Evaluation of Direct and Indirect Authentication Mechanisms in Mobile Networks

Dissertation

Submitted to:

Central Department of Computer Science and Information Technology,

Institute of Science and Technology

Tribhuvan University, Kirtipur, Nepal.

In Partial Fulfillment of the Requirements for the Degree of

Master of Science in Computer Science and Information Technology

Submitted by:

Deependra Prasad Bhatt

December, 2013

Tribhuvan University

Institute of Science and Technology

Central Department of Computer Science and Information Technology

Date: …….

Recommendation

I hereby recommend that the dissertation prepared under my supervision by **Mr. Deependra Prasad Bhatt** entitled **"Evaluation of Direct and Indirect Authentication Mechanisms in Mobile Networks"** be accepted as fulfilling in part requirements for the degree of Masters of Science. In my best knowledge this is an original work in computer science.

……

Mr. Jagdish Bhatta
Lecturer,
Central Department of Computer
Science and Information Technology,
Tribhuvan University, Nepal

(Supervisor)

LETTER OF APPROVAL

We certify that we have read this dissertation and in our opinion it is fully adequate and satisfactory, in scope and quality, as a dissertation in the partial fulfillment of Master Degree in Computer Science and Information Technology.

Date: …….

Evaluation Committee

.....	……
Assistant Prof. Nawaraj Paudel	Mr. Jagdish Bhatta
Head,	Lecturer,
Central Department of Computer Science and Information Technology,	Central Department of Computer Science and Information Technology,
Tribhuvan University, Nepal	Tribhuvan University, Nepal
(Head)	**(Supervisor)**
.....	……..
(Internal Examiner)	**(External Examiner)**

Acknowledgements

Foremost, I would like to express my sincere gratitude to my respected teacher and dissertation supervisor Mr. Jagdish Bhatta, Lecturer, Central Department of Computer Science and Information Technology (CDCSIT), Tribhuvan University for his excellent guidance, continuous help and support in all stages of this study.

I would also like to thank respected Head of Central Department of Computer Science and Information Technology, Asst. Prof. Nawaraj Paudel for his kind help, encouragement and constructive suggestions.

My sincere thanks goes to all respected teachers Prof. Dr. Shashidhar Ram Joshi, Prof. Dr. Subarna Shakya, Prof. Sudarshan Karanjeet, Asst. Prof. Min Bahadur Khati, Mr. Bishnu Gautam, Mr. Dinesh Bajracharya, Mr. Arjun Singh Saud, Mrs. Lalita Sthapit, Mr.Yog Raj Joshi, Mr. Bikash Balami and all others for granting me broad knowledge, inspiration and motivation during my study and during the academic period.

I thank my friends Lok Prakash Pandey, Rajendra Lamichhane, Prakash Bhatt, Bishnu Rawal, Harendra Bist and Ashok Kumar Pant for supporting me in this work. I extend my thanks to my brothers Jagdish Prasad Bhatt, Krishna Prasad Bhatt, Manoj Prasad Bhatt and sister Debaki Bhatt for their help and support during this study.

Finally, I would like to thank my family members for their continuous love, care and their supports in my decisions and encouraging me with their best wishes.

Deependra Prasad Bhatt

December, 2013

Abstract

The rapid progress in wireless mobile communication technology and personal communication systems has prompted new security questions. Typically, mobile networks are deployed in un-trusted environments. In mobile network there is unrestricted mobility and information access between unacquainted nodes and server occurs frequently from anywhere, anytime. In such conditions keeping the security and privacy of information from accessing illegally by any invalid user node is a big concern. The sharing of data and information between various parties from different locations through insecure channel is quite general. The vast majority of internet users are concerned about the safety of their secret information and personal details from being accessed by unauthorized entities. So, before sharing the secure and sensitive data, information and providing access to various resources, the identification of the intended or claimed entities is one of the major essential factors for any secure communication system. Cryptosystem is an important technique to identify the authenticity in order to protect the confidential and sensitive data in case of mobile networks. There are some direct and indirect authentication schemes that are based on different cryptographic systems such as RSA, ECC etc and some are based on the modified versions of Kerberos assisted authentication scheme. The selection of an efficient authentication scheme plays an important role in case of mobile networks where devices are resource constrained in nature. In this context, this study focuses on the implementation and analysis of computational cost of ECC based direct authentication, ECC based indirect authentication, RSA based direct authentication, RSA based indirect authentication, Kaman authentication mechanism and Chang Cheng's authentication mechanism so as to select the best authentication system for resource constrained devices in mobile network.

Table of Contents

Chapter 3

Chapter 4

List of Figures

List of Tables

List of Listings

List of Abbreviations

AES	Advanced Encryption Standard
ANSI	American National Standards Institute
AP	Authentication Problem
API	Application Programming Interface
AS	Authentication Server
BC	Bouncy Castle
CA	Certification Authority
CDC	Connected Device Configuration
CLDC	Connected Limited Device Configuration
CPU	Central Processing Unit
CRT	Chinese Remainder Theorem
DES	Data Encryption Standard
DH	Diffie-Hellman
DLP	Discrete Logarithm Problem

DSA	Digital Signature Algorithm
EC	Elliptic Curve
ECC	Elliptic Curve Cryptography
ECDLP	Elliptic Curve Discrete Logarithm Problem
ECDSA	Elliptic Curve Digital Signature Algorithm
GF	Galois Field
IDE	Integrated Development Environment
IFP	Integer Factorization Problem
ISO	International Organization for Standardization
J2EE	Java 2 Enterprise Edition
J2ME	Java 2 Micro Edition
J2SE	Java 2 Standard Edition
MIDP	Mobile Information Device Profile
MS	Main Server
NIST	National Institute of Standards and Technology

PDA	Personal Digital Assistant
PIN	Personal Identification Number
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RC	Registration Center
RA	Registration Authority
RSA	Rivest-Shamir-Adleman
SEC	Standards for Efficient Cryptography
SECG	Standards for Efficient Cryptography Group
SSL	Secure Socket Layer
SP	Service Provider
TLS	Transport Layer Security
TM	Trademark