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)**

telah 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 lisan 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	Tandatangan: *(Signature)*
Pemeriksa Luar *(External Examiner)*	:	Prof. Madya Dr. Hj. Mazani Hj. Manaf	Tandatangan: *(Signature)*
Pemeriksa Dalaman *(Internal Examiner)*	:	Encik Fazli Azzali	Tandatangan: *(Signature)*
Penyelia Utama *(Principal Supervisor)*	:	Prof. Madya Hatim Mohamed Tahir	Tandatangan: *(Signature)*
Setiausaha Panel *(Panel Secretariat)*	:	Dr. Mohd Syazwan Abdullah	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 UUm 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. Suhaidi 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:

Thesis list of figures

List of Abbreviations

TCP	Transfer Control Protocol
MPP	Markov Poisson Process
HMM	Hidden Markov Model
DCE	Data Communication Equipment
DTE	Data Terminal Equipment
IGRP	Interior Gateways Routing Protocol
EIGRP	Enhanced Interior Gateways Routing Protocol
RIP	Routing Information Protocol.
RIPv2	Routing Information Protocol version 2
OSPF	Open Shortest Pass First
MD5	Message Digest 5
IPX	Internetwork Packet eXchange
IP	Internet Protocol
NLSP	NetWare Link State Protocol
LSA	Link State Advertisement
OSI	Open Systems Interconnection
AS	Autonomous System
DV	Distance Vector
LS	Link State routing protocols
VLSM	Variable Length Subnet Masks
IGP	Interior Gateway Protocol
EGP	Exterior Gateway Protocol
UDP	User Datagram Protocol
CIDR	Classless Inter-Domain Routing
IS-IS	Intermediate System - Intermediate System
BGP	Border Gateway Protocol.
LED	Led Emitting Diode
LAN	Local Area Network
WAN	Wide Area Network

QoS	Quality of Service
VPN	Virtual Private Networks
DSU/CSU	Channel Service Unit/Data Service Unit
SNMP	Simple Network Management Protocol
NLSP	NetWare Link Services Protocol
RSVP	Resource Reservation Protocol
UTP	Unshielded Twisted-Pair
STP	Shielded Twisted-Pair
WIC	WAN Interface Card
DUAL	Diffusing Update Algorithm
CPU	Central Processing Unit
BSize	Bulk Size
FP	First Packet
SP	Step Packet
MP	Maximum packet
S-RIP	Scured-Routing Information Protocol.

List of publications

1. *Khalid Abu Al-Saud, Hatim Mohd Tahir, Adel Elzoghabi, Mohammad Saleh,* Performance Evaluation of Secured versus Non-Secured EIGRP Routing Protocol, in Proceedings of the 2008 **International Conference on Security & Management, SAM 2008,** Las Vegas, Nevada, USA, July 14-17, 2008. CSREA Press 2008, ISBN 1-60132-085-X.

2. *Khalid Abu Al-Saud, Hatim Mohd Tahir, Moutaz Saleh and Mohammad Saleh,* Impact of MD5 Authentication on Routing Traffic for the Case of: EIGRP, RIPv2 & OSPF, In **the Journal of Computer Sciences (JCS) 2008**, 244, 5th Avenue, Number S-207, New York, NY 10001, USA, Vol. 4(9): 721-728,.

3. *Khalid Abu Al-Saud, Hatim Mohd Tahir, Moutaz Saleh and Mohammad Saleh*, A Performance Comparison of MD5 Authenticated Routing Traffic with EIGRP, RIPv2 & OSPF, submitted in The **International Arab Journal of Information Technology (IAJIT),** accepted in January 2009 and will be publish in early 2010.

Table of Contents

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

[1] *Jeff Doyle, Jennifer DeHaven Carroll*, Routing TCP/IP, Volume II (CCIE Professional Development), Publisher: Cisco Press, Pub Date: April 11, 2001, ISBN: 1-57870-089-2.

[2] *Sackett, George,* Cisco Router Handbook. Blacklick, OH, USA, 1999.

[3] *Scott M. Ballew, 1997.* Managing IP Networks with Cisco Routers. 1st Edn., O'Reilly Media, Inc., Lawrence, MA, United States, pp: 352. ISBN: 1565923200.

[4] *Ravi Malhotra*, IP Routing, O'Reilly Online Catalog, O'Reilly & Associates Inc. *January 2002* accessed 4/3/2009

[5] *Merike Kaeo,* Designing Network Security Second Edition, Publisher: Cisco Press, Pub Date: October 30, 2003, ISBN: 1-58705-117-6

[6] *V. Anand and K. Chakrabarty,* Cisco IP Routing Protocols: Troubleshooting Techniques, Charles River Media 2004 - ISBN: 1584503416.

[7] *Gert De Laet, Gert Schauwers*, Network Security Fundamentals, Publisher Cisco Press, September 08, 2004 ISBN: 1-58705-167-2.

[8] *Wendell Odom,* CCNA INTRO Exam Certification Guide, Copyright© 2004 Cisco Systems, Inc., Published by: Cisco Press ISBN: 1-58720-094-5

[9] *Wendell Odom,* CCNA ICND Exam Certification Guide, Copyright© 2004 Cisco Systems, Inc. Published by: Cisco Press ISBN: 1-58720-083-x

[10] *Sam Halabi and Danny McPherson,* Internet Routing Architectures, Second Edition August 23, 2000 Publisher: Cisco Press, ISBN: 1-57870-233-X.

[11] *Jeff Doyle, Jennifer Carroll, Publisher,* CCIE Professional Development Routing TCP/IP, Volume I, Second Edition, Cisco Press, Pub Date: October 19, 2005; ISBN: 1-58705-202-4

[12] *Ivan Pepelnjak*, EIGRP-Network-Design-Solutions, Publisher: Cisco Press, Pub. Date: Jan 15, 2000.

[13] *Fung, K. T. (Kwok T.),* Network Security Technologies, Second Edition, Date: 2004, ISBN 0-8493-3027-0.

[14] *Merike Kaeo,* Designing Network Security Second Edition, Publisher: Cisco Press, Pub Date: October 30, 2003, ISBN: 1-58705-117-6

[15] http://www.cisco.com/en/US/docs/ios/12_0/np1/configuration/guide/1crip.html accessed 22/4/2009.

[16] http://www.oreilly.com/catalog/iprouting/chapter/ch04.html accessed 22/4/2009

[17] http://www2.rad.com/networks/1995/ospf/ospf.htm accessed 22/4/2009

[18] *B. Albrightson and J.J. Garcia-Luna-Aceves and J. Boyle*, EIGRP – A fast routing protocol based on distance-vectors, in: *Proceeding of Networld/Interop '94*, Las Vegas, NV, May 1994. accessed 11/1/2009

[19] *Talal M. Jaafar, George F. Riley, Dheeraj Reddy and Dana Blair*, SIMULATION-BASED ROUTING PROTOCOL PERFORMANCE ANALYSIS – A CASE STUDY, in the Proceedings of the 2006 Winter Simulation Conference 2006 IEEE 1-4244-0501-7/06, USA. Accessed 11/11/08

[20] *Ivan Pepelnjak 2000*, EIGRP network design solutions, Cisco Press ISBN 1578701651, Release Date 15 January 2000.

[21] *Mohamed G. Gouda, and Marco Schneider,* Maximizable Routing Metrics, in the proceeding of IEEE/ACM TRANSACTIONS ON NETWORKING, VOL. 11, NO. 4, AUGUST 2003 663. accessed 10/4/2009.

[22] *Nigel Houlden, Vic Grout, John McGinn and John Davies*, Extended End-to-End Cost Metrics for Improved, Dynamic Route Calculation, Proceedings of the 6th International Network Conference (INC 2006), University of Plymouth, 11-14 July 2006, pp89-96. accessed 10/3/2009.

[23] *Franck Le, Geoffrey G. Xie, Dan Pei, JiaWang and Hui Zhang,* Shedding Light on the Glue Logic of the Internet Routing Architecture, *in proceeding of SIGCOMM'08, August 17–22, 2008, Seattle, Washington, USA.* accessed 10/3/2009

[24] *Gary Scott Malkin,* RIP Version 2 Carrying Additional Information, Xylogics, Inc., November 1994 - RFC1723.

[25] *Tao Wan Evangelos Kranakis P.C. van Oorschot,* "S-RIP: A Secure Distance Vector Routing Protocol," *in the Proceedings of Applied Cryptography and Network Security (academic track)*, Yellow Mountain, China. June 8-11 2004. accessed 10/3/2009

[26] *Dan Pei, Dan Massey and Lixia Zhang*, "Detection of Invalid Routing Announcements in RIP Protocol," published *in GLOBECOM IEEE*, volume 3, Dec 2003. accessed 10/3/2009

[27] *Dan Pei and Lixia Zhang, Dan Massey*, "A Framework for Resilient Internet Routing Protocols," *IEEE Network*, March/April 2004. accessed 10/2/2009

[28] *Abdelaziz Babakhouya, Yacine Challal, Abdelmadjid Bouabdallah, SaYd Gharout*, "S-DV: A new approach to Secure Distance Vector routing protocols",. 10.1109/SECCOMW, Aug. 28 -Sept. 1, 2006, Baltimore, MD, ISBN: 1-4244-0423-1, IEEE 2006. accessed 10/3/2009

[29] *David A. Maltz, Geoffrey Xie, Jibin Zhan, Hui Zhang, G´ısli Hj ´almt´ysson, Albert Greenberg,* Routing Design in Operational Networks: A Look from the Inside, in proceeding of SIGCOMM'04, August 30–Sept. 3, 2004, Portland, Oregon, USA. accessed 15/3/2009

[30] *David Bauer, Murat Yuksel, Christopher Carothers and Shivkumar Kalyanaraman,* A Case Study in Understanding OSPF and BGP Interactions Using Efficient Experiment Design, in the Proceedings of the 20th Workshop on Principles of Advanced and Distributed Simulation (PADS'06) 2006 IEEE. accessed 10/1/2009

[31] *Bae, Sang; Henderson, Thomas R.,* Traffic Engineering with OSPF Multi-Topology Routing, in the proceedings of Military Communications Conference, 2007, MILCOM, IEEE 29-31 Oct. 2007 Page(s):1 - 7. accessed 10/2/2009

[32] *George F. Riley, Dheeraj Reddy*, Simulating Realistic Packet Routing Without Routing Protocols, in the Proceedings of the Workshop on Principles of Advanced and Distributed Simulation (PADS'05) 1087-4097/05, IEEE 2005. accessed 10/3/2009

[33] *Ching-Chuan Chiang, Chinyi. Chen, Dah-Lih Jeng, Shuenn-Jyi Wang, and Ying-Kwei Ho*, The Performance and Security Evaluations of Internet Routing Protocols, published in Journal of Informatics & Electronics, Vol.2, No.2, pp.21-27, March 2008. accessed 10/3/2009

[34] *F. Baker and R. Atkinson*, January 1997. RIP-2: MD5 Authentication. IETF RFC2082, Cisco Systems, United States, no of Pages 12. http://portal.acm.org/citation.cfm?id=RFC2082 accessed 10/3/2008

[35] *John Moy,* OSPF Version 2, Ascend Communications, Inc. Network Working Group, April 1998. RFC 2328. accessed 10/5/2008

[36] *Fred Baker,* DRAFT OSPF MD5 Authentication, Advanced Computer Communications, September October 1994, draft-ietf-ospf-md5-01.txt. accessed 10/4/2008

[37] *Emanuele Jones and Olivier Le Moigne,* OSPF Security Vulnerabilities Analysis, Alcatel Company Canada, Network Working Group, June 16, 2006. (draft-jones-ospf-vuln-02.txt). accessed 10/1/2008

[38] *Ronald L. Rivest*, Massachusetts Institute of Technology, MD5 Message-Digest Algorithm, *RFC 3121*, MIT Laboratory for Computer Science, April 1992 accessed 20/1/2008

[39] *R. Rivest.* The MD5 Message-Digest Algorithm, *IETF RFC 1321, MIT Laboratory for Computer Science and RSA Data Security Inc., April 1992. http://portal.acm.org/citation.cfm?id=RFC1321* accessed 15/3/2008

[40] *Khalid Abu Al-Saud, Hatim Mohd Tahir, Adel Elzoghabi, Mohammad Saleh,* Performance Evaluation of Secured versus Non-Secured EIGRP Routing Protocol, Proceeding of WORLDCOMP '08, Las Vegas, NV, July 14-17, 2008.

[41] *Khalid Abu Al-Saud, Hatim Mohd Tahir, Moutaz Saleh and Mohammad Saleh,* Impact of MD5 Authentication on Routing Traffic for the Case of: EIGRP, RIPv2 & OSPF, Proceeding in Journal of Computer Science, 244, 5th Avenue, Number S-207, New York, NY 10001, November 2008.

[42] *Ramaswamy Chandramouli, Tim Grance, Rick Kuhn, Susan Landau,* Toward Secure Routing Infrastructures, Proceedings of the IEEE SECURITY & PRIVACY 2006, pages 84-78, accessed 25/1/2008.

[43] *Bradly R. Smith and J.J. Garcia-Luna*, "Securing the Border Gateway Routing Protocol," Proceedings of the ISOC Symposium on Network and Distributed System Security '97, February 11, 1997. accessed 25/2/2008.

[44] *C.-T. Huang E. N. Elnozahy M. G. Gouda,* Hop Integrity and the Security of Routing Protocols, 2002, accessed 10/12/2007.

[45] *Deepakumara, J. H.M. Heys and R. Venkatesan.* FPGA implementation of MD5 hash algorithm. In the Proceedings of IEEE Canadian Conference on Electrical and Computer Engineering CCECE, May 13-16, 2001, Toronto, Ontario, Canada, pp: 919-924. accessed 15/3/2008

[46] *Dijiang Huang, Amit Sinha and Deep Medhi, 2003.* A double authentication scheme to detect impersonation attack in link state routing protocols. In the Proceedings of IEEE International Conference on Communications (ICC), pages 1723-1727, Vol. 3, May 11-15, Anchorage, Alaska 2003. accessed 10/3/2007.

[47] *F. Baker and R. Atkinson, October 1994.* OSPF MD5 Authentication, draft-ietf-ospf-md5-02.txt, Naval Research Laboratory, no Pages 11. accessed 18/2/2008.

[48] http://en.wikipedia.org/wiki/MD5 last visit 22/4/09

[49] *C. Demichelis and P. Chimento*, RFC: 3393, November 2002, IP Packet Delay Variation Metric for IP Performance Metrics (IPPM). accessed 15/3/2008

[50] *Schmitd, J.W., and Taylor, R.E. 1970. Simulation and Analysis of Industrial Systems*. Homewood, Illinois.

[51] *Averill, M.L. and Kelton, W.D. 2000. Simulation Modeling and Analysis*. Mc Graw Hill.

[52] *Jain, R. 2000.* The Art of Computer Systems Performance Analysis: Techniques for Experimental Design, Measurements, Simulation and Modeling. John Wiley, NewYork.

[53] http://www.cisco.com/en/US/products/hw/routers/ps221/index.html acc. 22/4/09

[54] Cisco-1721-1720datasheet.pdf, accessed 12/12/2007.

[55] http://www.cisco.com/univercd/cc/td/doc/product/lan/c3550/1216ea1/3550hig/35cable.htm last visit 22/4/2009

[56] *Kwok T. Fung*, Network Security Technologies, CRC Press, 2nd Edition, 2005.

[57] *Merike Kseo,* Designing Network Security, second edition, Cisco Press, October 30, 2003.

[58] *Kevin J. Healy, Richard A. Kilgore*, A JAVA-BASED PROCESS SIMULATION LANGUAGE, Proceeding of the 1997 Winter Simulation Conference, ed. S. Andradottir, K. J. Healy, D. H. Withers, and B. L. Nelson, accessed 15/3/2008

[59] *R. Albrightson and J.J. Garcia-Luna-Aceves and J. Boyle*, EIGRP – A fast routing protocol based on distance-vectors, in: *Proceeding of Networld/Interop '94*, Las Vegas, NV, May 1994. accessed 10/6/2007

[60] *Reinhard Finstenvalder*, A generic client/server architecture for distributed Web-based simulation experimentation, Computer-Aided Control System Design, 2000 (CACSD2000). IEEE International Symposium on Volume, Issue, 2000 Pages: 185 – 189 Digital Object Identifier accessed 10/4/2007.

[61] *N. Honn, N. Hohn, D. Veitch, K. Papagiannaki and C. Diot, 2004.* Bridging router performance and queuing theory. In Proceeding of the ACM SIGMETRICS/Performance'04, June 12–16, 2004, New York, NY, USA, pp:

355-366. http://portal.acm.org/citation.cfm?id=1005686.1005728. accessed 10/3/2008

[62] *Imad Antonios, Lester Lipsky 2002.* A performance model of user delay in on/off heavy-tailed traffic. In the Proceedings of the 2002 International Symposium on Performance Evaluation of Computer and Telecommunication Systems (SPECTS 2002), San Diego, CA, July, 2002. accessed 15/4/2008

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