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) : 3/1/1

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

Tandatangan
(Signature) :  

Tarikh (Date) : 3/1/11
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 Afolaji, Feyi, Ismail, Ayo Omotoso, Ridwan, Okere, Joe, Jelal, Mr. Aliyu, Mohammad Ali, Tunde Adelaja, Ayo Adelaja, Jide Adelaja, Ifalaja, 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

PERMISSION TO USE .............................................................................................................. i
ABSTRACT ................................................................................................................................. ii
ACKNOWLEDGEMENT .............................................................................................................. iii
TABLE OF CONTENTS ............................................................................................................. v
LIST OF TABLES ....................................................................................................................... viii
LIST OF FIGURES .................................................................................................................... ix
CHAPTER ONE: BACKGROUND OF THE STUDY ................................................................. 1
1 Introduction .......................................................................................................................... 1
   1.1 Problem statement ........................................................................................................ 3
   1.2 Research Questions ..................................................................................................... 3
   1.3 Research Objectives ................................................................................................... 3
   1.4 Scope of the Study ....................................................................................................... 4
   1.5 Significance of the study ............................................................................................ 4
   1.6 Limitation of the study ............................................................................................... 4
   1.7 Summary ..................................................................................................................... 5
CHAPTER TWO: LITERATURE REVIEW ............................................................................. 6
2 Introduction .......................................................................................................................... 6
   2.1 Mobile Technology ..................................................................................................... 6
      2.1.1 Wireless Data Transfer Options ..................................................................... 13
      2.1.2 Wireless LAN ..................................................................................................... 14
      2.1.3 Benefits of Wireless LAN .............................................................................. 14
      2.1.4 Wireless Internet .............................................................................................. 15
      2.1.5 Data Synchronization ...................................................................................... 16
   2.2 Mobile Application ..................................................................................................... 16
      2.2.1 Benefits of Mobile Computing ..................................................................... 20
   2.3 Wireless Application Protocol (WAP) ..................................................................... 21
      2.3.1 WAP Architecture ............................................................................................ 24
   2.4 Challenges of Mobile Computing ............................................................................. 26
      2.4.1 Security Threats and Attacks on Wireless Networks ...................................... 28
   2.5 Network Security ....................................................................................................... 41
      2.5.1 Security Challenges in Wireless Networks ...................................................... 42
      2.5.2 Wireless Network Security .............................................................................. 44
   2.6 Weaknesses in UnLayered Security Architectures .................................................... 46
LIST OF TABLES

Table 2.1: Comparisons of Mobile Computing (Turisco, & Case, 2001) ........................................8
Table 2.2: Potential Benefits from Health Care Mobile Computing Applications (Turisco, &
Case, 2001). ........................................................................................................................................21
Table 4.1: Development environment .................................................................................................75
LIST OF FIGURES

Figure 2.1: Mobile Computing Device (Turisco, & Case, 2001) ......................................... 8
Figure 2.2: Wireless Landscape Diagram (Turisco, & Case, 2001) ........................................ 9
Figure 2.3: Mobile Computing Infrastructure (Turban, Leidner, Mclean, & Wetherbe, 2007) 10
Figure 2.4: Mobile Computing Component (Turisco, & Case, 2001) ................................... 11
Figure 2.5: Basic WLAN Components (Burrell, 2002) ......................................................... 13
Figure 2.6: Wireless LAN Diagram (Turisco, & Case, 2001) .............................................. 14
Figure 2.7: Wireless Internet Diagram (Turisco, & Case, 2001) .......................................... 15
Figure 2.8: Data Synchronization Diagram (Turisco, & Case, 2001) ...................................... 16
Figure 2.9: WAP Protocol Stack (Wapforum, 2002a) ......................................................... 25
Figure 2.10: Passive Eavesdropping (Welch & Lathrop, 2003) ............................................. 31
Figure 2.11: Unauthorized Access (Welch & Lathrop, 2003) .............................................. 33
Figure 2.12: Man-in-the-Middle Attack (Welch & Lathrop, 2003) ....................................... 33
Figure 2.13: ARP Attack (Welch & Lathrop, 2003) ............................................................ 36
Figure 2.14: Session High-Jacking (Welch & Lathrop, 2003) .............................................. 37
Figure 2.15: Session High-Jacking (Welch & Lathrop, 2003) .............................................. 38
Figure 2.16: Replay attack (Welch & Lathrop, 2003) .......................................................... 39
Figure 2.17: Sybil Attack (Pathan, Lee, & Hong, 2006) ......................................................... 41
Figure 2.18: The Security Process (Cisco Validated Design, 2008) ........................................ 42
Figure 2.19: Shared-Key Authentication Process (Craiger, 2002) .......................................... 48
Figure 2.20: Wired Equivalent Privacy (Loeb, 2001) ............................................................ 50
Figure 2.21: 802.11x using Dynamic Key Session (Geier, 2002) ........................................... 53
Figure 2.22: 802.11x Authentication Process (Geier, 2002) .................................................. 54
Figure 2.23: 802.11x Session Hijacking (Cole, 2002) ............................................................ 55
Figure 2.24: Proposed Layered Security Approach (Ashley, 2006) ...................................... 58
Figure 2.25: Layered Security Approach (Erten, & Temur, 2004) ........................................ 60
Figure 2.27: Layered Defense Network Security Approach (Nortel, 2007) .......................... 64
Figure 3.1: Access Control/User Authentication (Ashley, 2006) .......................................... 67
Figure 3.2: System Development Life Cycle (Dennis A, Wixom B, & Teagarden D, 2010) .... 68
Figure 4.1: User Authentication and Access Control UML Use Case Diagram .................... 73
Figure 4.2: Sequence Diagram for Use Cases Login Authentication and Access Control ....... 74
Figure 4.3: Mobile User device Page ..................................................................................... 76
Figure 4.4: User Login/Authentication Page ......................................................................... 77
Figure 4.5: User Access Page ............................................................................................... 77
Figure 4.6: User Access Denied Page .................................................................................... 78
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


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


85


86


