFC 1321, MIT Laboratory for Computer Science, April 1992 accessed 20/1/2008


[63] www.karjasoft.com/files/clocksinc/ClockSync1.0.0.exe, last visit 22/4/09.