**LTE/SAE Security Issues on 4G Wireless Networks**

A Project Report submitted in partial fulfillment of the requirements for the

Award of the Degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE AND ENGINEERING

Submitted by:

Akshita M.V.V.S (1210312104) K.Sai Kishan (1210312122)

K.Srilekha Reddy (1210312125) Aditya Patri (1210312103)

Under the Esteemed guidance of

**S.K.RAGHU**

Assistant Professor

****

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

GITAM INSTITUTE OF TECHNOLOGY

GITAM UNIVERSITY

VISAKHAPATNAM - 530 045

(2012-2016)

GITAM INSTITUTE OF TECHNOLOGY

GITAM UNIVERSITY

VISHAKAPATNAM - 530045

(2012-2016)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

****

**CERTIFICATE**

This is to certify that the project report entitled LTE/SAE SECURITY ISSUES ON 4G WIRELESS NETWORKS is a bonafide record of the work carried out by **AKSHITA M.V.V.S, K. SAI KISHAN, K. SRILEKHA REDDY, ADITYA PATRI** submitted to the Department of Computer Science and Engineering, GIT, GITAM University, Visakhapatnam during the year 2015-2016, for the fulfilment of Project Phase-2.

**Head of the department Project Guide**

Dr. P.V.NAGESWAR RAO (Ph.D.)S.K. Raghu

Head of the Department Assistant Professor

Department of CSE Department of CSE

Gitam institute of technology Gitam institute of technology

GITAM UNIVERSITY GITAM UNIVERSITY

**ACKNOWLEDGEMENTS**

Final year project is an integral part of any under graduation. The knowledge gained by oneself is immense in an industry. I am very happy that I was given this opportunity to do the project under the guidance of Mr. S.K. Raghu, Assistant Professor.

During the course of this project work, our project guide was prudent. Without his help, always generally and unstintingly given, the completion of this project would have been immeasurably more difficult.

Firstly, I would like to thank my internal examiners Mr. A.S.VENKATA PRANEEL, Assistant professor and Dr. G.LAKSHMEESHWARI, Assistant Professor for their stimulating guidance and profuse assistance. I shall always cherish my association with them for their guidance, encouragement and valuable suggestions throughout the progress of this work. We consider it a great privilege to work under their guidance and constant support.

We would like to thank our project guide Mr. S.K. Raghu for his prolific assistance and always kindled us with his support. His suggestions have been invaluable to us during the course of our project and we always revere working with him.

Our sincere thanks to Dr. P.V.NAGESWAR RAO Ph.D., Honourable Head of the Department, Computer Science Engineering for inspiring us to learn new technologies and tools. Finally I adjudge to thank one and all who helped us directly and indirectly while we were through this project.

Akshita M.V.V.S (1210312104)

K. Sai Kishan (1210312122)

K. Srilekha Reddy (1210312125)

Aditya Patri (1210312103)

**DECLARATION**

We, hereby declare that this is an original work done for the department of Computer Science Engineering, GITAM Institute of Technology, GITAM UNIVERSITY, Visakhapatnam.

I am assuring that this report has not been submitted in any other University or college.

Akshita M.V.V.S - 1210312104

K.Sai Kishan - 1210312122

K.Srilekha Reddy-1210312125

Aditya Patri - 1210312103

**ABSTRACT**

**SECURITY ANALYSIS OF HANDOVER KEY MANAGEMENT IN 4G LTE/SAE NETWORKS**

The recent expansion of wireless network technologies and the emergence of novel applications such as mobile TV, Web 2.0, and streaming content have led to the standardization of the (pre-4G) Long-Term Evolution (LTE) protocol to become operational with the 3rd Generation Partnership Project (3GPP).The 3GPP has also begun the study of the standard’s future development, called System Architecture Evolution (SAE), set to evolve into the new era of 4G.

By looking at the authentication and ciphering algorithms, such as EAP-AKA (Extensible Authentication Protocol for Authentication and Key Agreement), currently operating within the LTE protocol, we analyze several vulnerabilities in LTE/SAE security architecture; specifically, insecure AKA key derivation procedures and the lack of fast re-authentications during handovers. One of the unique challenges of fourth-generation technology is how to close a security gap through which a single compromised or malicious device can jeopardize an entire mobile network because of the open nature of these networks. Handover key management in the 3GPP LTE/SAE has been designed to revoke any compromised key(s) and as a consequence isolate corrupted network devices.

This paper, however, identifies and details the vulnerability of this handover key management to what are called desynchronization attacks; such attacks jeopardize secure communication between users and mobile networks. Although periodic updates of the root key are an integral part of handover key management, our work here emphasizes how essential these updates are to minimizing the effect of desynchronization attacks that, as of now, cannot be effectively prevented.

Table of Contents

1. Introduction..........................................................................................................................1
2. Literature Review.................................................................................................................4
3. System Analysis..................................................................................................................10
   1. Existing System............................................................................................................10
      1. LTE/SAE 4G Network Security Architecture..................................................10
      2. LTE/SAE 3G Cryptographic Algorithms.........................................................11
   2. Problems with Existing System....................................................................................12
   3. Proposed System...........................................................................................................12
   4. Security Enhancements in LTE/SAE Standard............................................................13
4. System Requirements..........................................................................................................14
   1. Hardware Requirements................................................................................................14
   2. Software Requirements.................................................................................................14
5. Overview of Technologies and Tools…………..................................................................15
   1. Java................................................................................................................................15
      1. Java Programming Language……………………………….…….…………..15
      2. The Java Platform……………………………………………..………………16
      3. Networking TCP/IP Stack…………………………………….……………....16
      4. Sockets………………………………………………………….……….…….17
      5. Addresses………………………………………………………….…….……18
   2. Eclipse Luna IDE…………………………………………………………….……….19
6. System Modelling………....................................................................................................21
   1. Data Flow/Use Case/Flow Diagrams…………………………………….…………...21
   2. Notation………………………………………………………………….……………21
   3. Modelling Rules………………………………………………………….………...…22
   4. Architectural Diagram…………………………………………………..…………….23
   5. Dataflow Diagrams………………………………………………………..…………..24
   6. UML Diagrams…………………………………………………………..……………26
7. Implementation…...............................................................................................................29
   1. EPS-AKA…………………………………………………………………………….29
   2. Algorithm-Advanced Encryption Standard (AES)…………………………………...30
   3. Modules……………………………………………………………………………….31
      1. Server-Client Module………………………………………………………...32
      2. Optimal Key Management…………………………………………………....33
      3. Authentication Key Agreement……………………………………………....33
      4. Long-Term Evolution Security……………………………………………….34

1. System Study......................................................................................................................36
   1. Feasibility Study……………………………………………………………………..36
      1. Economic Feasibility........................................................................................36
      2. Technical Feasibility.........................................................................................36
      3. Social Feasibility...............................................................................................37
2. Sample Source Code…........................................................................................................38
   1. Key Generator………………………………………………………………………..38
   2. Available Nodes……………………………………………………………………...43
   3. Encrypt/Decrypt…...…………………………………………………………………46
3. Screenshots........................................................................................................................48
4. System Testing…………………………………………………………………………...56
   1. Types of Tests……………………………………………………………………56
   2. Test Cases………………………………………………………………………..59
5. Conclusion…………………………………………………………………………….....60
6. References……………………………………………………………………………......61