UNIVERSITI PUTRA MALAYSIA

TOKEN BASED AUTHENTICA METHOD USING BLUETOOTH-ENABLED MOBILE PHONE

RANIA ABDELHAMEED MOKHTAR.

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 MENGGUNAKAN 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 Abduallah, 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

LIST OF TABLES

LIST OF FIGURES

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 Taller 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: