



UNIVERSITI PUTRA MALAYSIA

**TOKEN BASED AUTHENTICATA METHOD USING BLUETOOTH-
ENABLED MOBILE PHONE**

RANIA ABDELHAMEED MOKHTAR.

FK 2005 47



**TOKEN BASED AUTHENTICATION METHOD USING BLUETOOTH-
ENABLED MOBILE PHONE**

By

RANIA ABDELHAMEED MOKHTAR

**Thesis submitted to the School of Graduate Studies, Universiti Putra
Malaysia, in Fulfillment of the Requirements for the Degree of Master of
Science**

October 2004



DEDICATION

To *My husband Rashid, and my daughter Shahd*



Abstract of thesis present to the Senate of Universiti Putra Malaysia in fulfillment of the requirement for the degree of Master of Science

TOKEN BASED AUTHENTICATION METHOD USING BLUETOOTH-ENABLED MOBILE PHONE

By

RANIA ABDELHAMEED

June 2004

Chairman: Sabira Khatun, PhD

Faculty: Engineering

Authentication is a mechanism to establish proof of identities; it ensures the right identification of a particular user or a particular system or device. Authentication is the first step in any cryptography solution, because unless the device knows who is using it, there is no point in encrypting device's contents. Current PC, laptop user authentication systems are always done once and held until it is explicitly revoked by the user, or frequently asking the user to reestablish his identity which encourages him to disable the authentication. In this thesis we propose a new model of authentication for laptop devices using a Bluetooth-enabled mobile phone. In this model the Bluetooth-enabled mobile phone works as an authentication token that provides the authentication for laptop over a Bluetooth short-range wireless link. The user doesn't need to authenticate frequently. Instead, the mobile phone continuously authenticate with the laptop by means of the short-range wireless link. This model ensures that a non-legitimate user's mobile phone cannot provide authentication services to other user's laptops, and it uses an



authenticated and encrypted Bluetooth wireless link to ensure that there is no eavesdropping, modification, and insertion of messages traveled over the link.



Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk ijazah Master Sains

**PENGGUNAAN “TOKEN” BAGI PENENTUSAHAN KOMPUTER
MENGUNAKAN TELEFON BERGERAK DENGAN BLUETOOTH**

Oleh

RANIA ABDELHAMEED

Oktober 2004

Pengerusi: Sabira Khatun, PhD

Fakulti: Kejuruteraan

Penentusahan adalah mekanisma untuk membuktikan sesuatu identiti; ia memastikan kesahihan pengguna, sesuatu sistem atau peralatan itu. Penentusahan adalah langkah pertama di dalam penyelesaian kriptografi kerana kecuali sesuatu peranti itu mengetahui siapa penggunanya, tiada makna dalam mengkriptografi kandungan peranti tersebut. Sistem penentusahan pengguna PC komputer riba kini selalunya dilakukan sekali dan kekal sehingga ianya secara jelasnya di batalkan oleh pengguna atau dengan kerap meminta pengguna untuk memperkenalkan semula identitinya yang mana menggalakkannya untuk memberhentikan penentusahan. Di dalam tesis ini kami mencadangkan model baru penentusahan bagi peranti komputer riba menggunakan telefon bimbit dengan Bluetooth. Di dalam model ini telefon bimbit berfungsi Bluetooth menjadi sebagai token penentusah yang menyediakan penentusahan kepada komputer riba melalui jarak pendek hubungan tanpa wayar Bluetooth. Pengguna tidak perlu menentusah secara kerap, sebaliknya telefon bergerak akan melakukannya secara berterusan dengan

komputer riba melalui hubungan tanpa wayar jarak pendek. Model ini memastikan telefon bergerak pengguna lain yang tidak sah tidak boleh menyediakan perkhidmatan penentusahan kepada pengguna komputer riba lain dan ia menggunakan hubungan tanpa wayar bertentusahan dan berinkripsi untuk memastikan tiada pencuri-dengar, pengubahsuaian dan kemasukan mesej melalui hubungan tersebut.

ACKNOWLEDGMENTS

I am extremely grateful to Third World Organization for Women in Science (TWOWS), for awarded me a TWOWS Postgraduate Training Fellowship to pursue the M.Sc. degree, and for supporting travel, visa, medical, and living expenses for the duration of the study. Special thank to TWOWS President Lydia P. Makhubu, and TWOWS finance Manuela Schipizza Lough, for their kind, careful, and quickly responses during the fellowship procedures.

I am deeply indebted to Dr. Sabira Khatun, the chairman of my supervisory committee for this research, who handles all the administrative tasks, without her help the completion of this work would have taken a great deal longer. I have learnt so much from her in so many ways, both personally and technically.

I am grateful to supervisory committee members, Prof. Dr. Borhanuddin Mohd. Ali, the director of Multimedia Institute (IBM), UPM, and Assoc. Prof. Dr. Abdul Rahman Ramli, the head of Intelligent System and Robotics laboratory, Institute of Advanced Technology (ITMA), UPM, for many valuable conversations about this work.

I also wish to thank Prof Dr. Mohd Khazani Abdualah, the head of the Computer and Communication Engineering Department, UPM, Prof. Aini Ideris, the dean of



School of Graduate Studies, UPM, and Dr. Elsadig A. Mohd Babiker, for the greatest assistances given by them during the fellowship procedures.

I wish to record my deep gratitude to Mr. Shaiful Jahari Hashim; also I am grateful to my colleagues in Wireless Broadband Research Group (WBRG), Networks and Communications laboratory, for their many supports.

I would like to thank Rococo Soft Company, for giving me their J2ME/J2SE/Bluetooth Development Kit free of charge.

Finally, no acknowledgments could complete without acknowledging my husband, Rashid, who actually helped me with a number of reviews, which carry a lot of meaning.



TABLE OF CONTENTS

	Page
DEDICATION	ii
ABSTRACT	iii
ABSTRAK	v
ACKNOWLEDGMENTS	vii
APPROVAL	ix
DECLARATION	xi
LIST OF TABLES	xvi
LIST OF FIGURES	xvii
LIST OF ABBREVIATIONS	xx
CHAPTER	
1 INTRODUCTION	24
1.1 Background	24
1.1.1 Security Model	24
1.1.2 Principles of Security	25
1.2 Authentication	26
1.2.1 Authentication Basics	26
1.2.2 Persistent and Transient Authentication	27
1.3 Special Security Considerations Needed for Laptop	29
1.4 Problem Statements	31
1.5 Motivation	31
1.6 Aim and Objectives	32
1.7 Study Model	34
1.8 Outline of the Thesis	35
2 LITERATURE REVIEW	37
2.1 Identity, Authentication and Authorization	38
2.1.1 Personal Authentication Mechanisms	39
2.1.1.1 Something the User Knows	39
2.1.1.2 Something the User Has	41
2.1.1.3 Something The User Is	44
2.1.2 Authentication for Cryptographic File System	46
2.2 Encryption	48
2.3 Other Laptop Security Tools	49
2.3.1 Physical locking devices	50
2.3.2 Monitoring and tracing software	51
2.3.3 Alarms	52



2.4	Disconnection and Reconnection Time	53
2.5	Interaction of Bluetooth Technology for Authentication	54
2.5.1	Power Requirements	57
2.5.2	Physical Links	57
2.5.2.1	Asynchronous Connection-Less Link	58
2.5.2.2	Synchronous Connection-Oriented Link	58
2.5.3	Logical Channels	59
2.5.4	Bluetooth Protocol Stack	60
2.5.5	Bluetooth Core Protocols	61
2.5.5.1	Baseband	61
2.5.5.2	Link Manager Protocol	62
2.5.5.3	Logical Link Control and Adaptation Protocol	63
2.5.5.4	Service Discovery Protocol (SDP)	63
2.5.6	Host Controller Interface (HCI)	64
2.5.7	Type of Connection	65
2.5.8	Bluetooth Security	66
2.5.8.1	Security Methods	66
2.5.8.2	Device Trust Levels	67
2.5.8.3	Security Level of Services	68
2.5.8.4	Bluetooth Hack Lexicon	69
2.5.9	Bluetooth APIs	70
2.6	Discussion	72
2.7	Conclusion	73
3	METHODOLOGY	75
3.1	Authentication System Principles	75
3.2	System Security Requirements	76
3.3	Authentication System Design	77
3.3.1	Security Module	77
3.3.1.1	Laptop-Cell phone Authentication System	78
3.3.1.2	User Authentication System	85
3.3.1.3	Encryption and Decryption Process	86
3.3.2	Communication Module	86
3.3.2.1	Devices Connectivity	87
3.3.2.2	Connection at Physical and Data Link Layers	87
3.3.2.3	Connection Establishment at Laptop Side	89
3.3.2.4	Connection Establishment at Mobile Side	90
3.3.3	Manual Disable Module	91
3.4	Implementation	91
3.4.1	Laptop system	91
3.4.2	Mobile phone system	92
3.4.3	Application Programs	93
3.4.3.1	Session Establishment	93
3.4.3.2	Connection Security	96



3.4.3.3	Frequent Reauthentication	97
3.4.4	Flow Charts	99
3.4.5	System Configuration and Management	104
3.4.6	System Testing Environment	106
3.5	Wireless link Security	106
3.6	Summary	107
3.7	Discussion	108
4	RESULTS	109
4.1	Maintain Performance and Ensure Security	109
4.1.1	System Security Issues	109
4.1.2	Security Function Performance	110
4.1.2.1	Performance of Mutual Authentication Function	110
Case I :	Right Access Case	111
Case II:	Hacking Case	113
4.1.2.2	Performance of Session Key Creation Function	115
4.1.3	User Disconnection and Reconnection Time	116
4.1.4	Attacks and Usability	119
4.2	System Control Panels	119
4.3	Manual Disable Function	123
4.4	Comparison of System Time with Existing Methods	123
4.5	Discussion	126
5	DISCUSSION	127
5.1	LABM System Security	127
5.2	Trust and Threat Model	127
5.3	Mobile Phone Vulnerabilities	128
5.4	Laptop Vulnerabilities	129
5.5	Bluetooth for LABM Wireless Link	130
5.5.1	Bluetooth	130
5.5.1	Infrared (IR)	131
5.5.2	Ultra Wideband (UWB)	132
5.5.3	ZigBee	132
5.6	Comparison with Existing Related Work	134
5.6.1	Zero Interaction Authentication (ZIA)	134
5.6.2	Microsoft Windows 2000 Authentication System	136
5.6.3	Biometric authentication	136
5.7	Powerful and Weaknesses of the System	137
5.8	Complexity of the System	138
6	CONCLUSION	139
6.1	Summary	139
5.1	Future Works	141



REFERENCE	143
APPENDICES	149
A Source Code	149
B Standardized Security Algorithm used in Project	183
BIODATA OF THE AUTHOR	193



LIST OF TABLES

	Page
2.1: Laptop Security Technologies	38
2.2: Bluetooth Protocol Layer	61
2.3: Java APIs for Bluetooth	71
3.1: A record store database	105
4.1: Time comparison with other systems	125
5.1: Comparison with ZIA system	135
B.1: Evaluation result of AES	187



LIST OF FIGURES

	Page
1.1: Absence of authentication	27
1.2: Study model	34
2.1: Built-in biometric fingerprint scanner	45
2.2: ZIA disconnection and reconnection time	54
2.3: Functional blocks in Bluetooth System	56
2.4: The Bluetooth Protocol Stack	60
2.5: Link Manager Protocol	62
2.6: SDP request/response model	64
2.7: Bluetooth Hardware Architecture	65
2.8: Bluetooth Piconet Networks	66
3.1 (a): Frequently the mobile phone authenticates with the laptop via short-range wireless link	76
3.1 (b): Secure laptop in absence of mobile phone (user)	76
3.2: Authentication system stack	77
3.3: Laptop- cell phone- authentication system	78
3.4: Mobile phone-laptop mutual authentication function	80
3.5: Session key creation	82
3.6: User present checking	83
3.7: Polling, laptop-mobile phone	83



3.8:	Declaring absence of user after three present check message(s) without acknowledgements	84
3.9:	Connection at Data link and Physical layers	88
3.10:	Laptop (client side) connection functions	89
3.11:	Mobile phone (server side) connection functions	90
3.12:	Using of java APIs in communication module	92
3.13:	Mutual Authentication flowchart	99
3.14	Encryption process using Advanced Encryption Standard (AES)	100
3.15	Decryption process using Advanced Encryption Standard (AES)	101
3.16:	Session key generation flowchart	102
3.17:	Polling, disconnection and reconnection	103
3.18:	State machine diagram	107
4.1 (a)	Performance of mutual authentication function in server side with a correct keys configuration and knowledge of other side public key.	111
4.1 (b)	Performance of mutual authentication function in client side with a correct keys configuration and knowledge of other side public key.	112
4.2 (a):	Performance of mutual authentication function in server side with a correct keys configuration and without knowledge of other side public key.	113
4.2 (b):	Performance of mutual authentication function in client side with a correct keys configuration and without knowledge of other side public key.	114
4.3 (a):	Performance of session key creation function in server side	115
4.3 (b)	Performance of session key creation function in client side	116
4.4:	Time required for user disconnection	117
		xviii



4.5:	Time required for user reconnection	119
4.6 (a):	Tab for laptop public and private keys configuration	120
4.6 (b):	Tab for mobile phone public key configuration	120
4.6 (c):	Tab for bin code configuration	121
4.7 (a):	System help menu	121
4.7 (b):	Keys configuration help topic	122
4.7 (c):	User guides to configure keys	122
4.8 (a):	Mobile phone keys setting screen	124
4.8(b):	Configuration of public key for mobile phone	124
4.8 (c):	Configuration of private key for mobile phone	125
4.8 (d):	Configuration of laptop public key for mobile phone	125
4.9:	Security screen with disable facility	126



LIST OF ABBREVIATIONS

Acronym	Meaning
ACL	Asynchronous Connection Less
AES	Advanced Encryption Standard
API	Application Programming Interface
APIs	Application Programming Interfaces
ARQ	Automatic Repeat Request
ATM	Automatic Teller Machine
BCC	Bluetooth Control Center
BIOS	Basic Input Output System
BPSK	Binary Phase-Shift Keying
CBS	Cell Broadcast Service
CFS	Cryptography File System
CLDC	Connected Limited Device Configuration
CPU	Central Processing Unit
ESS	Embedded Security Subsystem
FEC	Forward Error Check
FHSS	Frequency Hopping Spread Spectrum
GCF	Generic Connection Framework
HCI	Hardware Controller Interface
HEX	Hexadecimal



IDE	Integrated Development Environment
IEEE	International Electrical and Electronics Engineers
IP	Internet Address
IR	Infrared
IrDA	Infrared Data Association
ISM	Industrial Scientific and Medical
ISO	International Standard Organization
IT	Information Technology
J2ME	Java 2 Micro Edition
J2SE	Java 2 Standard Edition
JAWBT	Java APIs for Bluetooth Wireless Technology
JRE	Java Runtime Environment
JSR 82	Java APIs for Bluetooth Wireless Technology
JTWI	Java Technology for the Wireless Industry
KEA	Key Exchange Algorithm
L2CAP	Logical Link Control and Adaptation Protocol
LAN	Local Area Network
LC	Link Controller
LCD	Light Cathode Display
LM	Link Manager
LMP	Link Manager Protocol
MIDlet	MIDP Application



MIDP	Mobile Information Device Profile
MTU	Maximum Transmission Unit
OBEX	Object Exchange
OS	Operating System
OSI	Open System Interconnection
PAN	Personal Area Network
PC	Personal Computer
PDA	Personal Data Assistant
PDU	Protocol Data Unit
Piconet	Bluetooth network
PIN	Personal Identification Number
PKI	Public Key Infrastructure
PPM	Pulse Position Modulation
PPP	Point-to-Point Protocol
RF	Radio Frequency
RFCOMM	Radio Frequency Communication Protocol
RSA	Rivest Shamir Adleman (Public key cryptography algorithm named for its inventors)
SCO	Synchronous Connection Oriented
SDK	Software Development Kit
SDP	Service Discovery Protocol
SIG	Special Interest Group



SPINS	Session Personal Identification Numbers
TCP	Transport Control Protocol
UA	User Asynchronous channel
UDP	User Datagram Protocol
UI	User Isochronous channel
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
US	User Synchronous channel
UWB	Ultra Wideband
WLPAN	Wireless Personal Area Network
ZIA	Zero Interaction Authentication



CHAPTER 1

INTRODUCTION

1.1 Background

Most olden computers have physical key to lock the system, it had no, or at best, very little data security. This continued for a number of years until the importance of data was truly realized. Until then, computer data was considered useful, but not something to be protected. When computer applications were developed to handle financial and personal data, the real need for security was felt like never before. People realized that data on computers is an extremely important aspect of modern life. Modern computers assume that they are personal to the user and the operating system starts to provide adequate security and authentication. Therefore, various areas in security began to gain prominence. Two typical examples of such security mechanisms were as follows:

- User authentication
- Encoding of stored information

This research is focus in the part of user authentication in the context of mobile computers.

1.1.1 Security Model

There are several approaches to implement a security model: