

INTERNET-DRAFT  
Intended Status: Standards Track  
Expires: February 11, 2019

Naresh Kumar  
NIT Delhi  
K.Verma  
NIT Delhi

August 11, 2018

Security for 5G  
draft-naresh-kitten-security-for-5g-00.txt

## Status of this Memo

This Internet-Draft is submitted to IETF in full conformance with the provisions of [BCP 78](#) and [BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/lid-abstracts.html>

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>

## Copyright and License Notice

Copyright (c) 2018 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to [BCP 78](#) and the IETF Trust's Legal Provisions Relating to IETF Documents (<http://trustee.ietf.org/license-info>) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

INTERNET DRAFT

Security for 5G

August 11, 2018

## Abstract

This document proposes a new method which provides the capability to resolve issue of attack over Mobile Communication System. This document assumes that the reader is familiar with some concepts and details regarding Authentication and Encryption in generations of Mobile Telephony.

## Table of Contents

|                    |                                     |                   |
|--------------------|-------------------------------------|-------------------|
| <a href="#">1</a>  | Introduction . . . . .              | <a href="#">3</a> |
| <a href="#">2</a>  | Vulnerability Description . . . . . | <a href="#">3</a> |
| <a href="#">3</a>  | Terminology . . . . .               | <a href="#">3</a> |
| <a href="#">4</a>  | General Scenario . . . . .          | <a href="#">3</a> |
| <a href="#">5</a>  | Solutions of these issues . . . . . | <a href="#">4</a> |
| <a href="#">6</a>  | IANA Considerations . . . . .       | <a href="#">5</a> |
| <a href="#">7</a>  | Security Considerations. . . . .    | <a href="#">5</a> |
| <a href="#">8</a>  | Conclusions . . . . .               | <a href="#">6</a> |
| <a href="#">9</a>  | References . . . . .                | <a href="#">6</a> |
| <a href="#">10</a> | Acknowledgements . . . . .          | <a href="#">7</a> |
|                    | Authors' Addresses . . . . .        | <a href="#">7</a> |

INTERNET DRAFT

Security for 5G

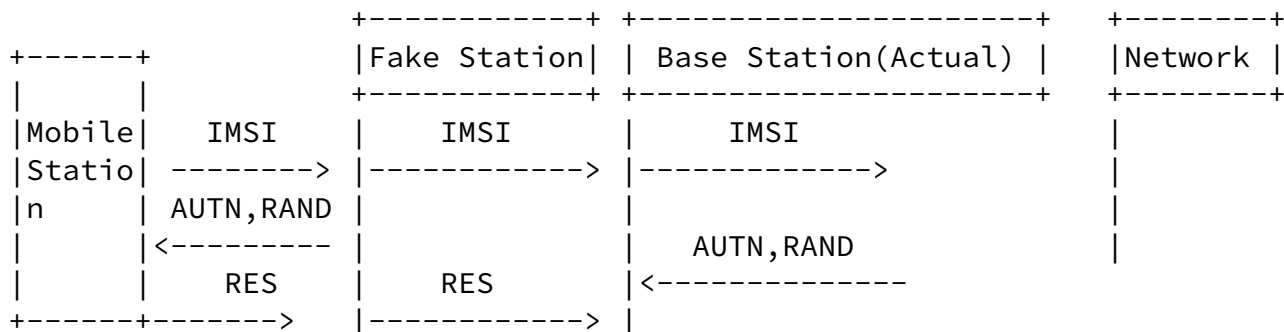
August 11, 2018

1 Introduction

In Mobile Communication,IMSI catching is the major issue today. In order to encrypt or decrypt data between Mobile Station and Base Station,various algorithms are implemented by generating keys required to provide confidentiality and integrity.

2 Vulnerability

Initially whenever UE attaches for the first time[3], it sends the IMSI to MME in clear text which is sent from MME to eNodeBs and from eNodeBs to UEs.An attacker can request without awareness of the user by using various social engineering tools and then trace messages between eNodeB and UE to decode them and fetch the IMSI . There is also another Fault that occurs whenever re-synchronisation occurs at the time of handover because at that time also, IMSI is sent in plaintext that can easily be sniffed by attacker.



3 Terminology

Refer 9.2[2] for better visualisation

3.1 IMSI: An international mobile subscriber identity is a unique number usually fifteen digits, associated with Global System for Mobile Communications i.e GSM and Universal Mobile Telecommunications System UMTS network mobile phone users. The IMSI is a unique number identifying a subscriber

3.2 AUTN: Authentication Token

3.3 MME : Mobility Management Entity,Handling all management like handover etc

3.4 HSS : Home Subscriber Server–User USIM Company

3.5 AAA :Authentication,Authorisation,accounting

3.6 C1,C2 : Ciphertexts

4 General Scenario

Normally in all advanced generations,excluding 1G/2G of Mobile

Communications "AUTHENTICATION AND KEY AGREEMENT(AKA)PROTOCOL" steps are applied for Mutual Authentication:

1. Mutual authentication between the network and UE.
2. Deriving keys for confidentiality and integrity protection.
3. confidentiality, integrity among various Entities like core network
4. Temporary identity like GUTI are used to hide IMSI

Now there are various Algorithms like in 9.1[1],[2] that can be applied in SIM and MME to generate the RES(Response),AUTN that includes sequence number etc in order to get the keys that help to verify each other identity and thus are required to encrypt the data for secure communication.This same procedure can be applied to 5G system.

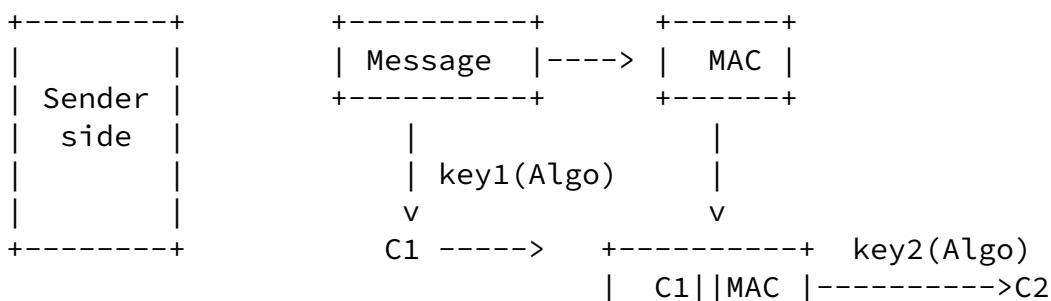
5 Solutions of these issues

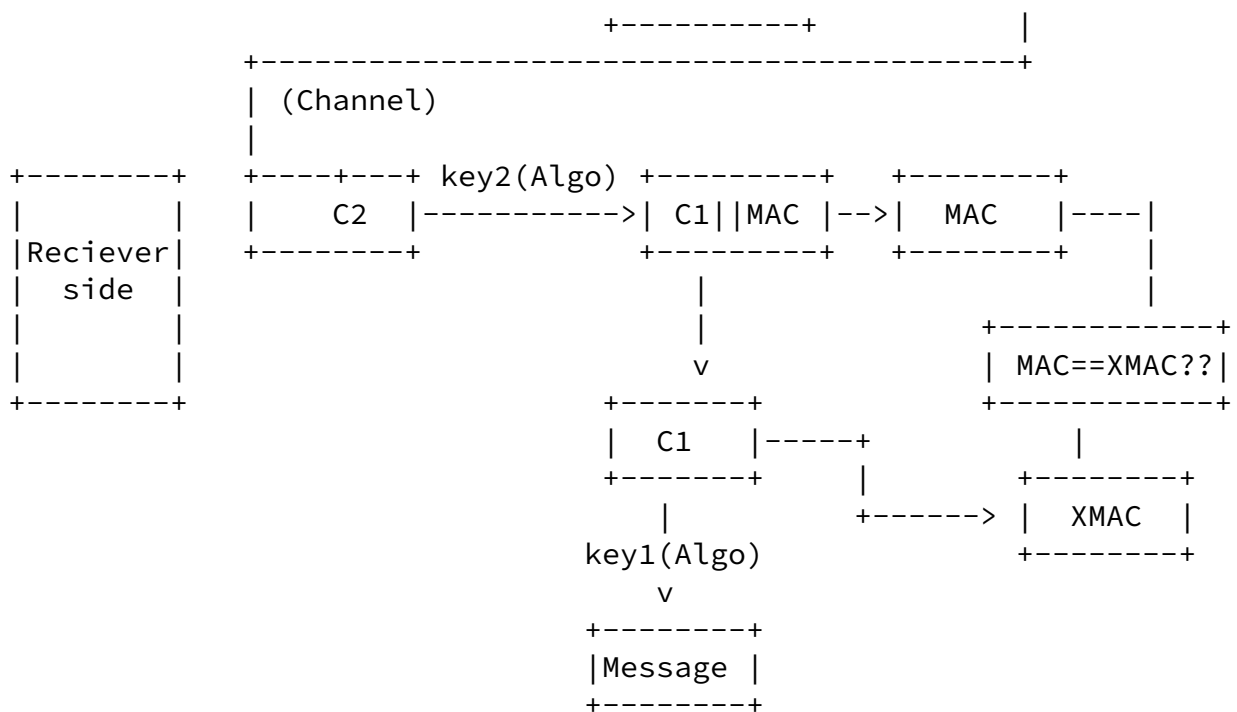
Now there are two methods to achieve protection against the attacker regarding IMSI catching:

5.1 We can use Public key Cryptosystem in order to encrypt IMSI to reduce problem of IMSI Catching and that particular algorithm which has been used to encrypt is confidential only to the UE and gNodeB Mobile station for 5G

5.2 Every time a mobile SIM try to connect Base Station, it should use a pseudonym IMSI that will be updated in both the station(Home Server as well as Mobile SIM) and there will be checking for all updations that will lead to provide Both Authenticity and Confidentiality. So each time user will get the new updated IMSI and will be identified by this Identity only.

Now coming to the main Method(Public key Cryptosystem)we have implemented various algorithms based on following scheme keeping the message constant:





According to the diagram, Message confidentiality and Authenticity is achieved using MAC(Message Authentication code)see[RFC 6476]. We have implemented three algorithms(Blowfish[],AES[RFC 3962])

Implemented Algorithms and their results:

| PARAMETERS        | FERNET(AES-128) | AES           | BLOWFISH                    |
|-------------------|-----------------|---------------|-----------------------------|
| KEY LENGTH (Bits) | 128             | 128,192, 256  | Variable key length(32,448) |
| ROUNDS            | 10,12,14        | 10,12,14      | 16                          |
| LEVEL OF SECURITY | Medium Security | Highly Secure | Excellent Security          |
| ENCRYPTION SPEED  | Moderate        | Faster        | Very fast                   |
| TIME(s)           | 0.004000        | 0.004003      | 0.004008                    |

## 6 IANA Considerations

Nil

## 7 Security Considerations

For solutions we have already described in [section 5](#) We can use different algorithms at different positions like at the time of generation of cipher C1 or C2 etc. There is no restriction over its sequence. We are considering that the keys have already been exchanged or already fixed in the center server's database corresponding to the particular SIM. for more details on architecture you can see 9.2[1]

Naresh Kumar, K.Verma Expires February 11,2019

[Page 5]

---

INTERNET DRAFT

Security for 5G

August 11, 2018

## 8 Conclusions

This document is mainly focussed over the major vulnerability of Mobile Generations in the form of IMSI transmission in plaintext. We can not only encrypt this confidential information but other details can also be secured. This can be effective in upcoming 5th Generation also.

## 9 References

### 9.1 Normative References

[RFC 6476] Errata Exist,P. Gutmann "Using Message Authentication Code (MAC) Encryption in the Cryptographic Message Syntax (CMS)"

[RFC 3962] K.Raeburn "Advanced Encryption Standard (AES) Encryption for Kerberos 5"

### 9.2 Informative References

- [1] <https://portal.3gpp.org/desktopmodules/Specifications/SpecificationDetails.aspx?specificationId=3144>.
- [2] E. Dahlman, S. Parkvall, J. Skold, 4G: LTE/LTE-advanced for mobile broadband, Academic, 2013.
- [3] <https://ieeexplore.ieee.org/document/7397256/>

INTERNET DRAFT

Security for 5G

August 11, 2018

## 10 Acknowledgements

This document is prepared for M. Tech 2nd year Major Project in National Institute of Technology, Delhi.

### Authors' Addresses

Naresh Kumar  
M. Tech Student  
Department of Computer Science & Engineering  
National Institute of Technology, Delhi  
Narela, Delhi-110040,INDIA

Phone: +91- 8839338318  
EMail: 172211007@nitdelhi.ac.in

Karan Verma  
Assistant Professor  
Department of Computer Science & Engineering  
National Institute of Technology, Delhi  
Narela, Delhi-110040,INDIA

Phone: +91-7568169258  
EMail: karan.verma.phd@gmail.com