Arab Academy for Science and Technology

& Maritime Transport

College of Computing & Information Technology

Mitigating Web Service Denial of Service Attacks Using Dynamic Client Puzzle Approach

A Thesis Submitted to College of Computing & Information Technology in Partial Fulfillment of the Requirements for the award of degree of

MASTER of Science in Information Systems

Submitted By

IHAB MOHAMED ABD ELWAHAB

Supervised by

Dr. BAHAA HASAN
Chairman& CEO at
Arab Security Consultants

Prof. Dr. IBRAHIM IMAM
College of Computing &
Information Technology
AASTMT

September 2012

Cairo

الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري

Arab Academy for Science, Technology & Maritime Transport

DECLARATION

We clarify that we have read the present work and that in our opinion it is fully adequate in scope and quality as dissertation towards the partial fulfillment of the Master Degree requirements in **Specialization: information system**

College of Computing and Information Technology (AASTMT)

Date: September- 2012

Thesis Title

"Mitigating Web Service Denial of Service Attacks Using Dynamic Client Puzzle Approach"

Submitted By

Ihab Mohamed Abd Elwahab Abd Elnabi

Supervisors:

Name: **Prof. Dr. IBRAHIM IMAM**

Position: Professor of Computer Science, Arab Academy for Science, Technology

Signature:..

Supervisors:

Name: **Dr. BAHAA HASAN**

Position: computer security consultant and information –arab academy office for security consulting

Signature:.........Bahaa.......................

Examiners:

Name: **Prof. Dr. Khaled. Shehata**

Position: Professor of Computer Engineering, Arab Academy for Science, Technology

Signature:..Khaled Shehata..................

Name: **Prof. Dr. Mohamed Zaki Abdel Megid**

Position: Professor of Computer Engineering, Al-Azhar University

Signature:..

Acknowledgements

First, I thank Allah (subhana wa taala) for providing me with patience and knowledge to complete this work.

I would like to thank Dr. Bahaa Hasan, for the guidance and suggestions throughout the whole research study to help me work towards the completion of my Master.

I would like to thank and to express my deep and sincere thanks to Prof. Dr Ibrahim - Imam for their time, discussions and valuable comments.

My father & mother, thank you for all your support. You have always been a great motivation to me and taught me the meaning of working hard. You are a pillar of strength.

I would like to express my deepest gratefulness and thanks to my wife, who has been a great source of strength all through this work, and my children, Tamer, Sief El-dine and Nour El-dine. Their love and support during long days and nights of work was of value to me.

Finally, I would like to thank all people who help me with any thesis assistance, and supported me throughout the working process.

Abstract

During the past few years, denial-of-service (DoS) attacks have become more risky to deplete the computing resources or bandwidth of the potential targets. The relative ease and low costs of launching such attacks, supplemented by the current inadequate state of any viable defense mechanism, have made them one of the top threats to the Internet community today. Since, the increasing popularity of web-based applications has led to several critical services being provided over the Internet. The most common DoS attacks typically involve flooding with a huge volume of traffic and consuming network resources such as bandwidth, buffer space at the routers, CPU time and recovery cycles of the target server. We have proposed a mechanism for protecting a web-server against a denial of service (DoS) attacks. We investigated the effectiveness of defending web services from DoS attacks using client puzzles, a cryptographic countermeasure, which provides a form of gradual authentication by requiring the client to solve some computationally difficult problems before access is granted. So, the first aim of this thesis is to adjust the mechanism of our client puzzle to dynamically change the puzzle difficulty. Furthermore, we established a web service with client puzzle to test the performance of the client puzzle in web service.

Table of Contents

List of Tables

Table of Figures

Nomenclatures

Symbols	**Nomenclatures**
DoS	Denial of service
DDoS	Distributed Denial of Service
HTTP	Hypertext Transfer Protocol
CPU	Central Processing Unit
TCP	Transmission Control Protocol
UDP	User Datagram Protocol
DNS	Domain Name System
ARP	Address Resolution Protocol
ICMP	Internet Control Message Protocol
WSDL	Web Service Description Language
SOAP	Simple Object Access Protocol
WCF	Windows Communication Foundation
API	Application Programming Interface
XML	Extensible Markup Language
HTTPS	Hypertext Transfer Protocol Secure
DCP	Dynamic Client Puzzle Difficulty

Bibliography

[1] S Surisetty, S Kumar ," Apple's Leopard Versus Microsoft's Windows XP: Experimental Evaluation of Apple's Leopard Operating System with Windows XP-SP2 under Distributed Denial of Service Security Attacks", Information Security Journal: A Global Perspective , Volume 20, Issue 3, 26 May 2011, pages 163–172

[2] Elizabeth Montalbano ,"Facebook confirms DOS attack same day as twitter" http://www.pcworld.com /article/169775/article.html, August 2009 .

[3] Factsheet: Root server attack , http://www.icann.org/en/announcements/factsheet-dns-attack-08mar07.pdf, February 2007.

[4] Peter Grabosky, "Requirements of prosecution services to deal with cyber crime ",Crime, Law And Social Change ,Volume 47, Numbers 4-5 , 2007, pages 201-223

[5] E. Skoudis. Counter Hack " A Step-by-Step Guide to Computer Attacks and Effective Defenses" Prentice Hall, Upper Saddle River, NJ, 2002.

[6] Johnny Ryan ,"A History of the Internet and the Digital Future" , Reaktion Books United Kingdom , First published,2010,Page 24 .

[7] M. Muthuprasanna , G. Manimaran, Zhengdao Wang, Suraj Kothari "A composable approach to design of newer techniques for large-scale denial-of-service attack attribution "Technical Report, lowa State University, USA, 2011 .

[8] Michael Calce , Craig Silverman "Mafiaboy: A Portrait of the Hacker as a Young Man" Lyons Press, August 2, 2011 .

[9] U Tariq, Y Malik, B Abdulrazak ," Defense and Monitoring Model for Distributed Denial of Service Attacks" , Procedia Computer Science, Volume 10, December ,2012, Pages 1052–1056 .

[10] Kline, E , " Shield: DoS filtering using traffic deflecting" ,Network Protocols (ICNP), 2011 19th IEEE International Conference ,17-20 Oct. 2011, Page(s): 37 - 42 .

[11] Rich Miller, "Outages for RIAA and SCO sites", http: // news. netcraft. Com/ archives/ 2004/ 02/28/ outages_for_ riaa_sco_sites.html , 28th February ,2004 .

[12] Steve Mansfield-Devine ," DDoS: threats and mitigation" , Network Security

Volume, Issue 12, December, 2011, Pages 5–12.

[13] Karson K. Thompson , "Note: Not Like an Egyptian: Cyber security and the Internet Kill Switch Debate* " ,Texas Law Review Association , December, 2011

[14] Nicolas Falliere, Liam O Murchu, and Eric Chien ," W32.Stuxnet Dossier" Symantec security response Version 1.4 ,February,2011 .

[15] C Decker - S. Cal. L. "Cyber Crime 2.0: An Argument To Update The United States Criminal Code To Reflect The Changing Nature Of Cyber Crime ", Southern California Law Review Vol. 81, 2007, Pages 959-1016 .

[16] Charalampos Patrikakis, Michalis Masikos, and Olga Zouraraki "Distributed Denial of Service" http://www.cisco.com/web/about/ c123/ac147/archived_issues/ipj_7-/dos_attacks.html Attack , The Internet Protocol Journal - Volume 7, Number 4 , December 2004 .

[17] Bryan Parno, Dan Wendlandt, Elaine Shi, Adrian Perrig, Bruce Maggs, and Yih-Chun Hu. Portcullis: Protecting connection setup from denial-of-capability attacks. In Proceedings of the ACM SIGCOMM, August 2007

[18] S. Ranjan, R. Swaminathan, M. Uysal, and E. Knightly. Ddos-resilient scheduling to counter application layer attacks under imperfect detection. In Proceedings of the IEEE Infocom, Barcelona, Spain, April 2006. IEEE.

[19] Sherif Khattab, Sameh Gobriel, Rami Melhem, Daniel Moss´e "Live Baiting for Service-Level DoS Attackers" INFOCOM 2008. The 27th Conference on Computer Communications. IEEE , 13-18 April , 2008,

[20] CERT/CC "CERT. MS-SQL Server Worm, Advisory CA-2003-04", http://www.cert.org/advisories/CA-2003-04.html, January 2003.

[21] Timothy John McNevin "Mitigating Network-Based Denial-of-Service Attacks with Client Puzzles" April, 2005

[22] X. Wang and M. K. Reiter. "Mitigating Bandwidth-Exhaustion Attacks using Congestion Puzzles (Extended Abstract)," in Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS '04). October 25-29, 2004, pp. 257–267.

[23] ZHANG FU ,"Mitigating Distributed Denial-of-Service Attacks: Application-defense and Network-defense Methods" THESIS FOR THE DEGREE OF LICENTIATE OF ENGINEERING, May, 2010 ,pages 6-8 .

[24] X. Liu, X. Yang, and Y. Lu. "To filter or to authorize: network-layer DoS defense against multimillion-node botnets". In SIGCOMM '08: Proceedings of the ACM SIGCOMM 2008 conference on Data communication, USA, 2008, pages 195–206.

[25] B.Waters, J. A. Halderman, A. Juels, and E. W. Felten. "New Client Puzzle Outsourcing Techniques for DoS Resistance," in Proceedings of the 11th ACM Conference on Computer and Communications Security (CCS'04). October 25-29, 2004, Pages 246–256.

[26] D. Dean a28nd A. Stubblefield. "Using Client Puzzles to Protect TLS," in Proceedings of the 10th USENIX Security Symposium, August 13-17, 2001

[27]A. Juels and J. Brainard. "Client Puzzles: A cryptographic defense against connection depletion attacks," in Proceedings of Networks and Distributed Systems Security (NDSS '99), February 3-5, 1999, pp. 151-165.

[28] A. Back , "Hashcash – A Denial of Service Counter-Measure," Available at: http://www.hashcash.org/papers/hashcash.pdf , August 2002 .

[29] Gal Badishi, Amir Herzberg, Idit Keidar ," Keeping Denial-of-Service Attackers in the Dark", IEEE Trans. Dependable Sec. Comput. , Volume 4, Number 3, July-September 2007 , Pages 191-204

[30] Suriadi Suriadi, Douglas Stebila, "Defending web Services Against Denial of S

[31] T. Aura, P. Nikander, and J. Leiwo. "DoS-resistant authentication with client puzzles". In Security Protocols Workshop 2000,.Cambridge, Apr 2000, pages 170 – 181.

[32] OASIS. Uddi 101. http://uddi.xml.org/uddi-101, 8 2006.

[33] Allen Brown Hugo Haas. web services glossary .http://www.w3.org/TR/ws-gloss/, February 2004 .

[34] Phillip A. Laplante, Seppo J. Ovaska "Real-Time Systems Design and Analysis: Tools for the Practitioner ", Wiley-IEEE Press, 4 Edition, 2011, page 11.

الملخص

خلال السنوات القليلة الماضية، أصبحت حجب الخدمة (DoS) من الهجمات الخطرة في استنزاف موارد الحوسبة أو سعة النطاق الترددي للشبكات من الاهداف المحتملة و نظرا للسهولة النسبية والتكاليف المنخفضة لشن هجمات من هذا القبيل، وعدم كفاية و تناسب آلية الدفاع الحالية مما يجعلها واحدة من أعلى التهديدات لمجتمع الإنترنت اليوم. منذ ذلك الحين، وقد أدى ازدياد شعبية الطلب على بعض التطبيقات المستندة إلى الخدمات الحرجة التي يجري تقديمها عبر الإنترنت واصبحت هجمات حجب الخدمة هى الأكثر شيوعا وعادة ما تشمل سيل من الهجمات لتدفق بيانات وهمية واستهلاك موارد الشبكة مثل مساحة سعة النطاق الترددي و أجهزة التوجيه، ووقت وحدات المعالجة المركزية ونظم استرجاع الخوادم المستهدفة . لذلك اقترحنا آلية لحماية خادم شبكة الويب ضد االحجب من هجوم الخدمة (DOS) وتحققا لفعالية الدفاع عن خدمات ويب من هجمات حجب الخدمة وذلك باستخدام الغاز العميل، والتشفير المضاد الذي يوفر شكلا من أشكال التحقق التدريجي عن طريق الاشتراط على العميل حل بعض المشاكل الصعبة حسابيا قبل منحه الوصول للخدمة . لذلك، فإن الهدف الأول من هذه الأطروحة هو لضبط آلية لغز العميل لتغيير صعوبة اللغز دينامكيا . وعلاوة على ذلك،تم إنشاء خدمة الويب مع لغز العميل لاختبار أداء لغز عميل في خدمة االويب.

الأكاديمية العربية للعلوم والتكنولوجيا والنقل البحري
Arab Academy for Science, Technology & Maritime Transport

قرار لجنة التحكيم والمناقشة

لمناقشة و تقييم رسالة الماجستير المقدمة من الباحث / **ايهاب محمد عبد الوهاب**

بعنوان

" معالجة خدمات الويب من هجوم منع الخدمة باستخدام منهجية ألغاز العميل الديناميكية"

Mitigating Web Service Denial of Service Attacks Using Dynamic Client Puzzle Approach

تم مناقشة هذه الرسالة وإجازها بتاريخ ١١/ ٩/ ٢٠١٢ م.

أعضاء اللجنة

الأساتذة المشرفون على الرسالة :

أ.د. ابراهيم امام **التوقيع (** ابراهيم **)**
استاذ علوم الحاسب – الأكاديمية العربية للعلوم والتكنولوجيا - **مشرف**

د. بهاء حسن **التوقيع (** **)**
استشارى أمن الحاسبات و المعلومات بالمكتب العربى للاستشارات الامنيه - **مشرف**

الاساتذة المحكمون:

أ.د. خالد شحاتة **التوقيع(** (Khaled Shehata
استاذ هندسة الحاسب – الأكاديمية العربية للعلوم والتكنولوجيا - **محكم**

أ.د محمد زكى عبد المجيد **التوقيع(**
استاذ هندسة الحاسب – جامعة الازهر – **محكم**

أودعت هذه الرسالة بالمكتبة بتاريخ: / /

الاكاديمية العربية للعلوم والتكنولوجيا

و النقل البحري

كلية الحاسبات و تكنولوجيا المعلومات

معالجة خدمات الويب من هجوم منع الخدمة باستخدام منهجية ألغاز العميل الديناميكية

ضمن المتطلبات اللازمة للحصول على درجة ماجستير العلوم في نظم معلومات
من كلية الحاسبات وتكنولوجيا المعلومات (القاهرة)

رسالة مقدمة من الدارس

ايهاب محمد عبد الوهاب

تحت اشراف

د /بهاء حسن
رنيس مجلس إدارة المكتب العربى
للاستشارات الهندسية والأمنية

أ.د/ابراهيم إمام
استاذ علوم الحاسب
الأكاديمية العربية للعلوم والتكنولوجيا

سبتمبر 2012

القاهرة

MITIGATING WEB SERVICE DENIAL
OF SERVICE ATTACKS USING
DYNAMIC CLIENT PUZZLE