MULTIFACTOR AUTHENTICATION FOR ENHANCED ACCESS CONTROL SECURITY FOR WEBSITES

MOHAMMED M. HASSOUN

UNIVERSITI UTARA MALAYSIA

2010

MULTIFACTOR AUTHENTICATION FOR ENHANCED ACCESS CONTROL SECURITY FOR WEBSITES

A project submitted to Dean of Postgraduate Studies and Research in partial fulfillment of the requirement for the degree

Master of Science of Information Technology

Universiti Utara Malaysia

By

Mohammed M. Hassoun

KOLEJ SASTERA DAN SAINS
(College of Arts and Sciences)
Universiti Utara Malaysia

PERAKUAN KERJA KERTAS PROJEK
(Certificate of Project Paper)

Saya, yang bertandatangan, memperakukan bahawa
(I, the undersigned, certify that)

MOHAMMED M. HASSOUN
(801600)

calon untuk Ijazah
(candidate for the degree of) **MSc. (Information Technology)**

telah mengemukakan kertas projek yang bertajuk
(has presented his/her project paper of the following title)

MULTIFACTOR AUTHENTICATION FOR ENHANCED ACCESS CONTROL SECURITY FOR WEBSITES

seperti yang tercatat di muka surat tajuk dan kulit kertas projek
(as it appears on the title page and front cover of project paper)

bahawa kertas projek tersebut boleh diterima dari segi bentuk serta kandungan dan meliputi bidang ilmu dengan memuaskan.
(that the project paper acceptable in form and content, and that a satisfactory knowledge of the field is covered by the project paper).

Nama Penyelia Utama
(Name of Main Supervisor): **DR. MOHD SYAZWAN ABDULLAH**

Tandatangan
(Signature) : _____

Dr. Mohd Syazwan Abdullah
PhD (Comp. Sci - York, UK)
Senior Lecturer
Graduate Department of Information System
Universiti Utara Malaysia

Tarikh
(Date) : 15 September 2010

DEAN OF POSTGRADUATE STUDIES AND RESEARCH
UNIVERSITI UTARA MALAYSIA

PERMISSION TO USE

In presenting this project in partial fulfillment of the requirements for a postgraduate degree from the 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 project in any manner in whole or in part, for scholarly purposes may be granted by my supervisor(s) or in their absence by the Dean of Postgraduate Studies and Research. It is understood that any copying or publication or use of this project 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 project.

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

Dean of Postgraduate Studies and Research

College of Arts and Sciences

Universiti Utara Malaysia

06010 UUM Sintok

Kedah Darul Aman

Malaysia

ABSTRACT

Nowadays, computer security becomes a major issue for users and developers. Security experts and developers are working together to bridge the security gaps by the realistic diagnosis of threats. They try to find the best ways to apply reasonable solutions in regard to cost, time, and usability. The issue of security has become one of the Common Era concerns.

Users are divided into two groups, firstly, computer users, secondly, internet users (website users). Website's users do not like to buy expensive or sophisticated devices, and they just want to access their data in the safety way possible. This research sheds light upon enhancing the access control of websites by employing mobile phone and email features to serve this purpose. The system using the ordinary username and password for user login, and the PassCode. It is generated for every login request. This PassCode has a special scenario, firstly, using email to send the encrypted PassCode to the user, secondly decrypt the PassCode before use it to login by an application installed on the user's mobile phone. Moreover, there are other features added to the system expired of password and Bluetooth device address of the mobile phone. The latter is used as identification to the user, to reach a high level of confidentiality.

ACKNOWLEDGEMENT

By the name of Allah, the Most Gracious, the Most Merciful and peace be upon his beloved Prophet Mohammad and his household (peace be up on them).

First, I would like to express my profound gratitude to Allah (God), his prophet Mohammed and his household for providing me the blessings to complete this work. Without their grace and mercy, this work would not have been come to fruition.

I would like to take this opportunity to extend my deepest gratitude to my supervisor, Doctor Mohd Syazwan bin Abdullah. He has got a sharp eye for details and superb analytical skill, these have been instrumental in the success of the research. His belief that it was, indeed, possible to finish keeping me going.

This acknowledgement would not be complete without mentioning my late father. His precious advices that he gave me still stick in my mind and push me to work harder and harder so as to reach my goal.

All thanks go to my Mother, for her love and prayers, my brothers, sisters and my wife for their support and encouragements.

Finally, never enough thanks to all my friends, colleagues and scholars who have helped me during my studies at UUM, given support and made my study easier.

Hopefully, this master's dissertation will not be the end of my journey in seeking for more knowledge to understand the meaning of life and contribute in the reconstruction of my beloved country "IRAQ".

Mohammed M. Hassoun

September 04, 2010

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF ABREVIATIONS

AOL	America Online
CSI	Crime Scene Investigation
CTI	*Computer telephony integration*
FBI	Federal Bureau of Investigation
ICL	International Computers Limited
PHP	Hypertext Preprocessor
QMUL	*Queen Mary, University of London*
RSA	Information Risk Management strategy integrates supporting capabilities in Identity Assurance, Data Security, Information & Event Management and significant additions to EMC's Global Services portfolio
SINTEF	Group is the largest independent research organisation in Scandinavia
TSB	Taranaki Savings Bank

CHAPTER ONE

INTRODUCTION

This chapter presents the background, problem statement, research questions, objectives, significance, and scope and limitation of this study.

1.1 Background

The society life increasing tends to be digitalized by using computer in real life and there are many realms integrated together to provide users with new technology. There are many issues in this regard. The most important issue of the computer realm is security issue. Organizations, researchers and developers still strive to brick the security gap in different computer systems for large and even small enterprises.

There are many studies dealt with data breaches and how it reflects to the user and the company behavior. Hilley (2007) stated that General Accounting Office (GAO) analyzed number of data breaches reported by the Privacy Rights Clearinghouse, Identity Theft Resource Center, and Attrition to get an idea of the problem scope. It is believed that 572 breaches collated by the three organizations from January 2005 to December 2006 to be an underestimation of the real number, it is estimated that the number will be over 80 million records were affected. The majority of organizations do not reveal security incidents to avoid the news media to annoy them.

The contents of the thesis is for internal user only

REFERENCES

Anderson, R. (2001). Why Information Security is Hard-An Economic Perspective. *Proceedings of the 17th Annual Computer Security Applications Conference held on 10-14 December 2010 at New Orleans* (pp. 356). Louisiana: IEEE Computer Society.

Anti-Phishing Working Group (APWG). (2007) Phishing Activity Trends, Retrieved July 12, 2010, from http://www.antiphishing.org/reports/apwg_report_january_2007.pdf.

Braber, F., Hogganvik, I., Lund, M. S., Stølen, K., & Vraalsen, F. (2007). Model-based security analysis in seven steps a guided tour to the CORAS method. *BT Technology Journal, 25*, 1, 101-117.

Bradbury, D. (2009). Cost of breaches rises. *Network Security, 48*, 2.

Bradley, T., & Carvey, H. (2006). *Essential Computer Security–Everyone's guide to e-mail, internet and wireless security*. Rockland, USA: Syngress Publishing Inc.

Barclay, K., & Savage, J. (2004). *Object-Oriented Design with UML and Java*. London, UK: Butterworth-Heinemann.

Boggs, W., & Boggs, M. (2002). *Mastering UML with Rational Rose 2002*. Alameda: Sybex.

Chandrasekaran, M. (2009). *An Introspective Behavior Based Methodology to Mitigate E-Mail Based Threats*. Unpublished PhD's thesis, State University of New York, Buffalo, USA.

Cranor, L. F. (2005). Regulatory and Policy Issues. *IEEE Communications Magazine*, 43, 18-19.

Canadian Wireless Telecommunications Association. (2009) Canada's Wireless Industry: A Global Success Story Continues. Retrieved August 1, 2010, from http://www.cwta.ca/CWTASite/english/index.html.

Economist Intelligence Unit. (2010) *The mobile data challenge*. Retrieved August 1, 2010, from http://graphics.eiu.com/upload/eb/Innopath_MobileData_WEB.pdf.

Emigh, A., & Labs, R. (2005). Online Identity Theft: Phishing Technology, Chokepoints and Countermeasures. Retrieved August 8, 2010, from http://www.antiphishing.org/Phishing-dhs-report.pdf.

Fu, Y., Farn, K., and Yang, C. (2008). CORAS for the Research of ISAC. *Proceedings of the 2008 International Conference on Convergence and Hybrid Information Technology held on 28-29 August 2008 at ICHIT* (pp.250-256). Washington DC: IEEE Computer Society.

Goel, S. & Shawky, H. A. (2009). Estimating the market impact of security breach announcements on firm values. *Information Management*, *46*(7), 404-410.

Gordon, L. A., & Loeb, M. P. (2006). Economic aspects of information security: An emerging field of research. *Information Systems Frontiers*, *8*(5), 335-337.

Gordon, L. A., Loeb, M. P., & Sohail, T. 2003. A framework for using insurance for cyber-risk management. *Communication of ACM, 46*(3), 81-85.

Grossman, J. (2007). *Technology Alone cannot Defeat Website Attacks Understanding Technical vs. Logical Website Vulnerabilities*. (Tech. Rep. No. 05.07.), USA: WhiteHat Security.

Halderman, J. A., Waters, B., and Felten, E. W. (2005). A convenient method for securely managing passwords. *Proceedings of the 14th international Conference on World Wide Web held on 10-14 May 2005 at Chiba,Japan* (pp. 471-479). New York: ACM.

Hilley, S. (2007). IT security breaches not behind most ID theft: GAO. *Computer Fraud & Security*, 2004(10), 6-10.

Hook, C. (1995).The cost of computer crime. *IEEE Review*, 41(1), 29-32.

Kimmel, P. (2005). *UML Demystified*. New York, USA: McGraw-Hill.

Khayal, S. H., Khan, A., Bibi, N., & Ashraf, T. (2009, Oct 19-21). *Analysis of Password Login Phishing Based Protocols for Security Improvements*. Paper presented at Emerging Technologies, Rawalpindi, Pakistan.

IBM. (2001). *Rational Unified Process Best Practices for Software Development Teams [White paper]*.Retrieved August 1, 2010, from http://www.ibm.com/developerworks/rational/library/content/03July/1000/1251/1251_best practices_TP026B.pdf.

Kroll, P., & Kruchten, P. (2003). *The Rational Unified Process Made Easy: A Practitioner's Guide to the RUP*. Boston, USA: Addison Wesley.

Kruchten, P. (1996). A Rational Development Process. Retrieved July 15, 2010, from website:http://classes.engr.oregonstate.edu/eecs/winter2008/cs361/rational_kruchten.pdf.

Li, B., Hu, S., & Liu, Y. (2006, Nov 6-9). *A Practical One-Time Password Authentication Implement on Internet*. Paper presented at the International Conference on Wireless, Mobile and Multimedia Networks, Hangzhou, China.

Long, M., & Blumenthal, U. (2010, Jan 10-14). *Manageable One-Time Password for Consumer Applications*. Paper presented at the International Conference on Consumer Electronics, Hillsboro, USA.

Lund, M. S., Solhaug, B., & Stølen, K. (2010). *Model-Driven Risk Analysis*. New York, USA: Springer.

Mizuno, S., Yamada, K., and Takahashi, K. (2005). Authentication using multiple communication channels. *Proceedings of the 2005 Workshop on Digital Identity Management held on 11-11 November 2005 at Fairfax, VA, USA* (pp. 54-62). New York: ACM.

Mahmoud, Q. H., & Popowicz, P. (2010, June 13-15). *Toward a Framework for the Discovery and Acquisition of Mobile Applications*. Paper presented at the Ninth International Conference on Mobile Business Global Mobility Roundtable, Athens, Greece.

McGregor, J. D., & A.Sykes, D. (2001). *A practical guide to testing object-oriented software*, Washington, USA: Addison-Wesley Longman.

Mukhopadhyay, A., Chatterjee, S., Roy, R., Saha, D., Mahanti, A., and Sadhukhan, S. K. 2007. Insuring Big Losses Due to Security Breaches through Insurance: A Business Model. *Proceedings of the 40th Annual Hawaii international Conference on System Sciences held on 03-06 January 2007 at HICSS* (pp. 158a). Washington, DC: IEEE Computer Society.

National Consumers League (1992). *NCL's Fraud Center*. Retrieved July 31, 2010, from http://www.fraud.org.

Ollmann,G.(2007).*Phishing*. Retrieved July 8, 2010, from http://www.technicalinfo.net/papers/Phishing.html.

Poindexter, J. C., Earp, J. B., & Baumer, D. L. (2006). An experimental economics approach toward quantifying online privacy choices. *SpringerLink*, 8(5), 363-374.

Ponemon Institute. (2006). *Annual Study: Cost of a Data Breach Understanding Financial Impact, Customer Turnover, and Preventative Solutions*. Retrieved July 15, 2010, from http://download.pgp.com/pdfs/Ponemon2-Breach-Survey_061020_F.pdf.

Prowell, S., Kraus, R., & Borkin, M. (2010). *Seven Deadliest Network Attacks*. Burlington, USA: Syngress.

Rubin, J., & Chisnell, D. (2008). *Handbook of Usability Testing*. Indianapolis, USA: Wiley Publishing.

Sun, H. and Wang, K. 2008. Defending Secret-Key Based Authentication Protocols against the Stolen-Secret Attack. *Proceedings of the 2008 international Symposium on Electronic Commerce and Security* held on 03-05 August 2008 at ISECS, IEEE Computer Society, Washington, DC, 385-389.

Vraalsen, F., Braber, F. D., Lund, M. S., & Stølen, K. (2005). The CORAS Tool for Security Risk Analysis. *SpringerLink*, 3477, 402-405.

Vyavhare, A. (2000). *Software Testing-Test Cases*. Retrieved August 18, 2010, from http://www.buzzle.com/articles/software-testing-test-cases.html.

Wang, L., & Zhang, R. (2008, Oct 12-15). *An Improved OTP System Based on Bidirectional Virtual Authorization in Mobile Commerce*. Paper presented at the International Conference on Service Operations, Logistics, and Informatics, Beijing, China.

Wang, W. (2003). *Steal This Computer Book 3: What They Won't Tell You About the Internet* (3rd ed.). San Francisco, USA: William Pollock.