DEVELOPING A SECURITY MECHANISM FOR NOKIA SERIES 60 BLUETOOTH-ENABLED MOBILE PHONES

BY

Ruby Jean D. Fernando

Dianne Mae A. Petines

Aaron T. Seng

SCHOOL OF ARTS AND SCIENCES

ATENEO DE DAVAO UNIVERSITY

MARCH 2005

DEVELOPING A SECURITY MECHANISM FOR NOKIA SERIES 60 BLUETOOTH-ENABLED MOBILE PHONES

An Independent Research

Presented to

The Faculty of the Computer Studies Division

Ateneo de Davao University

In Partial Fulfillment

of the Requirements for the Degree

Bachelor of Science major in Computer Science

by

Ruby Jean D. Fernando

Dianne Mae A. Petines

Aaron T. Seng

SCHOOL OF ARTS AND SCIENCES

ATENEO DE DAVAO UNIVERSITY

MARCH 2005

TABLE OF CONTENTS

ABSTRACT

The wide use of Bluetooth technology in digital devices has grown over the past seven years. Several handheld devices such as laptops, PDAs and mobile phones make use of Bluetooth technology. This technology enables devices to link together wirelessly in a flexible network topology. Recently, Bluetooth users discovered many security flaws. Thus, this study presents a comprehensive understanding of the Bluetooth technology and develops a security mechanism for Bluetooth-enabled mobile phones.

Keywords: Bluetooth, Network Topology, Security Flaws, Security Mechanism

CHAPTER 1

INTRODUCTION

1.1 Background of the Study

Bluetooth wireless technology, designed for simple wireless networks, connects multiple personal wireless devices equipped with specialized Bluetooth chips. Today, the world experiences the enormous growth of this technology.

Bluetooth technology presents numerous advantages. With Bluetooth, (1) one can create a personal network at home or on the road; (2) synchronization of calendars, address books, and notes between Bluetooth-enabled devices is possible; and (3) one is able to print pictures, access cell phone data, and receive e-mails.

Recently, users have discovered security flaws in Bluetooth technology. Devices equipped with Bluetooth are vulnerable to unauthorized access and manipulation. Several researches proved that Bluetooth-enabled devices are prone to intruders and outside attackers that could put the integrity of data at risk. In addition, these devices could be tools of industrial espionage and commercial spamming.

Presently, no software solution is available for these Bluetooth-enabled mobile phone security problems. The team is motivated to study and develop possible solutions to address these security problems.

1.2 Statement of the Problem

This study sought to answer the general problem: How can a security mechanism be developed to address the security flaws found in Nokia series 60 Bluetooth-enabled mobile phones?

Specifically, it sought to answer the following questions:

- How does Bluetooth technology work?
- In what ways do attackers carry out "Bluejacking" and other similar attacks in Nokia series 60 mobile phones?
- What is the existing security mechanisms found in Nokia series 60 Bluetooth-enabled mobile phones?
- How is it possible for intruders to gain access and manipulate Nokia series 60 mobile phones?
- What are the possible ways in filtering intentional and disturbing messages from unrecognized Bluetooth-enabled devices?
- In what way(s) can unauthorized access and manipulation be detected and prevented in Nokia series 60 mobile phones?

1.3 Objective of the Study

The study aimed to develop a security mechanism that addresses the security flaws found in Nokia series 60 Bluetooth-enabled mobile phones.

The proponents intended to accomplish the following objectives:

- Be familiar with Bluetooth's operation.

- Identify the existing security mechanism found in Bluetooth.
- Determine the ways on how Bluejacking and other similar attacks are done in Bluetooth-enabled mobile phones.
- Find out how intruders gain access to mobile phones allowing illicit data retrieval and manipulation.
- Look into the possible ways in filtering intentional and disturbing messages from unrecognized Bluetooth-enabled devices.
- Come up with ways on how data access and manipulation be detected and prevented.

1.4 Scope and Limitation of the Study

The study focused more on Bluetooth-enabled mobile phones particularly Nokia series 60 phones. The team aimed to resolve the problem of Bluejacking. Moreover, the most prominent glitch in Bluetooth security, which involved unauthorized access and manipulation, was dealt with.

A mobile software application was implemented to demonstrate how this security mechanism solved these Bluetooth security problems.

1.5 Significance of the Study

The study is significant to increase the security level of Bluetooth devices specifically in mobile phones without compromising its current networking capabilities. Hence, this will pave way for a more reliable and

effective security mechanism that Bluetooth-enabled mobile phones can utilize. The study conducted will benefit most users especially those who are currently dealing with Bluetooth vulnerabilities. Furthermore, the enhancement in Bluetooth security provides a way for Bluetooth developers and manufacturers to improve the current security mechanism employed in Bluetooth devices. Finally, this study will eventually help other researchers who would like to pursue further studies on the improvement of security mechanism found in Bluetooth devices particularly in mobile phones.

1.6 Definition of Terms

- Network Topology – The specific physical or logical arrangement of elements in a network.
- Framework – The software environment tailored to the needs of a specific domain.
- Platform – The type of computer or operating system on which a software application runs.
- Pairing – allows a user to have "trusted" connections between devices so that they can use each other's capabilities and services.
- Eavesdroppers – a secret listener to private conversations
- Unit Keys - a unit that uses a unit key is only able to use *one* key for all its secure connections. Hence, it has to *share* this key with all other

units that it trusts. Consequently all trusted devices are able to eavesdrop on any traffic based on this key.

- AES – automate encryption and signing.
- Snarfing – hacking or stealing information from another system or device.
- Bluejacking – the use of Bluetooth to send unsolicited messages to other devices.
- Passkey – the random numbers inputted for the pairing process.
- Firewall – a system designed to protect a device such as a computer from unauthorized access.
- Encryption – is the transformation of data into a form unreadable by anyone without a secret decryption key.
- Redfang – is a small proof-of-concept application to find non discoverable Bluetooth devices. This is done by brute forcing the last six (6) bytes of the Bluetooth address of the device and doing a read_remote_name().
- Symbian – Formerly Psion Software, Symbian is a joint venture between Psion, Ericsson, Nokia and Motorola to promote the EPOC operating system for wireless information devices. Symbian's main product is EPOC (derived from epoch – the beginning of an era), a 32-bit operating environment which has already been proven in the Psion Series 5 palmtop computer.