Layered Security Approach for Mobile Computing

Bakare, Mustapha Abiodun

(804716)

Universiti Utara Malaysia

2011

Layered Security Approach for Mobile Computing

A thesis submitted to the College of Arts and Sciences in Partial

Fulfillment of the requirement of Master of Science

(Information and Communication Technology)

Universiti Utara Malaysia

February 2011

By

Bakare, Mustapha Abiodun

Copyright © Bakare Mustapha Abiodun. All Rights

Reserved 2011

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, certifies that)

BAKARE MUSTAPHA ABIODUN
(804716)

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

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

LAYERED SECURITY APPROACH FOR MOBILE COMPUTING

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

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

Nama Penyelia
(Name of Supervisor) : **ASSOC PROF. DR.HATIM MOHAMAD TAHIR**

Tandatangan
(Signature) : ____________ Tarikh (Date) : 8/3/11

Nama Penilai
(Name of Evaluator) : **DR. ANGELA EMPHAWAN**

Tandatangan
(Signature) : ____________ Tarikh (Date) : 8/3/11

PERMISSION TO USE

In presenting this thesis in partial fulfillment of the requirements for a Master of Science in Information and Communication Technology degree from Universiti Utara Malaysia, I agree that the University Library may make it freely available for inspection. I further agree the permission of copying of this thesis in any manner, in whole or in part, for scholarly purpose may be granted by my supervisor or, in their absence by the Academic Dean 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 of any material from my thesis.

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

ABSTRACT

Mobile technology had been accepted to be a vital and important and advancing application to be made use of in facilitating our way of doing business, because of its mobility nature. This research focus on securing mobile computing devices using layered security approach in order to safeguard wireless network against any possible threat from unauthorized users from coming into the network. Five layered security levels was discussed in the literature review as an effective means of securing any wireless network from cyber terrorists attacks.

The main objective of this research is to deploy Authentication and Access Control security measures under the Network layer security approach, which happens to be one of the steps involved in securing mobile computing devices using layered security approach. The methodology for the research was adopted from SDLC which include Planning, Analysis, Design, Implementation and Evaluation.

Consequently, the findings of the research was hoped to motivate and encourage organizations to incorporate and deploy layered security approach in improving and enhancing their network security against any possible attacks from external mobile users.

ACKNOWLEDGMENT

I am forever indebted and thankful to the Almighty God for guiding me through the entire length of the way to success and without whose assistance I would never have reach this far and for giving me the strength, wisdom and sound health throughout my period of study in Universiti Utara Malaysia.

I also want to express my warmest and deepest gratitude to my wonderful supervisor in person of Assoc. Prof. Hatim Mohamad Tahir who willingly accepted to supervise, lead and guide me patiently as regard sharing his abundant source of knowledge in this dissertation. I will always be forever thankful and grateful to him because without his beneficial comments, this research would have never been possible.

Once again I thank the Almighty God for His direction and who had made me what I am today. Profound gratitude goes to all the authors whose materials have given me a lot of inspiration in the writing of this project, most of who are referenced.

I am indebted to my beloved parents, Mr. and Mrs. Bakare for all their love and encouragement as well as their financial, moral and spiritual support and for being able to see me through all this years of my studies and for trusting in me.

My appreciation also goes to my siblings in likes of Muyiwa, Wasiu, Kunle and Titilope for their love, assistance and encouragement.

My warmest gratitude also goes to Mr. and Mrs. Ali, Mrs Abudu, Mom Dare, Mom Iqmah, Mr. and Mrs. Odukoya and Mr. Adesiyan for their passionate love shown to enhance my educational development. May God bless you all (Amen).

I also own a lot to my cousins in likes of Lateef, Akeem, Ganiu, Khadijah, Dare, Bose, Damilola, Seun and the rest of the families whose names were not mentioned.

Somebody that you can always count on is your friend. My warmest and strongest appreciation goes to my friends: Mathew, Gbolahan, Sesan, Tola, Bukky, Shola, Folasade, Latifat Afiolaji, Feyi, Ismail, Ayo Omotoso, Ridwan, Okere, Joe, Jelal, Mr. Aliyu, Mohammad Ali, Tunde Adelaja, Ayo Adelaja, Jide Adelaja, Ifalaju, Kelechi, Segun Adebambo, Oyuke, Onuoha, Olamide, Sunday Sejoro, Jide Kuye, Abayo, Remi, Yemi Aleje, David Oduyebo, and so many others whose names were not mentioned. Am using this privilege to say a big thank you for being a friend indeed may the Almighty God continue to strengthen the cord of love that binds us all together. I love and appreciate you all.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER ONE

BACKGROUND OF THE STUDY

1 Introduction

Today wireless networks have gained increasing popularity, providing users with both mobility and flexibility in accessing information. However, existing trends have shown that wireless LAN networks have been exposed to security vulnerabilities, such as risk, threats and attacks (Baghaei, & Hunt, 2004).

To mitigate these risks, agencies need to adopt security measures and practices that help bring their risks to a manageable level (Karygiannis & Owens, 2002). There is a need for a well secured wireless network system, despite its numerous advantages such as strong return on investment, lower installation cost, higher availability and mobile connectivity. The risks to users of wireless mobile computing technology have increased exponentially as the service has become more popular. There were relatively few dangers when wireless technology was first introduced. Crackers had not yet had time to latch on to the new technology and wireless was not commonly found in the working place.

Karygiannis & Owens, (2002) founded that there are various numbers of security risks associated with wireless technology. At corporate level, it is the responsibility of the IT department to keep up to date with the types of threats including appropriate counter measures to deploy. Security threats are growing in the wireless area. Crackers have learned that there is much vulnerability in the

The contents of the thesis is for internal user only

REFERENCE

Agarwal, A, K., Wang, W., & McNair, J, Y. (2005). An Experimental Study of Cross-Layer Security Protocols in Public Access Wireless Networks: In proceedings of IEEE/GLOBECOM, pp. 1747-1751.

Agrawal, P., & Famolari, D. (1999). Mobile Computing in Next Generation Wireless Networks.

Amor (2002). Internet future Strategies: How pervasive computing services will change the world. USA: Prentice Hall.

Arbaugh, W. A., Shankar, N., and Wan, J. (2002). Your 802.1 I network has no clothes. IEEE Wireless Communications.

Ashley, M. (2006). Layered Network Security: A Best Practices Approach: In proceedings of CTO and VP of Customer Experience StillSecure.

Avancha, S. (2005). A Holistic Approach to Secure Sensor Networks PhD Dissertation University of Maryland.

Baghaei, N., & Hunt, R. (2004). IEEE 802.11 Wireless LAN Security Performance using Multiple Clients, Associate Professor, Department of Computer Science and Software Engineering University of Canterbury.

Baghaei, N., & Hunt, R. (2004). IEEE 802.11 Wireless LAN Security Performance using Multiple Clients, Associate Professor, Department of Computer Science and Software Engineering University of Canterbury.

Blackert, W. J., Gregg, D. M., Castner, A.K., Kyle, E.M., Hom, R.L., & Jokerst, R.M. (2003). Analyzing interaction between distributed denial of service attacks and mitigation technologies, Proc. DARPA Information Survivability Conference and Exposition, Volume 1, 22-24, pp. 26 – 36.

Borisov, N. Goldberg, I. & Wagner, D. (2001). Intercepting Mobile Communications: The Insecurity of 802.11. http://www.isaac.cs.berkeley.edu/isaac/wep-draft.pdf.

Borisov, N., Goldberg, I., and Wagner, D. (2001). Intercepting mobile Communications: The insecurity of 802.11, In Proceedings of the Seventh Annual International Conference on Mobile Computing and Networking.

Borisov, N., Ian G., & David W. (2001). Intercepting Mobile Communications: The Insecurity of 802.11, in the Proceedings of the Seventh International Conference on Mobile Computing and Networking.

Burell, J. (2002). Wireless Local Area Networking (WLAN) Security Assessment and Countermeasures. In proceedings of IEEE, 802.11 Wireless Network.

Carey, A. (2001). Wireless Security Vulnerabilities continue to Surface: Cigital Identifies the Latest. White Paper by Cigital, Inc. http://www.cigital.com.

Carlsson, C., Carlsson, J., & Walden, P. (2005). Mobile Services For The Hospitality Industry. Paper presented at the Thirteenth European Conference on Information Systems, Regensburg, Germany.

Carlsson, C., Carlsson, J., & Walden, P. (2005). Mobile Services For The Hospitality Industry. Paper presented at the Thirteenth European Conference on Information Systems, Regensburg, Germany.

Cheng, J. (2008). Testing and Debugging Persistent Computing Systems: A New Challenge in Ubiquitous Computing. In proceedings of IEEE/IFIP International Conference on Embedded and Ubiquitous Computing, pp. 408-414.

Cisco Systems. “Cisco Security Advisory (2001/2002): Catalyst 5000 Series 802.1x Vulnerability. URL: http://www.cisco.com/warp/public/707/cat5k-8021x-vuln-pub.shtml.

Cisco Validated Design, (2008). Wireless and Network Security Integration Design Guide: Americas Headquarters Cisco Systems, Inc. 170 West Tasman Drive San Jose, CA 95134-1706 USA http://www.cisco.com Tel: 408 526-4000 800 553-NETS (6387) Fax: 408 527-0883.

Cole, E. (2002). Hackers Beware. Boston, MA: New Riders.

Colubris Networks, Inc (2002). Comparing Colubris IPSEC Wireless Access Point Solutions with Cisco Safe for Wireless LANs. 2002 Webpage online available at http://download.colubris.com/library/whitepapers/WP-020912-EN-01-00.pdf.

Connolly, P.J. (2002). The trouble with 802.1x.” InfoWorld. 8 March 2002. URL: http://www.infoworld.com/articles/fe/xml/02/03/11/020311fe8021x.xml.

Corral, G., Cadenas, X., Zaballos, A., & Cadenas, M,T. (2005). A Distributed Vulnerability Detection System for WLANs: In proceedings of the First International Conference on Wireless Internet.

Craiger, J,P. (2002). Streamline IT security environments and compliance processes, 802.11, 802.1X, and Wireless Security.

Dankers, J., Garefalakis, T., Schaffelhofer, R., & Wright, T. (2002). Public key infrastructure in mobile systems. Electronics and Communication Engineering Journal.

Dawkins, J., & Dale, J. (2004). “A Systematic approach to Multi- Stage Network Attack Analysis”, Proceedings of the 2nd. IEEE IWIA’04, 0-7695-2117-7/04, 2004.

Dennis A., Wixom B, H., & Tegarden D, (2010). System Analysis and Design with UML: Object-Oriented Approach, Third Edition. John Wiley & Sons, Inc.

Dong W. J., & Doo-Kwon B. (2002). An Adaptive Mobile Computing Model for Dynamic Resource Management in Distributed Computing Environments remarkable, Springer-Verlag Berlin Heidelberg, LNCS 2344, pp. 671-678.

Douceur, J. (2002). The Sybil Attack: 1st International Workshop on Peer-to-Peer Systems.

El-Alfy, E.-S. M. (2005). A General Look at Building Applications for Mobile Devices.

Erten, Y, M,. & Tomur, E. (2004). A Layered Security Architecture for Corporate 802.11 Wireless Networks. In proceeding of IEEE, pp.123-128.

Farouzan, B, A., & Fegan, S, C. (2007). Data Communications and Networking, TCP/IP Protocol Suite Local Area Network, Business Data Communication, forth edition, McGraw- Hill Forouzan Networking Series, Higher Education.

Fitzgerald, J., & Dennis, A. (1993). Business Data Communications and Networking: Basic Concepts, Security and Design, 4th Edition.

Fleck, B. & Jordan D., (2002). Wireless Access Points and ARP Poisoning: Wireless vulnerabilities that expose the wired network. White Paper by Cigital, Inc. http://www.cigital.com.

Fluher, S., Mantin, I., & Shamir, A. (2001). Weaknesses in the Key Scheduling Algorithm of RC4. http://downloads.securityfocus.com/library/rc4_ksaproc.pdf.

Fluhrer, S., Martin, I., & Shamir, A. (2001). Weaknesses in the key scheduling algorithm of RC4, Eighth Annual Workshop on Selected Areas in Cryptography.

Geier, J. (2002)"802.11 WEP: Concepts and Vulnerability." 802.11 Planet.

Hoffer, J. A., George, J., & Valacich, J. (2002). Modern Systems Analysis and Design. http://staging.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml.

IEEE. "IEEE 802.1x-2001 (ISO/IEC 802-1x: 2001), Part 11: Wireless LAN Medium Access Local and metropolitan area networks: Port-Based Network Access Control." URL: http://standards.ieee.org/getieee802/download/802.1X- 2001.pdf.

International Engineering Consortium (2007). Web ProForums Retrieved August 13, 2009, from http://www.iec.org/online/tutorials/wap/index.html.

Ivan K. (1998). Software Vulnerability Analysis, Ph.D. thesis, Department of Computer Sciences, Purdue University, https://www.cerias.purdue.edu/techreports-ssl/public/98-09.pdf.

Kalkbrenner, G., & Nebojsa, F. (2001). Campus Mobil: Mobile Services for Campus and Student needs Retrieved August 15, 2009.

Kamara, S., Fahmy, S., Schultz, E., Kerschbaum, F., & Frantzen, M. (2001). Analysis of Vulnerabilities in Internet Firewalls: Center for Education and Research in Information Assurance and Security (CERIAS).

Karygiannis & Owens, (2002). Wireless Network Security 802.11, Bluetooth and Handheld Devices. Recommendations of National Institute of Standards and Technology, on Wireless Network Security, pp. 1-119.

Koudounas & Iqbal, (1996). Mobile computing: past, present and future.

Koudonnas, V., & Iqbal, O. (1991). Mobile computing: past, present and future. N. Sollenberger, N. Seshadri, and R. Cox, "The Evolution of IS-136 TDMA for Third Generation Wireless Services", IEEE Personal Communications, Vol. 6, No. 3.

Krishnamurthy, Prashnt, Joseph Kabara, Tanapat Anusas-amornkul. (2002). Security in Wireless Residential Networks, IEEE Transactions on Consumer Electronics, Vol 48, No 1, pp 157- 166.

Kurose, J, F., & Ross, K, W. (2008). Computer Networking A Top-Down Approach, fourth edition, Pearson International Education.Inc.

Kustin, S. (2002). The Proliferation of Wireless Internet Access Devices and its Effect on Consumer Behavior Patterns.

Lockhart, A. (2006). Network Security Hacks Second Edition.

Loeb, L. (2002). What's up with WEP? http://www.106.ibm.com/developerworks/library/s-wep/.

Lynn, M., & Robert B. (2002). Advanced 802.11 Attack, presentation to Black Hat Conference, Las Vegas, NV 31 July 2002. Available at http://www.blackhat.com/presentations/bh-usa-02/baird-lynn/bh-us-02-lynn-802.11attack.ppt.

Bishop, M., & Bailey, D. (1996). A critical analysis of vulnerability taxonomies," in Proceedings of the NIST Invitational Workshop on Vulnerabilities, July 1996, Also appears as Technical Report 96-11, Department of Computer Science, University of Califonia at Davis, http://seclab.cs.ucdavis.edu/projects/vulnerabilities/scriv/ucd-ecs-96-11.ps. Also see Classifying Vulnerabilities, A Taxonomy of UNIX and Network Security Vulnerabilities, as well as Vulnerabilities Analysis by same author.

Mishra, A., & Arbaugh, W. (2002). An initial security analysis of the 802.1x standard. http://www.cs.umd.edu/~waa/1x.pdf.

Mishra, A., & William, A. (2002). An Initial Security Analysis of The IEE 802.1X Standard. University of Maryland, Department of Computer Science and University of Maryland Institute for Advanced Computer Studies Techniacal Report CS-TR-4328 and UMIACS-TR-2002-10 6.

Moioli, F. (2000). Security in Public Access Wireless LAN Networks, Masters Thesis, Department of Teleinformatics, Royal Institute of Technology, Stockholm, Sweden. New Jersey: Prentice Hall.

Newsome, J., Shi, E., Song, D, & Perrig, A. (2004). The sybil attack in sensor networks: analysis & defenses", Proc. of the third international symposium on Information processing in sensor networks, ACM, pp. 259 – 268.

Nortel (2007). Layered Defense Approach to Network Security: Nortel, the Nortel logo, Nortel Business Made Simple, the Globemark, Alteon, BayStack, Contivity, Passport and Optivity are trademarks of Nortel Networks.

Nylander, S. (2004). Different Approaches to Achieving Device Independent Services an Overview: Swedish Institute of Computer Science.

Open Mobile Alliance (OMA) (2004). Open Mobile Alliance Overview Retrieved August 13, 2009,
from http://www.openmobilealliance.org/docs/OMAShortPaper_May2004v.1.pdf.

Pathan, A, K., Lee, H., W., & Hong, C, (2006). Security in Wireless Sensor Networks: Issues and Challenges. In proceedings of IEEE 8th International Conference. On Advanced Communication Technology, pp. 6-1048.

Pullen, M. (2000). The Internet Protocol Stack and the Network Workbench, Through Hands-On Programming, pp. 1-10.

Roshan, P. (2001). 802.1X authenticates 802.11 wireless." NetworkWorldFusion.URL: http://www.nwfusion.com/news/tech/2001/0924tech.html.

Quality.com (2009): Definition of Use Case. Retrieved August 25, 2009 from

http://searchsoftwarequality.techtarget.com/defination/

Schei, E., & Fritzner, T. C. (2002). MOWAHS: A Study of Applications for Mobile Work.

Schwartz, E. (2002). Researchers crack new wireless security spec." InfoWorld. 14 February 2002,
URL: http://www.infoworld.com/articles/hn/xml/02/02/14/020214hnwifispec.xml.
(12 June 2002).

Schwartz, E. (2002). Researcher crack new wireless security spec. InfoWorld.

Shuyao, Y., Youkun, Z., Chuck, S., & Kai, C. (2004). A security architecture for Mobile Ad Hoc Networks. Institute of Computer Technology, School of Software, Computer Network Information Bell Labs Computer Network, Center of Chinese Academy of Sciences,pp. 1-4.

Simon et al, (2005).Object-Oriented Systems Analysis and Design: Using UML. US, Third

edition, pp 230.

Simoneau, P. (2006). The OSI Model: Understanding the Seven Layers of Computer Networks. Global Knowledge Global Knowledge Training LLC, pp. 1-11.

Skoudis, E. (2002). Counter Hack: A Step-by-Step Guide t Computer Attacks and Effective Defenses. Prentice Hall, Upper Saddle River, New Jersey. pp 351-358.

Sung-Hoon, P. (2003). AN Efficient Election Protocol in Mobile Computing Environment", Springer-Verlag, Berlin Heidelberg, LNCS 2657, pp. 387-396.

Surman, G. (2002). Understanding Security Using the OSI Model, SANS Institute Information Security Reading Room. Assignment Version: GSEC Practical Version 1, pp. 1-20.

Tillwick., H, & Olivier., M. S (2004). A layered security architecture, in Proceedings of the Fourth Annual Information Security South Africa Conference, Midrand, South Africa.

Turban, E., Leidner, D., McLean, E., & Wetherbe, J. (2007). Information Technology for Management: Transforming Organizations in the Digital Economy (6th ed.): John Wiley & Sons.

Turisco, F., & Case, J. (2001). First Consulting Groups, Wireless and Mobile Computing, prepared for California Healthcare Foundation.

Walker, J., & Gmup, E. (2000). Unsafe at any key size: An analysis of the WEP encapsulation, IEEE 802.11 Task.

Wang, B.T., & Schulzrinne, H. (2004). An IP traceback mechanism for reflective DoS attacks", Canadian Conference on Electrical and Computer Engineering, Volume 2, 2, pp. 901 – 904.

WapForum (2002a). What is WAP Retrieved July 20, 2009, from http://www.wapforum.org/faqs/index.htm.

Wapforum (2002b). Wireless Application Protocol (WAP 2.0): Technical White Paper Retrieved from www.wapforum.org/what/WAPWhite_Paper1.pdf.

Welch, D., & Lathrop, S. (2003). Wireless Security Threat Taxonomy. In proceedings of IEEE Systems, on Man and Cybernetics Society, Information Assurance Workshop, 76-83.

Wenliang Du., & Aditya P. M. (1998). Categorization of software errors that led to security breaches," in Proceedings of the 21st National Information Systems Security Conference , http://www.cerias.purdue.edu/homes/duw/research/paper/nissc98.ps.

Wenliang Du., & Aditya P. M. (2000). Testing for software vulnerability using environment perturbation, in Proceeding of the International Conference on Dependable Systems and Networks (DSN 2000), Workshop On Dependability Versus Malicious Faults, pp. 603–612,http://www.cerias.purdue.edu/homes/duw/research/paper/ftcs30 workshop.ps.

Whalen, S. (2002). An Introduction to Arp Spoofing, April 2001 webpage online available at http://packetstormsecurity.nl/papers/protocols/intro_to_arp_spoofing.pdf last accessed.

Xi Wang, Xu Liu, Xiaoge Wang & Yu Chen. (2004). A Middleware Based Mobile Scientific Computing System- MobileLab" , Springer-Verlag Berlin Heidelberg, LNCS 3251, pp. 1013-1016.

Yang, H., Xie, L., & Sun, J. (2004). Intrusion detection for Wireless Local Area Network. In proceeding of IEEE Canadian Conference on Electrical and Computer Engineering, 4, 1949-1952.

Zhiming, Q., & Jingmei, W. (2009). Application of primary components analysis of security threat in wireless network. Journal of ISECS International Colloquium on Computing, Communication, Control, and Management.