ANALYSIS AND IMPLEMENTATION OF SECURITY ALGORITHMS FOR WIRELESS COMMUNICATIONS

ABDINASIR HASSAN ALI

A project report submitted in partial fulfilment of the requirements for the award of the degree of Master of Computer Science (Information Security).

Centre for Advanced Software Engineering (CASE)
Faculty of Computer Science and Information Systems
Universiti Teknologi Malaysia

MARCH 2010

DEDICATION

Dedicated to my beloved parents, my supportive uncles, my beloved wife and all my friends who always beside me.

ACKNOWLEDGEMENT

I would like to express my deepest appreciation to my supportive and helpful supervisor Assoc. Prof. Dr. Maslin binti Masrom who sincerely helped me to complete this project. Her role of this research was a crucial part to produce this master thesis.

I would like to thank all CASE lecturers and managements who always happy to help you and to encourage to complete our study. Thanks to Dr. Rabiah Ahmad for her sincerely helping and patience.

I would like to thank my parents who supported me to study my master's degree and all my friends who always encourage me.

PUBLICATIONS

1. Conference Papers

- Analysis and Implementation of Security Algorithms for Wireless Communication. 2nd International Conference on Computer and Automation Engineering (ICCAE 2010), Feb. 26- 28, 2010, Singapore.

- Analysis of Security Algorithms for Cellular Wireless Communications. (Abstract accepted).
  2nd International Cryptology Conference (Cryptology 2010).
  29,30 June -1 July 2010, Melaka, Malaysia.

ABSTRACT

Wireless communication is the process of communicating information in electromagnetic media over a distance through the free space environment, rather than through traditional wired or other physical conduits. The secure provision of mobile computing and telecommunication services is rapidly increasing in importance as both demand and applications in order to provide a large number of advanced services to mobile users. The first generation of cellular mobile communications systems contained few if any security measures to protect the system operator and users. The second generation generally did a lot better, and contained entity authentication and confidentiality protection. Although this was a major improvement, security protection in the second generation left a lot to be desired in terms of key management and strong security algorithms. With the advent of third generation a (3G) mobile system a serious effort has been made to create consistent security architecture based on the threats and risks a 3G system faces. The basic security mechanisms are confidentiality, integrity, and availability. In the case of the wireless communications (as in many other networks), authentication, authorization, and access control are also the basic security mechanisms to be attained. The goal of this research is to propose the security mechanism of wireless communication to protect against any attack using technical approach that implements the authentication and encryption process.

ABSTRAK

Komunikasi tanpa wayar adalah proses komunikasi maklumat dalam media elektromagnet jarak jauh melalui persekitaran ruang bebas berbanding dengan komunikasi berwayar atau konduit fizikal lain. Kelengkapan selamat bagi pengkomputeran bergerak dan perkhidmatan telekomunikasi kian meningkat kepentingannya memandangkan permintaan dan aplikasi yang begitu banyak diperlukan oleh pengguna segerak. Generasi pertama system komunikasi kudah gerak selular mempunyai ukuran keselamatan bagi melindungi pengendali dan pengguna system. Generasi kedua umumnya mempunyai ukuran keselamatan yang lebih baik, pengesahan entiti dan perlindungan kerahsiaan. Walaupun ini merupakan penambahbaikan utama, perlindungan keselamatan pada generasi kedua daripada perspektif pengurusan kunci dan algoritma tahap keselamatan yang tinggi adalah lebih baik. Dengan kedatangan generasi ketiga (3G) satu usaha yang serius telah dibuat untuk mewujudkan seni bina keselamatan yang konsisten berdasarkan ancaman dan risiko yang dihadapi oleh 3G. Mekanisme-mekanisme keselamatan asas terdiri daripada kerahsiaan, integriti, dan kebolehsediaan. Dalam kes komunikasi tanpa wayar, pengesahan, kebenaran, dan kawalan akses juga merupakan mekanisme-mekanisme keselamatan asas yang perla dicapai. Matlamat kajian ini adalah untuk mencadangkan mekanisme keselamatan komunikasi tanpa wayar untuk melindungi sebarang serangan menggunakan pendekatan teknik yang melaksana proses pengesahan dan enkripsi.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF APPENDICES

CHAPTER 1

INTRODUCTION

1.1 Background of the problem

The secure provision of mobile computing and telecommunication services is rapidly increasing in importance as both demand and applications in order to provide a large number of advanced services to mobile users. The advantages of wireless communications are likely to see these technologies featured in up-coming third-generation mobile systems such as the Universal Mobile Telecommunications System (UMTS) and offering many new services that will revolutionize the way that society handles information. Security issues were not properly addressed in the first-generation analogue systems. With low-cost equipment, an intruder could eavesdropper user traffic or even change the identity of mobile phones to gain fraudulent service. Given this background, security measures were taken into account in the design of second- generation digital cellular systems. To prevent fraudulent use of wireless service, the Global System for Mobile (GSM) network authenticates the identity of a user through a challenge-response mechanism. The second-generation mobile communication standards adopt the symmetric-key cryptography between users and their home networks to establish session keys.

The third generation systems such as the Universal Mobile Telecommunications System (UMTS) and the international Mobile Telecommunications-2000 (IMT 2000) take advantage of many advanced security technologies, especially public key cryptography (Bais, A. et al., 2006). Advantages of public-key based technique are effective within large and complex communication networks including scalability, easier key management and the lack of need for on-line server. But, low speed is usually unacceptable in practice and prevents the public key cryptography being widely deployed onto most of the applications running on lower-power wireless device.

1.2 Statement of the Problem

Security of wireless communication is extremely difficult and challenging because of facing more complicated environments compared with conventional wired networks. For instance, wireless communication could be disturbed by radio wave and thunderstorms or blocked by physical objects like mountains or skyscrapers. Even worse, high mobility coupled with a variety of explosively increased users makes existing security policies in wireless communication inefficient or even useless, meaning that wireless communication can be easily attacked by computer viruses, worms, spy wares, and similar threats.

These security threats cause downtime or continual patching in wireless communication and thus lead to severe disruption in wireless commercial business. Therefore, boosting security of wireless networks has become one of the most important issues in the arena of wireless communications. Wireless communications is taking over more and more and makes by no means difference between different application areas. Thus authentication and encryption of data are the areas like current interest, quality and security in evident focus. We are interested in

vulnerabilities that come with wireless communications and mobility and how they are related to threats and risks.

1.3 Research Questions

1. Why is security of wireless communication important?
2. Can we use wireless technology without implementing any security algorithms?
3. What is the significant of third generation wireless communication over the second generation?

1.4 Aim of the Project

The aim of this project is to propose and implement the security for wireless communication by analyzing their security algorithms based on second and third generations of wireless communications.

1.5 Objectives

1. To investigate different threats and the algorithms to counter these threats in wireless communication.

2. To examine the mechanism required to provide the security algorithms for wireless communications.
3. To compare the existing security algorithms between second generation and third generation wireless communication.
4. To propose and test the authentication and encryption process for wireless communications (GSM).

1.6 Scope of the Study

This project focuses on the comparison of security algorithms among wireless communication. In general, there are different types of wireless communication in today`s world, for example; (1) 2nd generation wireless technology which is known as Global System for Mobile Communication (GSM) and, (2) 3rd generation (UMTS) the Universal Mobile Telecommunications System. The project will focus on above two mentioned security algorithms for wireless communication, because of their popularity of uses and this is done by implementing the authentication and encryption process and comparing the security features between them.

1.7 Significance of the Study

Wireless communications security is an area of crucial importance to telecommunications industry, where authentication and data encryption are the major concern. Wireless communications devices are proliferating throughout the world and can pose significant security risks to national security and the wireless networking infrastructures if not properly implemented. Since wireless technology has emerged there has been an increased demand in the use of wireless

communications devices. With the demand, wireless communications also become a major source of new vulnerabilities. Related security solutions are being developed to address the new vulnerabilities. Wireless communication weaknesses are on the increase due to emergence of advanced services, because of need of proper authentication, and the large deployment of mobile technologies. This has created challenging issues in the security of wireless systems and applications operating in wireless environments. The significance issue is to seek for the development of new techniques, models and theories that help for a better protection of the mobile and wireless communication systems; assess and enhance the level of security of the current wireless communication systems, services and networks.

1.8 Summary

This chapter has presented and overview of wireless communications problem background, problem statement and objectives of this project which lead to implement the authentication and encryption process for wireless communications. It has also discussed the scope and the aim of this project; finally it has covered the significant of the project.