

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
Head,
Central Department of Computer
Science and Information Technology,
Tribhuvan University, Nepal

(Head)

.....

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

(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 untrusted 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

Description	Page No.
Abstract	i
Acknowledgements	ii
Table of Contents	iii
List of Figures	vi
List of Tables	vii
List of Listings	viii
Abbreviations	ix
Chapter 1	
1. Introduction	1
1.1. Objective	2
1.2. Thesis Organization	2
Chapter 2	
2. Problem Definition and Background Study	4
2.1. Problem Definition	4
2.2. Background Study	5
2.2.1. Cryptographic System and Secure Communication	5
2.2.2. Authentication Using Public Key Cryptography	7
2.2.3. RSA Public Key Cryptography	8
2.2.4. Elliptic Curve Cryptography	9
2.2.4.1. Group Law of EC Group of Points	10
2.2.4.2. Multiplication over an EC Group	12
2.2.5. Finite Fields: GF (p)	12
2.2.6. Mobile Network	13
2.2.7. Authentication	13

2.2.7.1. Direct Authentication	15
2.2.7.2. Indirect Authentication	15
2.2.8. Authentication Factors	15
2.2.9. Authentication Functions	16
2.2.9.1 Hash Functions	16
2.2.10. Certificate Distribution	17
Chapter 3	
3. Literature Review	18
3.1. ECC Based Authentication	19
3.1.1. ECC Based Direct Authentication	19
3.1.2. ECC Based Indirect Authentication	21
3.2. RSA Based Authentication	23
3.2.1. RSA Based Direct Authentication	24
3.2.2. RSA Based Indirect Authentication	25
3.3. Kaman Authentication Mechanism	27
3.4. Chang-Cheng's Authentication Mechanism	28
Chapter 4	
4. Implementation and Testing	31
4.1. Java™ 2 Micro Edition Overview	31
4.2. Third Party Lightweight Crypto API	32
4.3. Development & Emulation Environment: NetBeans Overview	33
4.4. Implementation Details	33
4.4.1. Implementation Details of ECC Based Direct Authentication	34
4.4.2. Implementation Details of ECC Based Indirect Authentication	35
4.4.3. Implementation Details of RSA Based Direct Authentication	37
4.4.4. Implementation Details of RSA Based Indirect Authentication	38
4.4.5. Implementation Details of Kaman Authentication Mechanism	39
4.4.6. Implementation Details of Chang-Cheng's Authentication Mechanism	41

4.5. Sample Test Cases	43
Chapter 5	
5. Analysis	46
5.1. Empirical Analysis	46
5.1.1. Authentication Code Generation and Authentication Verification	
Time Analysis for Key size in bits 192 / 1536	47
5.1.2. Authentication Code Generation and Authentication Verification	
Time Analysis for Key size in bits 224 / 2048	48
5.1.3. Authentication Code Generation and Authentication Verification	
Time Analysis for Key size in bits 256 / 3072	49
5.2. Final Result	50
Chapter 6	
6. Conclusion and Future Work	52
6.1. Conclusion	52
6.2. Recommendation	52
References	54
Appendix	59

List of Figures

Figure 2.1: Geometric addition of elliptic curve points, $P+Q=R$	11
Figure 2.2: Geometric doubling of elliptic curve point, $2P=R$	11
Figure 3.1: Protocol flow of ECC based direct authentication	20
Figure 3.2: Protocol flow of ECC based indirect authentication	22
Figure 3.3: Protocol flow of RSA based direct authentication	25
Figure 3.4: Protocol flow of RSA based indirect authentication	26
Figure 3.5: Protocol flow of Kaman authentication mechanism	28
Figure 4.1: Java™ and J2ME™ Technologies	32
Figure 5.1: Graph shows authentication code generation and authentication verification time for key size in bits 192 / 1536 for specified algorithms.	47
Figure 5.2: Graph shows authentication code generation and authentication verification time for key size in bits 224 / 2048 for specified algorithms	48
Figure 5.3: Graph shows authentication code generation and authentication verification time for key size in bits 256 / 3072 for specified algorithms	49

List of Tables

Table 5.1: Authentication Code Generation and Authentication Verification Time (in milliseconds) for key size in bits 192 / 1536	47
Table 5.2: Authentication Code Generation and Authentication Verification Time (in milliseconds) for key size in bits 224 / 2048	48
Table 5.3: Authentication Code Generation and Authentication Verification Time (in milliseconds) for key size in bits 256 / 3072	49

List of Listings

- Listing 4.1:** Java code to perform auth verification in ECC based direct authentication 35
- Listing 4.2:** Java code to perform auth verification in ECC based indirect authentication 36
- Listing 4.3:** Java code to perform auth verification in RSA based direct authentication 38
- Listing 4.4:** Java code to perform auth verification in RSA based indirect authentication 39
- Listing 4.5:** Java code to perform auth verification in Kaman based authentication 41
- Listing 4.6:** Java code to perform auth verification in Chang-Cheng's Auth Mechanism 43

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