MEE 09:27

SWOT Analysis of IP Multimedia Sub System Security Authentication Schemes

Master of Electrical Engineering with emphasis in Telecommunication

Author(s):

Syed Majid Ali Shah Bukhari
E-mail: syedmaji@hotmail.com

Inayat Ullah Khan
E-mail: inayat4ur@hotmail.com

28th May, 2009

University Supervisor:

Charlott Eliasson
Department of Telecommunication

University Examiner:

Markus Fiedler
Department of Telecommunication

Department of Electrical Engineering
School of Engineering
Blekinge Institute of Technology
SE – 37 79 Karlskrona
Sweden

Internet : www.bth.se/tek
Phone : +46 457 38 50 00
Fax : + 46 457 279 14

Abstract

SWOT analysis is performed on IMS security authentication schemes to demonstrate the effectiveness of each schemes in terms of multiple parameters and associated dependencies for users and network operators. Due to SWOT tool we have been able to describe strengths, weakness, opportunities and threats in each authentication scheme separately. The analysis performed mostly based on the state of art studies, SWOT tool itself approximates authentication schemes but in the discussion chapter we illustrated clearly what is necessary to adopt individually between Non SIM and SIM base authentication schemes. It will help MOBICOME project and network operators to choose the most appropriate authentication technology/ technologies for design and implementation.

Acknowledgement

Our great love and appreciation is for our families who always encourage us, strengthen our weakness and blessed us with the prayers to ALLAH.

We highly acknowledge the help and support during the entire research study of our thesis supervisor Charlott Eliasson and examiner Markus Fielder at Department of Telecommunication Systems, Blekinge Tekniska Högskola (BTH), Sweden.

Our supervisor extremely assisted us with knowledge of report writing and structuring skills to be able to produce the thesis report in time and accurate manner.

We are thankful to Mikeal Åsman and Lena Magnusson their continuous help, support and guidance throughout our master degree.

LIST OF CONTENTS

List of Abbreviations

Acronym	Description
3GPP	3 Generation Partnership Project
AV	Authentication Vector
AUTN	Authentication Token
BSS	Base Station Controller Base
BTS	Base Transceiver Station
CDMA	Code Division Multiple Access
CPN	Customer Premises Network
CSCFs	Call Session Control Functions
CPE	Customer Premises Equipment
CK	Confidentiality Key
DOS	Denial Of Service
EDGE	Enhanced Data Rates for GSM Evolution
EEPROM	Electronically Erasable Programmable Read Only Memory
FQDN	Fully Qualified Domain Name
FMC	Fixed Mobile Convergence
GPRS	General Packet Radio Service
GGSN	Gateway GPRS support node
GTP	GPRS Tunneling Protocol
HSS	Home Subscriber Server
HTTP	Hypertext Transfer Protocol
IMS	IP Multimedia Subsystem
ISIM	IP Multimedia Services Identity Module
IMSI	International Mobile Subscriber Identity
ICT	Information Communication and Technology
I-CSCF	Interrogating Call Session Control Function
IMPI	IMS Private User Identity
IMPU	IMS Public User identity
ISDN	Integrated Services Digital Network
IRG	Internet Residential Gateway
IK	Integrity Key
MSC	Mobile service Switching Centre
MSISDN	Mobile Station International ISDN Number
MAC	Media Access Control
NASS	Network Attachment Sub System
NIC	Network Interface Card
NIST	National Institute of Standard and Technology
P-CSCF	Proxy Call Session Control Function
PDP	Packet Data Protocol
RAND	Random Number
RG	Residential Gateway
RARP	Reverse Address Resolution Protocol
RAN	Radio Access Network
S-CSCF	Serving Call Session Control Function
SSO	Single Sign On
SWOT	Strengths, Weaknesses, Opportunities, and Threats
SIM	Subscriber Identity Module
SIP	Session Initiation Protocol
SGSN	Serving GPRS Support Node
TISPAN	Telecommunications and Internet converged Services and Protocols for Advanced Networking
UICC	Universal Integrated Circuit Card
USIM	Universal Subscriber Identity Module
UE	User Equipment
UMTS	Universal Mobile Telecommunications System
UA	User Agent
VLR	Visitor Location Register
WIMAX	Worldwide Interoperability for Microwave Access
XRES	Expected Response

Authentication is the mechanism of permitting users to access service by authorizing and registering them to system; IMS authentication employs same procedure with its predefined set for call session control functions (CSCF's) and HSS database maintaining user profiles. Due to the nature of IMS, IMS can be deployed in GPRS, UMTS, LTE (future), WIMAX, etc. easily and users means to IMS access are authenticated through UICC cards in the mobile devices. Non SIM phenomenon will be utilized to access IMS network outside of the above network access scopes. Furthermore, two authentication categories in IMS access i.e. SIM base and Non SIM base have different procedures i.e. algorithms to authenticate with the IMS system that can be analyzed through numerous access parameters define in SWOT as security, simplicity, complexity, usability, user friendliness, dependability, costly, efficiency, technology, standards, etc latter in chapter 5 and chapter 6.

1.1 Problem definition/Goals:

Thesis work requires encompassing SWOT analysis of IMS access security authentication schemes. Mainly evaluation dilemma caters information pertains to SWOT analysis to overwhelm and determine IMS authentication schemes categorized in Non- SIM and SIM base authentication. "MOBICOME" is a project of Mobile/ Fixed Convergence in Multi Access Environments and aims to identify different IMS authentication schemes for harmonizing control by extending seamless access feasible. The thesis report is preliminary project requirement to address the most subsequent authentication scheme/s selection in both authentication access categories (SIM and Non SIM) for design and implementation. Our current technologies use multiple security authentication techniques at different area and level of access. IMS is an emerging technology for providing seamless access and services provisions at higher level of security, reliability, and robustness. There is an access mechanism in IMS that provides facilities to all the user equipments to authenticate but with different mode/level of security depending upon the network. Furthermore, aim of the study leads criticizing and praising comprehensions for decision makers to establish and choose the most appropriate authentication technology to access IMS network in terms of security, simplicity, complexity, user friendliness, etc.

1.2 Motivation:

We are dealing with an internet through various access platforms and for multiple application services. Internet is an open gateway for and to us; our access is critical to our social life and sometimes unlimited to others. An increase in the information communication and technology (ICT) and IP evolution attract us to purely immerse and utilized telecommunication services composed of high quality and rich service delivery. IP multimedia services not only facilitates and brings our everyday life at single sign on and the freedom to relocate the seamless access is few steps ahead of what we can see, these great deals of easy access mechanism generates multiple problems for us. User information and data security/integrity are highly obstructed through easy access mechanisms. How and what path does invader will opt to reach us is undefined. It's quite sophisticated to stop everything associated with us directly by simply refusing any of the services than to find appropriate measures to halt unwilling intruders lying to our next doors even permitting ourselves with emerging technology facilities.

1.3 Research Questions

We have developed some logical questions for research study which will answer by SWOT analysis study.

- How to identify secure, user-friendly, and simple authentication schemes for Non SIM and SIM base IMS authentication?
- Can we combine multiple authentication schemes to improve security or user friendliness?
- What is the most important parameter for User and for network Operator/business?

1.4 Expected Outcomes

Authors entitle to comprehend the "MOBICOME" project, security researcher consultant and other scientific communities associated with the IMS security authentication access technology about detail features and short falling of each authentication mechanism. Possible outcomes will reveal information to decision makers in execution of design and implementation of the selectable authentication scheme.

1.5 Thesis Outline

Chapter 2 will represent background knowledge of IMS, SIP, GPRS and UMTS technologies.

Chapter 3 will define the research methodology phases and their description, problem identification to research question, proposed solution and evaluations.

Chapter 4 addresses brief introduction about IMS authentication Schemes divided into two categorizes i.e. Non-SIM base authentication and SIM base authentication.

Chapter 5 is key chapter producing empirical results for Non SIM base authentication which can be understood first section of the analysis part and analysis is performed by means of SWOT tool.

Chapter 6 is also a key chapter producing empirical results for SIM base authentication with the same SWOT analysis tool.

Chapter 7 encompasses complete discussion based on the SWOT analysis in terms of Non SIM and AIM base authentication, and further suggests which will be more appropriate IMS access mechanisms focusing on security and user friendliness.

Chapter 8 illustrates conclusions and future work of the research. Conclusions imply to conceive the concatenation of two authentication schemes to increase security.

Chapter 2 Technical Background

This chapter contains preliminary information about network technologies focus in the study during authentication procedures.

2.1 IP Multimedia Sub Systems (IMS):

IMS is universal IP access independent standard architecture providing voice and multimedia fixed and mobile services in the telecommunication domain. IMS architecture is defines in [1, 2] and contains three key elements.

2.1.1 Call Session Control Functions (CSCFs):

There are mainly three types of CSCF which handle the authentication process with the UE, the first point of contact is P-CSCF, an I-CSCF and S-CSCF. S-CSCF further in the authentication procedure authenticates the UE based on the provided parameter form the HSS and UE and validate the connection.

2.1.2 Home Subscriber Server (HSS):

HSS is a central repository residing in the IMS core network and maintain all user profile information relevant for session establishment/ authentication process, CSCF's allocation, authorization, etc. HSS consist of user profiles, registration information, user identities and access parameters. Two types of user identities in IMS are private (IMPI) and public identities (IMPU) necessary during IMS authentication/registration process. HSS also provide user specific requirements to S-CSCF, and information is utilized by I-CSCF for selecting most suitable S-CSCF for user.

2.1.3 Media Resource Function Control and Media Server:

They serve application server to provide media processing services i.e. audio, speech, mix audio, voice XML, etc. P-CSCF is use for IP security and integrity and confidential protection for SIP signaling. This means that when UE is register with P-CSCF, then P-CSCF is able to provide confidential protection and provide integrity to sip signaling. IMS emergency session are not fully specified, working is ongoing in Release 7 and its very important that IMS networks detects emergency sessions and guide UMTS UE to use CS (circuit switching) network for emergency sessions.

2.1.4 IP Multimedia Subscriber Identity Module (ISIM):

IP Multimedia Services Identity Module is a module/ application running on UICC (Universal Integrated Circuit Card). ISIM contain IMS (IP Multimedia Subsystem) security related information used for authenticating user. UICC can also bear additional information about SIM and USIM applications to authenticate GSM and UMTS networks respectively.

2.2 Session Initiation Protocol:

Sip is an application layer protocol used to establish, modify and terminate multimedia sessions in IP networks.

2.2.1 SIP Architecture:

SIP architectural elements [2] can classify as User Agents (UAs) and intermediaries (servers). SIP UA is a terminal which can send and receive SIP requests and responses. SIP intermediaries (Servers) are the entities through which the SIP messages can pass to their final destinations. The servers can be a proxy servers, redirected servers, registrar servers, locations servers etc.

2.2.2 SIP Message format:

SIP message consist of 3 parts depicted in figure1, i.e. Start line, message body and headers.

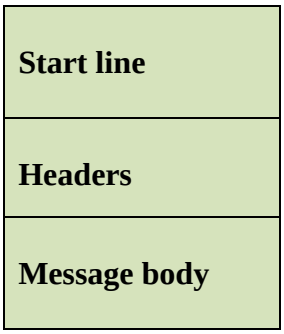

Figure 1: SIP Message Format

2.2.2.1 Start Line:

Contents of Start line depends on SIP message whether it's a request or status (response) and in case of request it's called as "request line" while for response it's called as "status line". Request line has three components;

- **Method Name:**
  Method name shows type of the request i.e. INVITE, CANCEL, BYE, ACK and BYE used for session creation, modification and termination. REGISTER request is used to register user contact information.

- **Request URI:**
  Request URI identifies a resource that the request is addressed to.

- **Protocol Version:**
  Protocol version identifies current version of the SIP.

Status line also has three components;

- **Protocol Version:**
  It is same as protocol version in request line.

- **Status Code:**
  Status code is a 3 digit code which identifies the nature of the response.

- **Reason Phrase:**
  It is free text field which provide a short description of the status code.

2.2.2.2 Header fields:

It contains information related to the request e.g. Initiator of the request, recipient of the request and call identifier. The syntax of the header filed as:

Header name: header value

Some of headers are mandatory in very SIP response and request such as TO, FROM, CALL ID, Cseq, Via etc.

2.2.2.3 Message Body:

The message body also called payload can carry any text information, while the request and response methods determine how the body should be interpreted.

2.2.3 SIP URI:

SIP Uniform Resource Identifier has the same form as email address (user@domain).
There are two URI schemes:

- sip:inayat.khan@nokia.com is a SIP URI. This is the most common scheme and defines in [3].
- sips:inayat.khan@nokia.com is a SIPS URI. This is a new scheme and defines in [3].

There are two types of SIP addresses states as:

- **Address Of Record (AOR):**
  A SIP addresses which identifies a user. This address can be assigned to people in much the same way as a phone number e.g. sip:inayat.khan@nokia.com.

- Fully Qualified Domain Name (FQDN) or IP address (which identifies a device) of the host e.g. sip:inayat.khanco@192.168.0.103.

2.3 General Packet Radio Service (GPRS):

In [4], GPRS is a packet based communication service allows mobile devices to send and receive data across mobile telephone networks. GPRS is an often referred to as 2.5G but is step towards 3G networks. Since GPRS is not a separated network from Global System for Mobile communication (GSM), many devices such as Base Station Controller Base (BSC) and Base Transceiver Stations (BTS) are still in used. However in GPRS network there are two main functional components are added which play important role in GPRS network. They are Serving GPRS Support Node (SGSN) and the Gateway GPRS support node (GGSN). The main tasks of SGSN including routing of the packets, IP address assignment and handover. SGSN provide a logical connection to the mobile GPRS station. For example you are in the car and travelling on a long journey and browsing internet through GPRS device. You pass from different cells so here the job of the SGSN is to make sure the connection is not interrupted by moving from cell to cell. It is also the job of the SGSN to route connection to the desire BSC. GGSN is responsible for interworking between GPRS network and other external packet switching networks. GGSN is a router, gateway, and firewall rolled in one entity which hides internal infrastructure of the GPRS network from outside network. The connection between SGSN and GGSN is made with a protocol called GPRS Tunneling Protocol (GTP). In order to access the IMS services UE of the GPRS request to establish PDP context to peruse its authentication with IMS core network elements.

2.3.1 Subscriber Identity Module (SIM):

A Subscriber Identity Module card is just like a smart card but small in size and fit into mobile phone, and provides identification of the user to the network. SIM allow the user to provide services to the user such as text messaging, emails, internet and telephony.SIM contain microcomputer which can process commands store in RAM(random access memory),also contain EEPROM(Electronically Erasable Programmable Read Only Memory) which store user files. The SIM card Operating system can store in ROM (Read Only Memory) which can operate all information and then provide to the user. Whenever SIM card is activated then microcomputer load the operating system from ROM to RAM and process the user commands. The SIM operating system comes into two main types .i.e. Native and java cards, Native SIM,s are based on vender specific while java SIM,s cards based on standards. Each SIM card can store IMSI (International Mobile Subscriber Identity) which identify the user on the Mobile telephony devices such as Mobile phones, PDAs and computers. The format of IMSI as: The first 3 digits represent Mobile Country Code; the next 2 represent Mobile Network Code while the remaining 10 digits represent mobile station identification number.

2.4 Universal Mobile Telecommunication System (UMTS):

UMTS is 3rd generation packet based broadband transmission of triple play i.e. voice, video, text and multimedia at the rate of 2 MB per second. The UMTS basic architecture [5] consists of two important sub networks.

2.4.1 Radio Access Network (RAN):

RAN is an interface which connects user equipment (UE) with core network. It contains radio transceiver called Node B equivalent to base station Controller (BSC) and Base Transceiver Station (BTS) in GSM. This unit communicates with various UEs. It also communicates with Radio Network Controller (RNC) and RNC component of RAN connect core network.

2.4.2 Core Network (CN):

The core network of UMTS is divided into Circuit and packet switching domains. Which means that circuit switching elements in UMTS is used for GSM and Packet switching elements are used for GPRS and Enhanced Data rates for GSM Evolution (EDGE). Some of circuit switching elements are Mobile service Switching Centre (MSC), Gateway MSC and Visitor Location Register (VLR) and packet switching elements are Gateway GPRS Node (GGSN) and Serving GPRS Support Node (SGSN).

2.4.3 Universal Subscriber Identity Module (USIM):

USIM is the most advance version of SIM (subscriber identity module) and contain user specific information's to authenticate user to the access network. USIM can store authentication information, text messages, telephone numbers, preferences as well as user subscriber related information. USIM has international Mobile Subscriber Identity (IMSI) and Mobile Station International ISDN Number (MSISDN). In UMTS the terminal is called Mobile Equipment. The concept of function blocks known as domains exists in UMTS standard. Thus USIM card is USIM domain; the functions of the terminal belonging to Mobile equipment domain. Both these domains together form User equipment domain. When talking about UMTS mobile, one just simply calls it User Equipment (UE).

Chapter 3 Research Methodology

Methodology terms to identify an orderly study of principals, methods, and procedures governing an investigation for finding solutions to a problem(s) in selected discipline. Mainly there are two kind of research methodologies established i.e. qualitative and quantitative.

3.1 Research Methodology

The aim of the research involves extensive state of the art study along with current emerging technologies, so quantitative research is carried out to investigate the authentication techniques with SWOT analysis tool.

SWOT is well-organized tool for measuring strength, weakness, opportunities and threats of any objective in making valuable decisions especially for determining the strategy implementation in context of choosing single path in between multiple paths. SWOT is widely used in the business-oriented projects by viewing external factors impacting on internal factors.

The objective of the study is to use SWOT analysis tool for IMS access security authentication schemes for SIM and Non SIM base authentication. To make use of current research studies for analyzing each authentication scheme to produce solid information in making decisions for the desired problem/s.

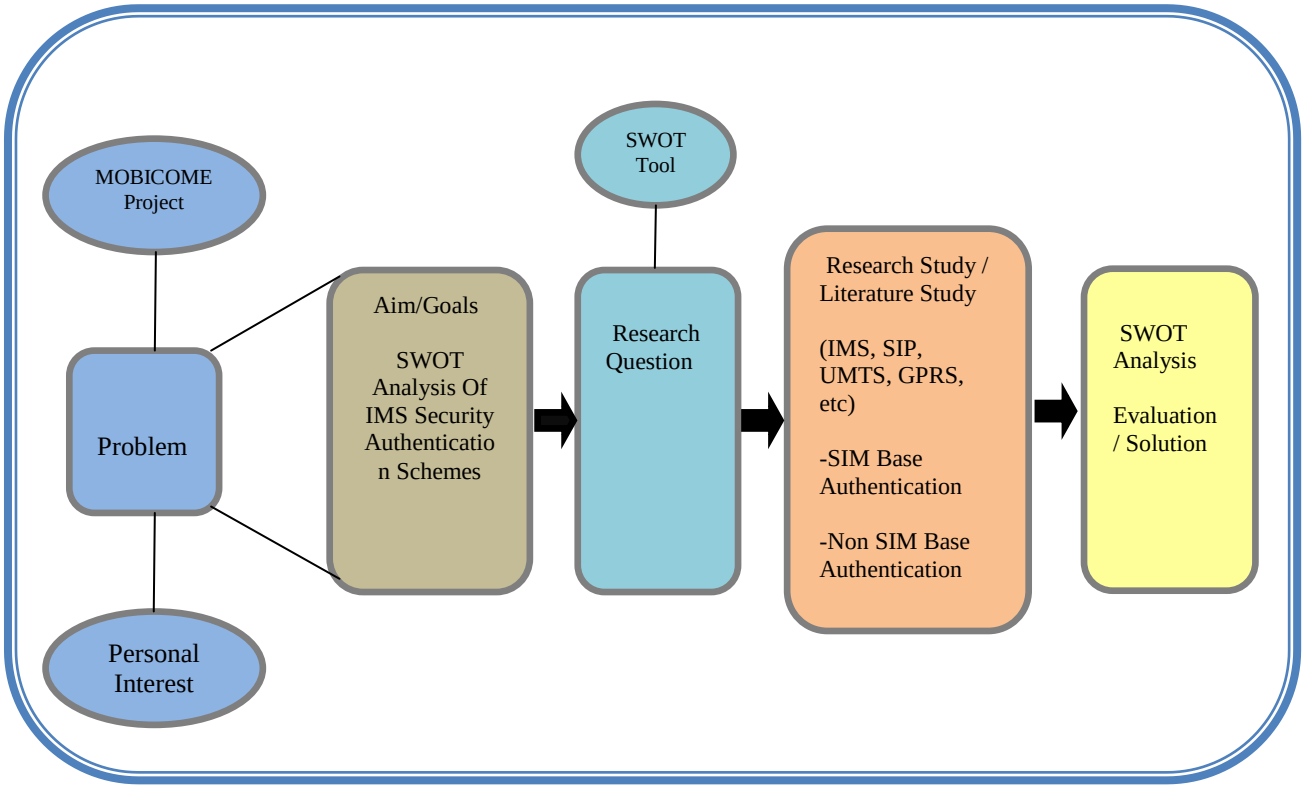

Figure 2: Research Methodology

3.2 SWOT

SWOT stands for Strength, Weaknesses, Opportunities and Threats. It's very powerful technique and used to understand and measure Strength, Weaknesses, Opportunities and Threats that you face. Here Strength and Weaknesses are internal to an organization, product or service while Opportunities and Threats are external factors. SWOT analysis is a process that demonstrate your strong and weak area as well make prediction based on strengths and weakness about possible opportunities and threats, proving clues about attacking area and defending strategies. SWOT analysis is not limited to company/business or product but can work efficiently on services.

3.3 How to Conduct SWOT Analysis:

Conducting SWOT analysis for company, product, and service requires considering some important steps defined herein to become successful.

1. **Information Gathering:**
   It involves collection of data for SWOT through interviews with the concerned in an interaction with the system, product, or a service with directly to peoples individually or in a group forming brainstorm.
   Since it was slightly possible to take help form the supervisor, and mostly we rely on the state of the technology and internet material to learn the about the authentication procedures.

2. **Plane of Action:**
   This step involved all possible workout of each individual IMS authentication technique, and then considering an important points and eliminates unnecessary point in each of S, W, O, T analysis.

3. **Strengths:**
   It explicitly defines advantages, unique resources, what can be done better, and what property/parameter does peoples see as your strength.

4. **Weakness:**
   It illustrates what should be improved, avoided, or that is done poorly.

5. **Opportunities:**
   The new opportunities/trends facing a head, it can also be made possible to cut down your weakness or use your strength to make more opportunities.

6. **Threats:**
   What could be possible problem occurrence probability in future?

Chapter 4 IMS Security Authentication Schemes

Authentication is the process of user logging into a web site or security system that verifies that person is who he claims to be. There as different authentication schemes for IMS services and categorized as SIM base and NON-SIM base authentication schemes, so we will provide brief overview about each of them.

4.1 Username / Password Authentication:

Username and password is the simplest and commonly used authentication schemes in our daily lives. User have to enter user ID (account name, user name, login ID) and a password (PIN) to get authenticated with the desired system/web application. Two parameters are mandatory i.e. user name and password, so when you can enter user and password, subsequent system can check user profile in the data base repository for user validation/verification.

There are two types/modes of scheme, “Basis” and “Digest” defined in [6]. Basic scheme can support almost all web browsers while Digest can support i.e. Mozilla ver. 1.9.7, internet explorer ver. 5, safari ver. 1.0 and Netscape ver. 7, etc. Basic send the username and password messages in the plain text format during data transmission, while Digest encrypt the username / password provided by the user by MD5 algorithm.

4.2 Smart Card Authentication:

Smart card are also termed as integrated circuit card (ICC)[7] or chip card and is a small pocket size card with embedded IC used for processing of data. The chip in the card is used to store data of the user and other information. Usually data can access from a chip through a card reader but current technologies can access data without physical connection to the device. Smart card are used in different places such as banking, transportation, healthcare, E-commerce, physical access, libraries, etc. There are two main types of smart cards i.e. contact card (which require smart card reader to be authenticated), and contactless card (which require a close distance of about few inches to the reader for authentication). There are many different categories of smart card.

4.3 SMS Authentication:

Form [8], specifications to SMS authentication involves person identity verification, the technique works in better in addition to some other authentication technique to improve security. Two-factor authentication (T-FA) is a system where two different factors e.g. user name/password plus SMS are used in conjunction to authenticate. Two factors authentication provide much more security as compare to one factor authentication. Any deficiencies in the other technique i.e. username/password are controlled by using this technique. It uses a code send through SMS, and if another technique is monitored by sniffer/ man in the middle attack/ eavesdropping occurred, then unauthorized user will not be able to access the service. Reply attacks are also not possible and time factor involved during encryption will have implicit impact on the authentication procedure. The advantages of this scheme over user name/password as that user do not have to remember any type of ID and PIN code. A user must provide up to date phone number to the system because SMS base Scheme the secret key is send to user by an SMS. SMS can here be regarded as the ``something-

you-have`` factor in the authentication scheme. User then manually can copy this key from mobile phone to system. There as also another option to send secret key from mobile phone to system and that as ``Bluetooth`` but for this system and mobile set must be within a range.

4.4 MAC Address Authentication:

In computer network MAC address/ hardware address/ NIC adapter address or Ethernet Hardware Address (EHA) is a physical address which uniquely defines device on the internet through network interface cards (NICs). These addresses are assigned by device manufactures. The standard format MAC-48 addresses in human-friendly form is six groups of two hexadecimal digits and are separated by colons (:) or by hyphens (-) e.g. 98-76-54-32-01-ir or 98:76:54:32:01: ir. 48 bit address contains 2^{48} Or 281, 474, 976, 710, 656 possible MAC addresses either administered locally or globally.

4.5 Simple NASS Authentication:

Simple Network attachment subsystem is defined by IMS service access through landline implicit connectivity. NASS functionality includes dynamic IP address assignment (DHCP), UE authentication, network access authorization, UE location management. Simple NASS involves implicit authentication depending in the access network, wire broadband network at layer2 (L2). In [9] an implicit authentication form knows as line authentication ensures access line authentication by accessing CNG. Line ID is used during authentication process while operator defines its authentication policy. In figure 3, IRG (internet residential gateway) contains ISIM module and the location of the IRG is determined during authentication procedure.

4.6 Digest NASS Authentication:

UE is connected to NASS implementing digest algorithm during data communication i.e. ISIM present in each UE connect the NASS through NAT filtering and after successful location identification request is forwarded to IMS P-CSCF. In figure 3, it's clear that every UE should explicitly contain ISIM module in such way it can directly authenticate with S-CSCF.

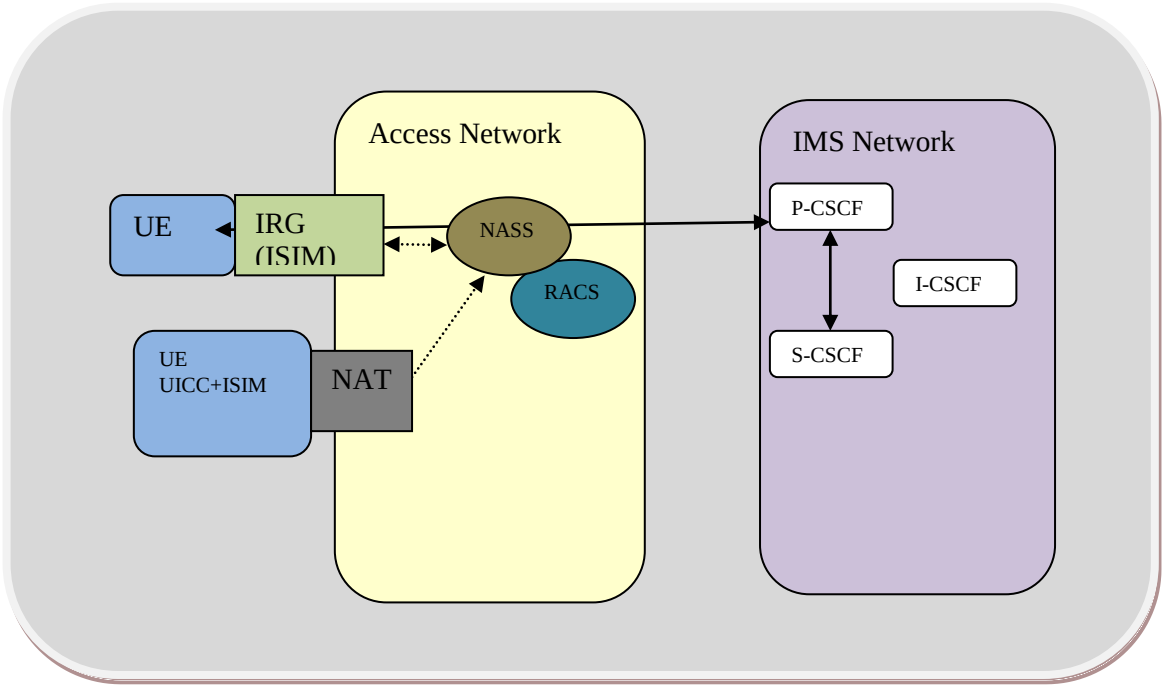

Figure 3: Simple and Digest Network Attachment Subsystem connectivity with IMS network [9]

4.7 IMS AKA Authentication:

For IMS AKA to work, the ISIM module contains SIP identities and share secret key for authentication with IMS. In IMS AKA authentication procedure [10], the subscriber sends Register Request to the IMS entry point (P-CSCF), P-CSCF forward the request to I-CSCF, which assigns a desire S-CSCF to the user. To get the register request from the user, the S-CSCF cheek the IMPI and IMPU of the desire request, and request Authentication Vector (AV) from HSS (Home Subscriber Server). HSS send AV which contains IMSI and the number of AVs requires. AV contains authentication token AUTN, random number (RAND), Expected Response (XRES), Integrity Key (IK) and Confidentiality key (CK). Only one AV is used for one authentication request. After receiving the AV from HSS, S-CSCF save the XRES and send the remaining challenge to the P-CSCF, P-CSCF stores the integrity and Confidentiality keys and send the remaining challenge to the UE, which include RAND, IMPI and AUTN. UE can take AUTN from challenge, find SQN and MAC and verifies that SQN is correct and calculate the XMAC. If the calculated XMAC of the UE matches the MAC which is extracted from random challenge then UE verify the network authenticity and calculate Response (RES). After this with second register request RES is sent to the S-CSCF and compare RES with XRES. If both RES and XRES match in the S-CSCF then subscriber will authenticate and IMPU is registered. Due to the authentication procedure the network authenticate subscriber and subscriber authenticate network, this is called mutual authentication and provide strong authentication.

4.8 Early IMS Authentication:

3GPP defines IMS architecture and specifications for early IMS deployment as an interim solution. Early IMS are because of non USIM/ ISIM module support at UE. Network operators of 2.5G cannot directly implement ISIM module and requires upgrading in the network hardware and UE UICC modules. Early IMS implements no IMS level security and rely on subscriber's authentication, underlying network access and IP address. Detailed authentication procedure is explained in [11].

4.9 One Pass GPRS Authentication:

In one pass GRPS authentication in UMTS, UE connects with the UMTS PS through GPRS utilizing IMSI. UE access IMS service through criteria is defined in [12], in the first step both IMSI and IMPI are used by the UMTS UE to send over the PS domain to P-CSCF for further computations. This method improves network efficiently through avoiding 50 % excessive network registration/ authentication traffic and in AVs storage. SIP application Level gateway is maintained by SGSN. Please refer [12] for complete explanation.

4.10 Evolutionary IMS Authentication:

E-IMS authentication is an efficient and provable IMS authentication scheme proposed for UMTS UE accessing IMS service framework. UE must contain USIM or ISIM module, IMS AKA security architecture is preserved along with efficiency improvement (i.e. mutual authentication, CK, IK, RSN, RAND, ITK, etc) through avoidance duplicate authentication messages. The require parameters for the authentication procedure are send in advance, further illustrated in [13].

Chapter 5 SWOT ANALYSIS of Non SIM Authentication Schemes

5.1 Username/ Password Authentication

STRENGTHS	WEAKNESS
• User friendly. • Multiple browser support. • Diverse usage/Commonly used. • User defines password security. • Cost effective. • Users trust and experience. • Complexity/ low response time • User access during mobility.	• Plain text transmission. • Password security. • Less efficient. • Dependability of IP layer security.
OPPURTUNNITIES	**THREATS**
• Password definition level guidelines. • Selection of TLS/SSL with multiple browsers and/or SHTTP. • Uses only digest authentication technique.	• Security attacks. • User dependent password. • Login attempts.

5.1.1 Strengths

- **User Friendly:**
  Large population of the computer technology is familiar with username/ password scheme [14]. It is obvious that users feels and understands the concept of using this technique. It has quite different but simple appearances for the user interface to enter the login and password and the main theme of information processing for authentication lies below the normal user understanding.

- **Multiple Browser Support:**
  Since this technique have two modes of authentication procedure i.e. basic and digest, so basic provides support for almost all existing web browsers in use while digest provides support for selected number of web browsers i.e. Mozilla ver. 1.9.7, internet explorer ver. 5,

safari ver. 1.0 and Netscape ver. 7, etc. This is why no specialized software is desired for the authentication procedure. Multiple browser support for authentication encourages the businesses to deploy this technique while users are not bounded/ limited to access.

- **Diverse Usage:**
  This technique is adopted by major portion of the user community due to its simplicity in understanding and working and is a pioneer approach for authentication.

- **User Define Password:**
  The password can be merely created by user at an individual basis. So, it makes easy for the user to remember and change password according. It provides increase flexibility in choosing a password instead of system define passwords.

- **Cost Effective:**
  This technique does not require any specialized software and hardware to implementation and is available in many browsers. The software development, maintenance and upgrading cost are also not involved because MD5 [15] and other encryption algorithms are available freely.

- **User Trust and Experience:**
  It is the foremost advantage of the technique that generally users are well known to this technique and as maximum number of the users are unaware of the problems in this technique that why they to use it. They believe that the password they hold is quite secure from the external world. As a pioneer technique by the business market, users hold experience in using it.

- **Complexity/ Low Response Time:**
  Since time is very critical factor when administering the user behavior, so lower the complexity, lower will be the time required by the user to authenticate with the system. Since the scheme does not hold significant complexity in algorithm in implementing higher degree of encryption in the basic and digest, so the performance at user and server end is assumed to be high.

- **User access During Mobility:**
  User is totally free to move around only requiring username/ password to remember to use the service. No need to carry some sort of hardware or specialized software to access the service.

5.1.2 Weakness:

- **Plain Text Transmission:**
  The most widely authentication mode is “basic”. It contains the problem of sending the data in the plain text without any encryption which helps in reducing complexity and improving simplicity but severely affects the privacy and secrecy of the data during transmission. Spoofing i.e. man in the middle could occur during the data transmission and probably result with unauthorized access to the data and services and also reply attacks are likely afterwards.

- **Password Security:**
  Easy passwords are easy to guess, the possibility for user define password could be harmful in a sense, if the password level is low. Most of the users are not expert users to the technology so they cannot keep hard password as they are difficult to memorize. Even with possibility to build higher and dynamic user define passwords, it’s important to notice that “basic” send the password in the plain text format, so it’s highly vulnerable. If “digest”

method is used, the encryption holds significant importance at the either end but if the data during transmission is monitored through spoofing, password can be decoded with small efforts because MD5 algorithm is freely available. Also when we enter the username/ password, it remains in the browsers cache until we exit the browser completely.

- **Less Efficient:**
  It requires double processing time and data transmission because when the access is requested, browser receive the reply from authenticating server to enter the username and password and then browser sends the data again i.e. second time for authentication. Also without having and intelligent server, it is likely that for access each secure page double authentication is required. Whereas new explores utilizes the stored username/ password in cache and reduces the number of login attempts.

- **Dependability of IP layer Security:**
  Since basic and digest authentication schemes doesn't provide enough security and data is transmitted either in plain text form or encrypted through MD5 algorithm, it is highly valuable to notice that IP Security Association (SA) is essential to protect the data during transmission. TLS/ SSL and IPSec are extremely proposed to implement for username / password authentication scheme.

5.1.3 Opportunities:

- **Password Definition Level Guidelines:**
  Users are free to choose username and password but it's crucial to notify the users about the level of secure password selection. This can be implemented by the IMS system in a sense that alpha numeric passwords in concatenation with suitable password length size should be defined. Also to keep the password security, common policy to change the password with the same level of security will be provided in limited number of days.

- **Selection of TLS/SSL with Multiple Browsers and/or SHTTP:**
  It is extremely recommended to implement security at either ends depending upon the browsers involved as well as the transmission medium.

- **Uses Only Digest Authentication Technique:**
  With only possibility to choose between "basic" or "digest" technique, it's complemented to implement digest technique in order to have secrecy and confidentiality of the password. An improve algorithm can also be implemented to overcome the deficiency to totally control the possibility of decoding the messages.

5.1.4 Threats

- **Security Attacks:**
  Numbers of security attacks are certain subject to "basic" and "digest" schemes to gain unauthorized access to the system and service e.g. man in the middle attack [16], session hijacking, replay attacks [17] and eavesdropping.

- **User Dependent Password:**
  Higher risk and uncertainty is associated with the user perceptions in choosing the password. It's difficult for the user to remember hard passwords containing alpha numeric values/digits. An attempt to access the service from unauthorized user could result in access due to weak security protection of the user itself. It could be because the user have chosen password like its name, telephone number, date of birth, city and country name, which are very easy to guess. Also a problem is associated with the standard password chosen by the user but unable to protect it i.e. write on piece of a paper, in mobile, some text file that are vulnerable to security attacks (physically and remotely).

- **Login Attempts:**
  High security requires improvement in the software as well as an extra work load on the server and personnel UE side. Wrong login attempt could grew higher processing tasks, causing network traffic increase and low response time, and could also results in denial of service (DOS) [18] attack at extreme situations.

5.2 Smart Card Authentication

STRENGTHS	WEAKNESS
• Increase usability options • Added security • Multiple application data storage capability • User friendliness • ISO standard	• Multiple programmable development. • Physical security. • Costly • Hardware dependability
OPPURTUNNITIES	**THREATS**
• Bright future technology • Higher security implementation	• User privacy and information confidentiality • Time consuming • Technology Conquest

5.2.1 Strengths:

- **Increase Usability Options:**
  The technology has been around for several decades [19] which make it widely available, acceptable and comfortable to use. Smart cards can be reused and disposed off when changes occur in the functionality, design, operation and requires re-programming in its module. It supports single sign on (SSO) [7] facility which impacts clear authentication procedure from the user prospect and reduce time response.

- **Added Security:**
  It contains separate hardware and software for authentication through digital signatures/ certificates [7], software are programmed in the smart card chip with multiple programming languages and ISO 7816-4 [20] security mechanism. An extra advantage in the smart card [19] is that they are likely to generate quality random number for cryptographic protocols. Smart card as a physical entity and a PIN [21] required for the card holds significant importance in increase security.

- **Multiple Application Data Storage Capability:**
  Smart card has increase memory size and computation power [19] which supports for separate multiple application development [19], storage and execution for different network access i.e. UMTS, edge, WIMAX, etc.

- **User Friendliness:**
  It's user friendly [22], simple plug and play device with single sign on authentication functionality and offers no complexity in its usage.

- **ISO Standard:**
  Around the world it adoptability is due to the open government policies as it follows ISO 7816 [20] which is the international Organization for standardization (ISO).

5.2.2 Weakness:

- **Multiple Programmable Development:**
  An essence of the smart card are the security and language tools so its vital to stay towards simple but strong security implementation through programming languages which has clear implementations but difficult and complex security breaches/ mechanisms. The smart cards are traditionally written in C and assembly language [22] while the modern smart cards are more likely programmable in JAVA language.

- **Physical Security:**
  As a physical entity smart card requires some sort of care and security by the user and organization. Possible physical attacks includes [22] invasion-if the micro-electrodes are implanted on the data paths, destroy connections, if without PIN enable cards are used, it makes an easy gateway to access the services/authentication.

- **Costly:**
  Smart card technology improvements involve [20] increase memory, semiconductors, software development and hardware cost. Smart card cost up to few US dollars depending upon the mode of operations and functionality it contain.

- **Hardware Dependability:**
  In order to use the technology, it's apparent to hold a card, users are very much dependent upon its existence and availability, when required. The size of the card makes it carry easily during mobility but still require have considerable attention.

5.2.3 Opportunities:

- **Bright Future Technology:**
  Smart cards at present have proven to be a benchmark in many business i.e. banks, offices, transports, universities, building, etc. Its flexibility in use, simplicity and enough security at every level (with or without PIN depending upon the area of use) makes it much interesting and adoptable. Less cost in the future due to electronic industry evolution will also have great impact on many growing businesses.

- **Higher Security Implementation:**
  Ongoing research has implication towards integrating technologies to improve security by means of biometric technology [23]. Several business have already build biometric oriented smart cards for highly secure identification but are only available to and adopted in high security areas. This scheme will provide higher level of security if implemented with PIN and Biometric. In this way it will cover the complete set of National Institute of Standard and Technology (NIST) guidelines, [24].

1. Something you have (smart card)
2. Something you know (PIN)
3. Something you are (biometric technology i.e. fingerprint, face, iris, etc)

5.2.4 Threats:

- **User Privacy and Information Confidentiality:**
  Poorly programmed, less secure cards could clearly subject to security risks. Consider the simple smart card; the reason of "IF" lies in many situations. If the cards is used without PIN, it has most severe outcomes when lost, if is used contactless, the user data is vulnerable to many card readers (data secrecy and confidentiality). The best possibility use to this technology is to follow NIST [24] guidelines to strictly follow 1, 2 and 3 above.

- **Time Consuming:**
  To keep up using smart card at every next instant consume extra time frame, multiple application running on the same smart card will also have some sort of dependence on related applications. If the smart card has been utilized by one application (even though it offers multi-processing and multi-tasking operation), the requirement to remove it from the user equipment and swap it over the door, etc or it may be to look for smart card within bundle of cards carrying along involves time.

- **Technology Conquest:**
  We know that SIM/ ISIM/ USIM technologies are parallel in use and development. The size and shape of smart card is big as compared to other technologies, UICC card for SIM, USIM/ISIM are similar to electronic chip implanted on the smart cards and the possibility of similar operations and functionality lies in its development.

5.3 SMS (Short Messaging Service) Authentication

STRENGTHS	WEAKNESS
• Extra added security • User perception, reliability and acceptability • Telecom standards for SMS data integrity	• User hardware dependence. • Multi user input • Extra network software/ hardware requirement. • Internet traffic increase
OPPURTUNNITIES	**THREATS**
• IP network Evolution. • Reduce effort in service delivery.	• SMS delays. • Full hardware dependability.

5.3.1 Strengths

- **Extra Added Security:**
  As many other authentication techniques are available, so this technique works in addition to some techniques that improves security. Any deficiencies in the other technique i.e. username/password are controlled by using this technique. It uses a code send through SMS technique defined in [8], if another technique is monitored by sniffer, man in the middle attack, unauthorized user will not be able to access the service. Reply attacks are also not possible and time factor involved during encryption will have implicit impact on the authentication procedure.

- **User Perception, Reliability and Acceptability:**
  Usability issues are keenly observed by the businesses to ensure the users perception about the products. It is highly observable that during many financial transactions an involvement of the random code generator improves user trust and confidence in the working. Similarly, SMS [25] is also understandable as a high security feature which results in users rely in the technology usage and acceptability. SMS are sometimes free, simple and easy to use, so it makes a sense that this technology will not require extra learning capability for the users and most users will likely to accept this technique.

- **Telecom Standards for SMS Data Integrity:**
  In 3GGP, [26] have define standards for SMS data integrity. GSM and UMTS clearly state that there will be no change during SMS transmission between mobile node and MSC and vice versa.

5.3.2 Weakness

- **User Hardware Dependence:**
  In order to receive SMS from the IMS (SMS Application server), it is essential to use some hardware device i.e. mobile phone to receive SMS containing code for the device authenticating with IMS network. It is not possible to use the same device to receive SMS for initiating authentication with IMS network.

- **Multi User Input:**
  As the SMS is sent through IMS network, so it probably takes some time to receive SMS. Also user requires time to wait and enter the code i.e. double input from the user. This causes inefficiency in the performance during authentication procedure/completion.

- **Extra Network Software/ Hardware Requirement:**
  Providing with the possibility to increase strong security, network software and hardware should be develop and deployed at IMS network, each authentication query will be process twice resulting in extra processing time, complexity and utilizing and network recourses.

- **Internet Traffic Increase:**
  It will also contribute in an increasing network traffic and signaling with in IMS network and outside internet.

5.3.3 Opportunities:

- **IP Network Evaluation:**
  In near future our network will encompass through IP, thus it shall be very cheap to send SMS through Application server.

- **Reduce Effort in Service Delivery:**
  SMS is pioneer service in the telecom industry and has simple and easy deployment. The maintenance of the application server will not require extra efforts.

5.3.4 Threats:

- **SMS Delays:**
  Telecommunication networks heavily rely on the IP network due to packet switching technology. IP network itself holds to significant network congestion hitches and probabilistic nature which causes undeterminable time delay for successful data transmission. No or week signal strength due to limited converge area also causes delays in SMS delivery.

- **Full Hardware Dependability:**
  It is uncertain if mobile phone is lost, mobile SIM become damage or battery power empties suddenly, so SMS cannot be delivered to the define mobile number store in the database. It's the most difficult and time consuming situation, as it requires new hardware (SIM, phone number) and exchange of user profile in the company network authentication database (HSS).

5.4 MAC Address Authentication

STRENGTHS	WEAKNESS
• Usability • Negligible Cost • Simplicity	• Small Network Focus • Security Risks • No Global Implementations/ Recommendation • Hardware Limitation in Mobility.
OPPURTUNNITIES	**THREATS**
• Easy Spoofing detection • Portable hardware Mobility.	• Replay Attacks • Diminishing Technology • MAC Address/Hardware Change Necessity.

5.4.1 Strengths

- **Usability:**
  Authentication is transparent to the user as MAC addresses is part of the control messages [27] and are often not encrypted whereas only payload is encrypted. It's quite easy and simple to use this authentication method as it doesn't require anything to remember. Modern hardware includes MAC address that uniquely identifies the device on the network.

- **Negligible Cost:**
  All the user equipments (UE) have built in Network Interface Card (NIC) holding MAC address and entail no extra cost except only for those reasons when UE entails to change NIC card or buy wireless card.

- **Simplicity:**
  MAC address authentication uses simple algorithm as MAC layer headers are not encrypted but only payload is encrypted [27] so no complexity exists during authentication mechanism. Time required to authenticate is merely less which plays negative contribution in complexity. Although some fields are necessary for the authentication procedure further to validate the user identity.

5.4.2 Weakness

- **Small Network Focus:**
  MAC authentication is implemented for very small network due to weak security, only for specific users to access the network services. It involves configuring wireless Access Point (AP) with a limited number of MAC address and re-configuration at every new user necessity to access the services. HSS in the IMS has sufficient memory to hold numerous MAC address and use this scheme but the fact is that MAC header are not encrypted and the wireless medium is completely vulnerable to spoofing attacks/ sniffers.

- **Security Risks:**
  Very high risk of security attacks [28] exists i.e. MAC address spoofing, session hijacking and access control lists. This weak security confronts with the NIST guidelines [24] and single level of security is present "something you have". Simple commands and free software's are available to used for changing MAC address for malicious intent, once its required to sniff communication and analyze the MAC address, and then change it according to the authenticated/authorized user MAC address.

- **No Global Implementations/ Recommendation:**
  It's highly valuable to find MAC authentication as a landmark in the society on large scale. Since IMS network will offer clean authentication and seamless access to the services but also requires strong user identification as a security reason. Due to MAC address weak security flaws, no larger implementation of this authentication technique are found to the best of our knowledge. Microsoft technology also doesn't recommend [29] MAC address authentication even for wireless small office networks.

- **Hardware Limitation In Mobility:**
  The question of maybe or may not be, well mostly modern trends doesn't bound us to daily life happening or requirements, but still to clinch access to the service, it's necessary to carry/hold the same MAC address built-in UE for service. The MAC address authentication doesn't let you move freely without the UE and mostly you have to keep up thing unwillingly.

5.4.3 Opportunities:

- **Easy Spoofing Detection:**
  Many methods for spoofing detection are proposed in state of the art technologies i.e. Reverse Address Resolution Protocol (RARP) is a simple technique to determine whether two or more users are connected using the same MAC address. During the MAC address authentication procedure, MAC address is bind with the single IP address. RARP offers an opportunity to check if any MAC address is spoofed by running RARP check and if multiple IP addresses are returned, which indicates spoofing attack.

- **Portable Hardware Mobility:**
  As every UE has built-in MAC address it can be made possible to use external wireless card that connects the access point and use this external network interface card (NIC) MAC address for configuring in AP/HSS.

5.4.4 Threats

- **Replay Attacks:**
  The most common security attacks associated with MAC address are replay attacks [28] as its one time hard work to find and change the MAC address similar to the authorized user MAC address. Once through spoofing /packet sniffing, MAC address has been identified, it's simple to change the MAC address and access the user services.

- **Diminishing Technology:**
  Due to very weak security, upcoming security mechanisms will leave this authentication method far behind and it will only be used as a supplementary portion to any other authentication or maybe eradicated for any authentication schemes.

- **MAC Address/Hardware Change Necessity:**
  Physically meant single MAC address is associated with each identified individual UE. If the MAC address has been spoofed and used, so the technology will require the user to change the MAC address/ hardware to obtain new MAC address as its open to unsecure world.

5.5 Simple NASS Authentication

STRENGTHS	WEAKNESS
• Single Device Authentication • Dynamic User Authentication Support • User friendly, Simplicity and Usability	• IRG Dependence • Time Consuming • Increase Cost. • No Mobility. • CPN Security.
OPPURTUNNITIES	**THREATS**
• Security Improvement • Required Mobility	• Customer/User define Security • CPN Limitations

5.5.1 Strengths

- **Single Device Authentication:**
  ISIM module is present in the IMS residential Gateway [30] at the customer premises network (CPN) available to connect customer premises equipments (CPE) through wire line with the access network consisting of NASS and then back to core IMS. Only IRG is supposed to be authenticated in the CPN, while CPE residing the CPN will directly request IRG to IMS authentication, for services. IMS core network doesn't entail CPE to be separately authenticated for IMS services. So for this reason only users need to connect to the IRG to obtain the IMS access.

- **Dynamic User Authentication Support:**
  Since IRG is the form of residential gateway (RG) which authenticates the CPE [9] through NASS function i.e. Connectivity session Location and repository Function (CLF) manifest to uniquely obtain the CPE location for authentication mechanism, so every user connected to CPN have complete possibility of accessing IMS services defined on the user groups/policies authorizations.

- **User friendly, Simplicity and Usability:**
  The only requirement for connecting IMS core network through NASS [30] in this scheme is through ISIM module presence in IRG which makes it easy for the CPE to have simple connection with CPN. So every CPE, connecting CPN have access to the authenticate IMS service through IRG device present in CPN network. CPE connecting the CPN in a traditional way (wire line) is quite mature method and NASS authentication follows the same procedure. There are no extra requirements of ISIM module in the CPE; else the CPN may have its own authentication methods for connecting CPE's.

5.5.2 Weakness

- **IRG Dependence:**
  All the CPE's are dependent on the IRG and NASS [9] for connecting IMS network authentication and services. There is no alternate solution present, if some hitches occur at IRG or NASS except CPE should hold ISIM module individually to authenticate which is in fact Digest NASS and must not be considered as an alternate solution rather than solving existing hitches associated with IRG and/ or NASS.

- **Time Consuming:**
  The traditional authentication schemes for IMS authentication and services forward request to P-CSCF and so on, but with more subsystems i.e. NASS [31] deployments in the architecture will have definite impact on more signaling messaging between each significant NASS entity, to keep record of CPE's attached. Alongside each individual NASS entity will also have the risk to control CPE data flow which will have processing and delay in the individual sub system, so overall NASS can be affected due to enormous processing.

- **Increase Cost:**
  The solutions define for the NGN TISPAN [30, 9, 31, 32] involves hardware, software and functional /operation requirements that exhibits/ measures every single activity influenced by the cost factors involved. Generally, NASS will have impact on the operator budget to deploy NASS and higher IT staff for its maintenance and so forth. Also CPN requires healthy network infrastructure to filter the authorized users to access the IMS services through IRG.

- **No Mobility:**
  The release 7 of IMS is for NGN TISPAN [9], which offer implicit authentication base on line authentication i.e. layer 2 physical / logical identities. So for sure, the CPE are connected to through wire and have no wireless access procedure within the CPN.

- **CPN Security:**
  IMS and operator network losses the control of security at the CPN network, as every single CPE connected to the IRG absolutely acquire IMS connectivity due to NASS –CLF functionality. So, its uncontrolled form the operator and IMS network to identify single individual CPE instead of just authenticating IRG in the CPN network.

5.5.3 Opportunities

- **Security Improvements:**
  It's highly the responsibility of the CPN network administrator to cope with the unauthorized access to IRG at their side. To protect the network form an illegal use by enforcing strong security policy at CPN. Analyze, log and administer the network traffic and systems to make the CPE's authentication transparent and efficient. Govern IRG access to only limited/required number of CPE's based on high access security mechanisms that follow NIST guideline [24] "something you are" i.e. biometric procedure.

- **Required Mobility:**
  As [32] explores the description of CPE access network mechanisms in security perspective, the uniqueness of CPE access to IMS through IRG lies with CPN administrator. However, CPN might improve the mobility by connecting its CPN network through secure communication medium i.e. VPN. CPE's at connected to any end in the CPN cluster network will receive same set of service with wire line connectivity.

5.5.4 Threats

- **Customer/User Define Security:**
  The role of CPN administrator is highly critical at this stage when single entry point IRG access is available for multiple CPE's, including IRG security itself. IRG could be affected through DOS attacks initiating from CPN. It's not much clear about the IT staff requirements at the beginning and during deployment and configurations.

- **CPN Limitations:**
  There will be some limitations associated with the IRG CPE access, so not all CPE's residing in the CPN will have the possibility to access the service instantly, also limitation in the CPN network traffic is dangerous as the bandwidth is limited. Delay in the IMS access authentication could also be possible due to increase network traffic; mechanisms of user priority within the organizations are must to cope with the network congestion and QoS classes where the demand for IMS access is significant.
  Similar factors of carelessness at the CPN end referring to CPE/IRG theft (lost) and open connection line (RJ-45 connector) will have severe impact in the IRG access.

5.6 Digest NASS Authentication

STRENGTHS	WEAKNESS
• Security • User friendly and Usability.	• Limited Mobility/ Nomadicity • Complexity • Less Efficiency • ISIM and Device Dependence.
OPPURTUNNITIES	**THREATS**
• Security Improvement • Mobility Improvement	• Hardware Associated problems. • CPN Limitations.

5.6.1 Strengths

- **Security:**
  It follows NIST guidelines [24] two level security i.e. “something you have” that is the ISIM module present in the CPE and “something you know” as a http digest password for connecting RG i.e. may be IRG. So it offers acceptable level of security define in [32, 33] that NASS subsystem will enforce encryption for IP connectivity. Network Address Translation functionality is necessary for IP connectivity during transmission of digest password to NASS for authentication.

- **User Friendly and Usability:**
  Username password technique is a pioneer technique for authenticating users at systems, servers, services, etc, so users are often use to this technique and also use it without hesitations. Several aspects of username/ password technique are already defined in this report. Http digest mechanism is used in the technique which is transparent to the users and the control of user’s security, privacy and confidentiality lies in the strength of the passwords. Also ISIM module is present in the CPE [34] is similar to SIM modules in size and shape but different in functionality and operation, since users are used to SIM, they will find no difficultly in operating it through ISIM.
  Both user friendliness and usability of this authentication procedure is simple, understandable and adoptable easily.

5.6.2 Weakness:

- **Limited Mobility/ Nomadicity:**
  According to [30], the technical specification illustrate that in case of P connectivity only limited mobility/ nomadicity is achieved, which is actually due to the IRG present at the CPN. Since IRG will maintain well define signal and the number of users connecting the IRG for IMS authentication requires CLR approval, it's necessary to limit the user access to its just location.

- **Security:**
  There is very little possibility of IP spoofing as http digest mechanism is implemented which has shared key mechanism concatenated with time factor, so even if password is spoofed, sniffed and analyzed in the wireless traffic, the presence of ISIM module is highly required for reply attacks.

- **Complexity:**
  HTTP digest implement MD5 128 bit encryption algorithm and thus have manageable complexity in decryption at either side, defined earlier before. It's also difficult for the user to remember strong passwords which are required by IMS NGN.

- **Less Efficiency:**
  Due to complex encryption, use of password and ISIM module, and NASS function entities requires more time to evaluate the user for authentication. Information pertaining to CPE is contained at different location i.e. IRG/RG, NASS and IMS-UPSF, where each of them has to manage signaling and processing to authenticate, authorize, and assign CPE with its service profile. Wireless medium at the CPN may also invoke problems associated with CPN.

- **ISIM and Device Dependence:**
  An important aspect of this authentication is that every individual CPE have to implement ISIM module along with http digest mechanism. So CPE users are bound to maintain ISIM module, remember password and only connect through valid CPN with limited mobility. It's also noticeable that RG and NASS should also be present to access IMS network whereas, only ISIM module seems enough in other techniques defined latter.

5.6.3 Opportunities:

- **Security Improvements:**
  In order to obtain very level of security, security at CPN as well as "something you are" i.e. biometric information from NIST guidelines [24] should be implemented.

- **Mobility improvement:**
  Seamless access to the services requires mobility, whereas mobility leads to security breaches. To balance the probability in between them, it's possible to keep the security tight with implementing extra security i.e. biometric and thus allowing CPE to connect IMS network directly when outside of the CPN, it's because that ISIM module already exist in CPE and password is also required to authenticate, while it will full secure the authentication procedure. It may also be possible to interconnect CPN networks with secure connection to append access services during mobility.

5.6.4 Threats:

- **Hardware Associated Problems:**
  CPN plays vital role in offering wireless connection to connect NASS, so any problems associated with CPN network are destructive. In case of ISIM module theft, lost or damage a

new ISIM module required will have significant time factor involved whereas the security cannot be directly violated as password is also required to access IMS services.

- **CPN Limitations:**
  Limitations concerned with CPN are highly valuable as network traffic may become congested, signal strength maybe weak at certain indoor areas or due to jammer which contribute in deny or delay form the IMS service access.

Chapter 6 SWOT Analysis of SIM Base Authentication Schemes

6.1 IMS AKA/ISIM Authentication

STRENGTHS	WEAKNESS
• IMS level security/Low security risk. • User adoptability/Experience • Technology evolution • Technology Standard.	• Complexity • User friendliness • Hardware dependence • Technology Immaturity • Reduce Efficiency
OPPURTUNNITIES	**THREATS**
• FMC(Fix mobile conversion) • User Trust.	• Efficiency trade off • Network Behavior/Delay.

6.1.1 Strengths

- **IMS level security/Low security risk:**
  3GPP[35] defines mutual authentication for IMS access i.e. user UE authenticating IMS network and IMS network authenticating UE separately resides in IMS AKA, due to mutual authentication exchange of important information messages including XRES, RAND, CK,IK, AUTHN etc protects from IP spoofing, session hijacking ,man in the middle attacks and replay attacks. Cryptographic and integrity keys maintain IPSec Security Association (SA) restricting most of the security threats at the access network side.

- **User Adoptability/ Experience:**
  An existing of SIM technology composed of UICC card physical resemble to traditional SIM module, so ISIM module required for IMS AKA will have no implicit impact on the user usage and adoptability.

- **Technology Evolution:**
  The IMS AKA implements IP technology which is evolving in telecommunication; the core network had been highly emerged with IP solutions. The evident IMS AKA will probably progress to contribute in new technology evolution.

- **Technology Standard:**
  IMS AKA had been standardize by various 3GPP TS/ES [35] and thus holds significant importance for accessing IMS services.

6.1.2 Weakness

- **Complexity:**
  IMS AKA requires heavy algorithm computations [10] for deducing authentication vector (AV) parameters along with multi directional signaling traffic between UE and IMS network.

- **User Friendliness:**
  Depending on the user device interface design which exhibits authentication progress, time required for authenticating with the IMS network, UE operations and user experiences, it could be justified what the technique could yield but to view bit closer at the computational and signaling complexity to improve security which reflects that more time will be necessary to uphold the authentication procedure successful.

- **Hardware Dependence:**
  IMS AKA explicitly requires new hardware deployment at operator/provides core and access network side where as individual modules i.e. SIM/USIM present in the UE also need to be changed ultimately, which is however impossible due to time constrains, business policies, costs/expenses, and quality staff.

- **Technology Immaturity:**
  Due to supplementary researcher's interest and working in ISIM authentication access mechanism to IMS, problems yet lie behind foggy pathway. To accept technology evolution in an immature stage is a strong challenge to cater in the current industry.

- **Reduce Efficiency:**
  Complexity has severe affect on the overall functionality, thus in IMS AKA complexity posed due to increase security and reduces overall authentication efficiency, it could also because due to signaling messages between UE, HSS, CSCF, network, etc[10].

6.1.3 Opportunities

- **FMC(Fix Mobile Conversion):**
  IMS AKA is standard authentication schemes defined in the 3gpp specifications [35], and success to the IMS network implementation creates satisfactory results to cope with future implementations successive to FMC.

- **User Trust:**
  User behavior is undeterminable, although parameters affecting the users greatly concerns with users information, resources, and services security. IMS AKA completely promises to protect all the security attacks and enforces strong security (IPSec-SA) [10]. Matters concerning user friendliness and simplicity will improved successfully as researchers are producing their novel contributions in authentication mechanisms.

6.1.4 Threats

- **Efficiency Trade Off:**
  As the authentication mechanism comprises of multiple AV sent form HSS to S-CSCF, the need is dependent on the probability to determine UE connectivity/re-registration/re-authentication with IMS network. The fewer UE connects/re-register/re-authenticate with IMS network, the more efficiency decreases because the number of AV stored in S-CSCF will be useless if UE authenticates only for once. It mainly depends upon the UE availing IMS service/s, the type/kind of IMS service might hold enough information to measure the correct authentication scheme.

- **Network Behavior/Delay:**
  Since IMS AKA had be develop to implemented in the ISIM modules, with an increase in the number of UE, network traffic will increase and performance of the IMS equipments (HSS, CSCF, AS, etc) and network will also be degraded because IMSAKA have strong complexity.

6.2 One Pass GPRS Authentication

STRENGTHS	WEAKNESS
• Simplicity • User Friendly • Multi Purpose of hardware(SIM) • User adoptability	• Weak security
OPPURTUNNITIES	**THREATS**
• Security Trade-off	• Replay attacks • Unauthorized access • User confidentiality and data integrity • User trust/business good will

6.2.1 Strengths

- **Simplicity:**
  The authentication schemes [12] implements simple values without any strong parameter calculation and an advance transmission of the required messages are send form UE to IMS network.

- **User Friendly:**
  Reduce complexity gives rise to user friendliness and simplicity, due to less signaling messages between UE and IMS network less time is utilized which however states that users have little to wait for accessing IMS service with quite experience UE.

- **Multi Purpose of hardware (SIM):**
  Users are not forced to change their UICC (SIM/ USIM) cards temporary/ permanently, thus allowing those to access and use IMS service through their SIM cards. It maybe because users maintain their important information (contacts) in the SIM cards which they don't want to loss and also aims to access IMS services.

- **User Adoptability:**
  SIM card is around for several years and users have better adoptability/ familiarity with it, UE supporting ISIM card will require little effort to up fit and use it with new and exciting features and functionality provided by IMS.

6.2.2 Weakness:

- **Weak Security:**
  One pass GPRS [12] doesn't provide enough security as defined in the 3gpp[35] for IMS access, in fact it is vulnerable to all kind of security attaches i.e. IP spoofing, session hijacking, man in the middle attacks, eavesdropping, replay attacks due to lack of mutual authentication mechanism and implementation of IPSec SA (cryptographic keys and Integrity keys)[10].

6.2.3 Opportunities:

- **Security Trade-Off:**
  The only possibility to cope with the security threats is to protect communication between UE and IMS network; also it is necessary to define IPSec and mutual authentication for security improvements.

6.2.4 Threats:

- **Replay Attacks:**
  Due to eavesdropping, illegitimate user have the strength to produce replay attacks that highly affect user access services, information protection, IMS network resources, etc.

- **Unauthorized Access:**
  Mainly caused due to IP spoofing, session hijacking, eavesdropping, etc attacks on the user's privacy/ confidentiality and data integrity that can occur anytime.

- **User Trust/ Business Good Will:**
  Every user is keen to its information privacy and protections claimed by the business/ organization if devalued once, might have devastating effects in the long run.

6.3 Early IMS Authentication

STRENGTHS	WEAKNESS
• Simplicity • Network Integration Support • GGSN Base security • IMS Access without USIM/ISIM	• Security and Access Limitation • Network Hardware up gradation • Complexity
OPPURTUNNITIES	**THREATS**
• Time relaxation	• Security Risks

6.3.1 Strengths

- **Simplicity:**
  Early IMS define packet data protocol (PDP) context between UE and P-CSCF detained by GPRS through binding UE IP address. IP address had been used for authentication procedure for quite several years and there exist least algorithm computations.

- **Network Integration Support:**
  Early IMS maintain interim authentication solution with coexistence of SIP/IP core network.

- **GGSN Base Security:**
  IP spoofing is likely to be protected by GGSN [11], which might have NAT/firewall solution to filter the IP addresses.

- **IMS Access without USIM/ISIM:**
  Early IMS only uses UICC (SIM) module for authentication and user has great flexibility to access IMS service only through SIM module.

6.3.2 Weakness:

- **Security and Access Limitation:**
  Early IMS doesn't provide IMS level security but only an interim security i.e. access network or GPRS with PS domain through PDP context in UMTS, mainly lie on the underlying IP network [10] so the access independences is not encourage, also there is no IPSec SA's, and is unable to use IPv6 which is exclusively standardize by 3gpp [35] for IMS access. There is no mutual authentication, involvement of CK, IK, sequence number (SQN) [11] that arises major security attacks i.e. man in the middle attack, IP spoofing, session hijacking, and eavesdropping.

- **Network Hardware Up-gradation:**
  Possible hardware deployments are necessary to handle ISIM modules for authentication, however it's quite much to say as early IMS is only design to support SIM modules.

- **Complexity:**
  Since IMPU and IMPI are required for the IMS authentication, they are derived from IMSI for each user, along with this there is also enough communications between UE and IMS network.

6.3.3 Opportunities:

- **Time Relaxation:**
  The early IMS authentication schemes make use of the SIM and USIM modules and provide the network operators enough time to replace/upgrade the network and UE UICC cards simultaneously.

6.3.4 Threats:

- **Security Risks:**
  Possible security risk involves in the future are replay attacks, user information and data integrity/confidentiality, and access to IMS resources and services.

6.4 E-IMS Authentication

STRENGTHS	WEAKNESS
• Complexity • Security • USIM/ISIM support	• No SIM Support • Eavesdropping
OPPURTUNNITIES	**THREATS**
• Security protection	• User re-authentication Unpredictability

6.4.1 Strengths

- **Complexity:**
  E-IMS has complex algorithm for computing different values required during authentication procedure [13] i.e. mainly RAND, ITK, and DP. Apart from these extensive calculations, SIP and diameter messaging are reduced with respect to IMS AKA.

- **Security:**
  IMS level security in comprehended in E-IMS; mutual authentication, digest password, IPSec SA, use of CK and IK [13], etc are all utilize to fully secure the communication between UE and IMS network.

- **USIM/ISIM Support:**
  E-IMS only support USIM/ISIM base UICC cards in the UE which means that this authentication mechanism will support UMTS users along with IMS users to access IMS services.

6.4.2 Weakness:

- **No SIM Support:**
  Main disadvantage in E-IMS is that it doesn't support SIM module in the UE.

- **Eavesdropping:**
  Despite of strong security, eavesdropping can occur in the beginning of the session establishment but it has no ultimate effect on the security breaches, as reply attacks can't occur due to the use of RAND [13].

6.4.3 Opportunities:

- **Security Protection:**
  The key in pinching communication is eavesdropping, that could be possible in the beginning of E-IMS session establishment but high security implementation with an addition of RSN [13] protects form replay attacks even if once the communication had been scanned.

6.4.4 Threats:

- **User re-authentication predictability:**
  The only future threat seen in the E-IMS is that only single AV is computed for each single user [13], which means that for every re-authentication after session timeout, E-IMS have to repeat complete set of authentication procedure again causing an increase in complexity, simplicity, computations, etc, and session disconnection occurs at every session time out.

Chapter 7 Discussions

Research methodology approach illustrated in chapter 3 depicts the work flow where as in the beginning chapters we address introduction and problems associated with IMS security authentication to access seamless services. The expected results were achieved through SWOT analysis of Non SIM and SIM base authentication separately in chapter 5 and chapter 6 that makes considerable contribution in the selection of authentication schemes that are secure, simple, user-friendly and effective to deploy.

In research methodology, we follow simple and extensive technological and state of art study, further we get the outcomes based on the SWOT analysis tool, expectation of the study results are valid and significantly maximum.

Non SIM authentication schemes analyzed are username/ password authentication, short messaging service authentication, smart card authentication, MAC address authentication, simple network attachment subsystem and digest network attachment subsystem authentications. The first four authentication schemes does not require authenticating hardware i.e. UICC cards in UE except for smart cards which its self is a card and have more or less everything alike UICC card but different in size and shape describe earlier section 4.2, which helps to maintain NIST guidelines “something you have” and “something you know” two level security for MOBICOME project.

For Non SIM authentication, we address that we should allow some tradeoff between security, simplicity, complexity, and user friendliness, etc. our recommendations enlighten the selection and of following authentication mechanisms;

- Digest username/password scheme with protection form weakness and threats defined in section 5.1.2 and 5.1.4 which is possible to integrate with SMS authentication scheme to increase security and limit weakness and threats associated with username password schemes.

- We recommend implementing smart cards authentication alone because we obtain two level securities [24] if we can tradeoff between hardware dependability/ usage and its complexities defined in section 5.2.2 and 5.2.4.

- We cannot use SMS and MAC authentication schemes alone defined in section 5.3 and 5.4, and they are either integrated with other authentication schemes like username/password or avoided.

- NASS authentication has absolutely different mode of implementation with limited user mobility then other Non-SIM authentication schemes. We recommend simple NASS authentication if security at the CPN network is highly manage by the CPN IT staff, i.e. IRG containing ISIM module and UE accessing IRG to extend access to IMS network, otherwise we insist to implement digest NASS where each UE containing ISIM module separately and thus NAT is performed when accessing NASS system due to improve security describe in section 5.6.1 and 5.6.3.

Current SIM base authentications offer two level security “something you have” and “something you know” [24], although numerous security risks during accessibility are involved that have harmful results however we produce following complements.

- Early IMS authentication is necessary for 2G network accessing IMS services, but here what we can do is to control weakness and threats explained in the SWOT analysis.

- In case of UMTS and IMS subscribers (UE's) inhibiting USIM and ISIM UICC modules, it was analyzed that evolutionary IMS offers much similar security addressed by 3gpp specification for IMS access and authentication.

Above explanation extracted from SWOT analysis provide investigation about all IMS authentication techniques and is answer to our first research question.

Second research question states that we can integrate Username/Password with SMS and/ or with Smart Card to overcome username/password weakness and threats described in section 5.1.2 and 5.1.4.

"Security" of information concerns users including their privacy, confidentiality, secrecy, etc and also the network operators including their business, systems, networks, resources and services as whole is an answer to our third research question.

Chapter 8 Conclusions and Future Work

8.1 Conclusions:

In this thesis we have accomplish SWOT analysis of IMS security authentication schemes for IMS network services. SWOT analysis for IMS security authentication schemes are divided into two main categories i.e. SIM based authentication and Non SIM based authentication. Analysis results provided strengths, weaknesses, opportunities and threats about an individual authentication scheme. The selection of authentication scheme is important for design and development within the MOBICOME project. SWOT analysis tool itself exhibit necessary information for advantages and disadvantages.

The study holds significance, because of IMS deployment in the FMC environment to achieve seamless access to the services. The goal of the thesis was achieved by defining and selecting the most appropriate authentication schemes after conducting SWOT analysis in Chapters 5 & 6.

The Non SIM based authentication category contains six authentication schemes, i.e. username/password authentication, smart card authentication, SMS authentication, MAC address authentication, simple NASS authentication and Digest NASS authentication. The first four non SIM based authentication schemes have different mode of authentication as compared to the last two, because the former four schemes operate on wireless access mediums while the latter two schemes only operate through wired medium. This means that the non SIM authentication analysis will result in the selection of two authentication schemes, one for wireless medium and one for wired medium.

Our conclusions are based on the SWOT analysis and recommend the selection of the smart card authentication scheme for the first four non SIM based authentication schemes and the Digest NASS authentication scheme for the former two non SIM based authentication schemes. SWOT analysis in section 5.2 and section 5.6 explain the contents of the selected schemes in more detail.

The SIM based authentication category contains four authentication schemes, i.e. Early IMS authentication, IMS AKA authentication, Evolutionary IMS authentication and one pass GPRS authentication. The Evolutionary IMS authentication scheme is our recommendation for 3G and higher technology generations (UMTS, WIMAX, and LTE, etc) and IMS clients presented in section 6.4.

Since the one pass GPRS authentication is the only authentication scheme available for accessing IMS services, we have to select this scheme for implementation, but the SWOT analysis defined in section 6.3 will be helpful to minimize security risks associated with weaknesses and threats. The only possible opportunity is to wait until the telecommunication service providers move to new technology implementations and use USIM & ISIM for authentications.

8.2 Future Work:

There is much to perform in practical measurements for each set of authentication schemes addressed in the thesis report. Thus, we can investigate the true level of important parameter like security and complexity. Usability testing for user friendliness, simplicity, adoptability, awareness

and learn ability might based on user survey to observe user behaviors. However, usability studies address the suitable authentication scheme.

IMS test bed for simulating non SIM and SIM based authentication schemes will probably play a vital role once it is developed, as it will validate the selection of IMS authentication schemes. Hypothesis illustrated below could be highly valuable for future research studies:

H1: Is smart card authentication more secure than username/ password authentication, SMS authentication and MAC address authentication.

H2: Does Digest NASS offer higher security than Simple NASS authentication scheme.

H3: Does E-IMS provide less complexity than IMS AKA authentication?

Hypothesis H3 is related to the number of UE connectivity with IMS network. It's impossible at present to measure the UE authentication/ re-authentication with IMS network in specified time. After the IMS development and implementation in reality we can measure the minimum, average and maximum number of authentication and re-authentication attempts by a single user for different application services (Presence, Push to talk, VOIP, IPTV, etc). These measurements will provide investigation about the user behaviors with respect to different application services. The observations assist us to conclude appropriate authentication scheme for different application services based on user profile.

References

[1] M. Koukal and R. Bestak, "*Architecture of IP multimedia Subsystem," IEEE Multimedia Signal Processing and Communication, 48 international Symposium ELMAR.,* pp.323-326, June 2006.

[2] P. Miikka, M. Georg, K. Hisham, and N. Aki, *The IMS: IP Multimedia Concepts and Services*. 2nd ed. John Wiley & Sons, 2006

[3] Request for Comments: 3261, "SIP: Session Initiation Protocol," *Network Working Group*, June 2002. [Online]. Available http://www.ietf.org/rfc/rfc3261.txt [Accessed: Jan. 29, 2009]

[4] Y. B. Lin, H. C. –H. Rao, and I. Chlamtac, "General Packet Radio Service, Architecture, Interface and development," IEEE Wirel. Commun. Mob. Comput. , pp. 77-92, 2001.

[5] F. Muratore, *UMTS Mobile Communication for the Future.* Wiley, pp. 264, Jan 2001

[6] Request for Comments: 2617, "HTTP Authentication: Basic and Digest Access Authentication," *Network Working Group*, June 1999. [Online]. Available http://www.ietf.org/rfc/rfc2617.txt [Accessed: Jan. 20, 2009]

[7] B. Holcombe, "Government Smart Card Handbook", *U.S. General Service Administration.* Feb 2004. [Online]. Available: http://www.smartcard.gov/information/smartcardhandbook.pdf. [Accessed: Jan. 15th, 2009]

[8] 3rd Generation Partnership Project, "Technical realization of the Short Message Service (SMS), release 6," *Technical Specification Group Terminals*, 3GPP TS 23.040 v6.6.0, Dec. 2005. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/23_series/23.040/23040-660.zip [Accessed: Jan 16, 2009].

[9] European Telecommunications Standards Institute, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture; Network Attachment Subsystem (NASS)," *European Telecommunications Standards Institute,* ETSI ES 282 004, Feb. 2008. [Online]. Available: "http://www.tech-invite.com/Ti-tispan-standards.html [Accessed: Jan 26, 2009].

[10] 3rd Generation Partnership Project, "Technical Specification Group Services and System Aspects, 3g security; Access Security for IP-based services, release 8," *Technical Specification Group Terminals*, 3GPP TS 33.203, Dec. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/33_series/33.203/

[11] 3rd Generation Partnership Project, "Technical Security aspects of early IMS, version 8.0.0, Release 8," *Technical Specification Group Terminals*, 3GPP TR 33.978, Dec. 2008. [Online]. Available: http://www.3gpp.org/ftp/Specs/archive/33_series/33.978/

[12] Y. B. Lin, M. F. Chang, M. T. Hsu, and L. Y. Wu, "One-Pass GPRS and IMS Authentication Procedure for UMTS", *IEEE Jour. on Select. Areas in Commun.*, Vol. 23, June 2005.

[13] C. M. Huang and J. W. Li, "Efficient and Provably Secure IP Multimedia Subsystem Authentication for UMTS", *Oxford University Press, the Computer Journal, Vol. 50 No.6*, Oct 2007.

[14] J. Wolter, "A Guide to Web Authentication Alternatives", Oct 2003. [Online]. Available: http://unixpapa.com/auth/homebuilt.html [Accessed: Jan. 14, 2009].

[15] Request for Comments: 1321, "the MD5 Message-Digest Algorithm," *Network Working Group*, April 1992. [Online]. Available http://www.ietf.org/rfc/rfc1321.txt [Accessed: Jan. 29, 2009]

[16] Request for Comments: 4169, "Hypertext Transfer Protocol (HTTP) Digest Authentication Using Authentication and Key Agreement (AKA) Version-2," *Network Working Group,* Nov. 2005. [Online]. Available http://www.ietf.org/rfc/rfc4169.txt [Accessed: Jan. 29, 2009]

[17] Request for Comments: 2617, "HTTP Authentication: Basic and Digest Access Authentication," *Network Working Group*, June 1999. [Online]. Available http://www.ietf.org/rfc/rfc2617.txt [Accessed: Jan. 20, 2009]

[18] Request for Comments: 2069, "An Extension to HTTP: Digest Access Authentication," *Network Working Group*, June 1999. [Online]. Available http://www.ietf.org/rfc/rfc2069.txt [Accessed: Jan. 20, 2009]

[19] I. Z. Berta and Z. A. Mann, "Smart Cards – Present and Future," *Híradástechnika, Journal*, Dec. 2000. [Online]. Available: http://www.crysys.hu/publications/files/BertaM2000hir.pdf. [Accessed: Jan. 29, 2009].

[20] "ISO/IEC 7816 Part 4: Interindustry command for interchange," Nov. 26, 1998. [Online]. Available: http://www.ttfn.net/techno/smartcards/iso7816_4.html#ss5_2. [Accessed: Jan. 30, 2009].

[21] "Smart-Card-HOWT," Sept. 19, 2001. [Online]. Available: http://www.faqs.org/docs/Linux-HOWTO/Smart-Card-HOWTO.html#SMARTCARDINTRO. [Accessed: Jan. 30, 2009].

[22] "Smart card security from a programming language and static analysis perspective," Sept. 19, 2001. [Online]. Available: http://pauillac.inria.fr/~xleroy/talks/language-security-etaps03.pdf. [Accessed: Jan. 30, 2009].

[23] C. Barral and S. Vaudenay, "A protection Scheme for MOC Enabled Smart Cards", *IEEE Biometric Symposium*, 2006.

[24] NIST, *National Institute of Standard and Technology guidelines,* [Online]. Available: http://www.nist.gov/index.html. [Accessed: Jan. 15, 2009].

[25] M. A. Zomai, A. Josang, A. M. Cullagh and E. Foo, "Strengthening SMS-Based Authentication through Usability", *IEEE Int'l. Symp. On Paral. And Distb.Proces. with App.* 2008.

[26] 3GPP, Third Generation Partnership Project, [Online]. Available: http://www.3gpp.org/. [Accessed: Jan. 16, 2009].

[27] Y. Sheng, K. Tan, G. Chen, D. Kotz and A. Campbell, "Detecting 802.11 MAC Layer Spoofing Using Received Signal Strength", *IEEE the 27th Conf. on Comp. Comm. INFOCOM*, 2008.

[28] Q. Li, W. Trappe, "Light Weight Detection of Spoofing in Wireless Networks", IEEE Int'l Conf. on Mobile Ad hoc and Sensor System, 2006.

[29] Microsoft TechNet, "Recommendations for Small Office or Home Office Wireless Networks", Dec. 2006. [Online]. Available: http://technet.microsoft.com/en-us/library/bb727047.aspx#EGAA. [Accessed: Feb. 5, 2009].

[30] European Telecommunications Standards Institute, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture," *European Telecommunications Standards Institute,* ETSI TS 187 003, Feb. 2009. [Online]. Available: http://pda.etsi.org/exchangefolder/ts_187003v020101p.pdf [Accessed: Feb. 30, 2009].

[31] European Telecommunications Standards Institute, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture," *European Telecommunications Standards Institute,* ETSI TS 282 001, March 2009. [Online]. Available: http://pda.etsi.org/exchangefolder/es_282001v020000p.pdf [Accessed: March 2009].

[32] European Telecommunications Standards Institute, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security (SEC); Requirements," *European Telecommunications Standards Institute,* ETSI TS 187 001, Dec 2008. [Online]. Available: http://pda.etsi.org/exchangefolder/ts_187001v020105p.pdf [Accessed: March 2009].

[33] European Telecommunications Standards Institute, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threats, Vulnerability and Risk Analysis," *European Telecommunications Standards Institute,* ETSI TS 187 002, Dec 2008. [Online]. Available: http://pda.etsi.org/exchangefolder/tr_187002v020101p.pdf [Accessed: March 2009].

[34] European Telecommunications Standards Institute, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Service and Capability Requirements," *European Telecommunications Standards Institute,* ETSI TS 181 005, Nov. 2007. [Online]. Available: http://pda.etsi.org/exchangefolder/ts_181005v020401p.pdf [Accessed: March 2009].

[35] 3rd Generation Partnership Project, "Technical Specification series," *Technical Specification Group Terminals,* 3GPP. [Online]. Available: http://www.3gpp1.net/ftp/Specs/html-info/31-series.htm