RESEARCH ARTICLE OPEN ACCESS

GSM and UMTS Security

Amrita Sajja[1], D.K Kharde[2], Chandana Pandey[3]

Depatment Electronics and Telecommunication Engineering
Mahatma Gandhi Mission's College of Engineering and Technology, Kalamboli,Mumbai.

Abstract:

Due to the radio message between the user and the base location, security necessities and services of a mobile communication method differ extensively from those of a fixed set of connections. To identify the user for routing and charging purposes, there is no physical link in the form of a (fixed) telephone line between the user and the local switch. To stop impostors from taking on the radio path confirmation by means of cryptographic events is thus necessary, intercepting data or tracing the whereabouts of a user by listening to signalling data are other serious pressure.

Keywords **— GSM , Networking , UMTS, Communication system .**

INTRODUCTION

The fastest increasing service industry in the world nowadays is the Mobile communications; users not only talk over their cellular phones but also have right use to many other services such as internet access, chat services, online banking, data transfer, etc. are becoming very general in these days. But as services increase so do the security measures to be taken, more valuable and private in sequence is sent through wireless networks every day and this information has to go secluded from malintentioned community who may try to access it. With the older analogue-based cellular telephone systems such as the advanced mobile phone system (AMPS) and the total access communication system (TACS), it is a relatively simple matter for the radio hobbyist to interrupt cellular telephone conversation with a scanner.

Why Security more of a concern in wireless:

- no inherent physical protection
  - physical connections between procedure are replaced by logical associations
  - Sending and receiving messages do not need physical access to the network infrastructure (cables, hubs, routers, etc.)
- broadcast communications
  - wireless generally means radio, which has a broadcast nature
  - transmissions can be overheard by anyone in range
  - anyone can generate transmissions,
    - which will be received by other devices in range
    - which will interfere with other nearby transmissions and may prevent their correct reception (jamming)

GSM: Introduction, History and How It Works

GSM initially stood for The Group Special Mobile, a French group who wanted to create a digital standard for all European country that stayed as close to the recognized ISDN as possible. Eight years later, in 1990, using the equal initials, they created the first Global System for Mobile Communication specification. Today, it has come a long way and is now used by over a billion people, in over 200 countries, making it 70% of the world's mobile phone market.

GSM can handle three similar types of service. Bearer services are for interact with the IDSN and PSDN areas of the set of connections. Tele services are the basic services you expect from a mobile

phone: expert encrypted voice transmissions, Short Message Service (up to 160 characters) and fax facilities. These services were later enhanced when features such as the Wireless Application Protocol (WAP) promoted internet applications and the general packet radio service (GPRS) which enabled larger packets of data to be sent, hence adding extra features and a new 'data based' way for company to bill customers rather than the common time based way. Supplementary services are network provider services such as call forwarding and user identification.

The GSM Network is best described by contravention it up into its three main components. The Base Station Subsystem is made up of many base transceiver stations (BTC) which handles all reaction and communication to your mobile phone. These BTCs come in many shapes and forms, with different ranges and capacity. Together these BTCs form a cell formation to cover the entire area with cells, large and spread out in rural areas and small and tight in urban area. There even exist microcells for use inside in shopping centres, airports, etc. These BTCs be in touch with a base station controller (BSC) which controls the 'handover' (i.e. when you go from one cell to an extra, so that your call isn't dropped), 'paging' (i.e. sending out a signal to which a specific phone responds) and relating to the mobile switching centre (MSC).

This MSC is the backbone of GSM and is in the Network and Switching Subsystem. It performs tasks such as handover between diverse BSCs and additional services mentioned above. Also in this part of the network is the home location register (HLR) and visitor location register (VLR). These work together as a record of user information for all people in the system and the immediate location area. While the HLR stores the user records permanently, the VLR dynamically stores the user records of people in their position area to save time linking to the HLR.

The third component is the process Subsystem, which contains an authentication centre (AUC) and equipment identity register (EIR), is used for security.

GSM Security:

1. main security requirement

– Subscriber authentication (for the sake of billing)

- challenge-response protocol
- long-term secret key shared between the subscriber and the home network operator
- supports roaming without revealing long-term key to the visited networks

2. other security services provided by GSM

– Confidentiality of communications and signalling over the wireless interface

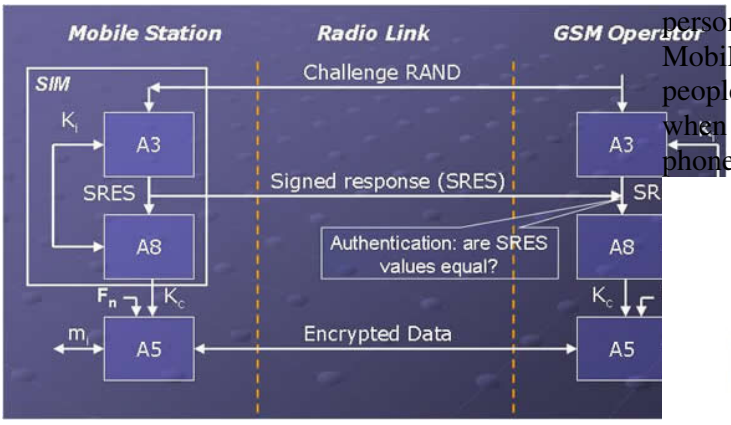
• Encryption key shared between the subscriber and the visited network is recognized with the help of the home system as part of the subscriber authentication protocol

– Protection of the subscriber's identity from eavesdroppers on the wireless interface

• Usage of short-term temporary identifiers

The SIM Card (Subscriber Identity Module)

- tamper-resistant
- protected by a PIN code (checked locally by the SIM)
- removable from the terminal
- contains all data specific to the end user which have to reside in the Mobile Station:
    - IMSI: International Mobile Subscriber Identity (permanent user's identity)
    - PIN
    - TMSI (Temporary Mobile Subscriber Identity)
    - Ki : User's secret key
    - CK : Ciphering key
    - List of the last call attempts
    - List of preferred operators
    - Supplementary service data (abbreviated dialling, last short messages received...)



The Algorithms:

The A3 and A8 algorithms implement on the SIM are generally used together as one algorithm (A38) to compute SRES and Kc in parallel. These two algorithms use COMP-128 a keyed hash purpose. It takes the 128-bit challenge, the 128-bit Ki as inputs and outs a 128-bit value, split into: 32bits of the confront, 32bits for the SRES, and 64bits for the Kc. This algorithm can be not working in about 8 hours, and the specification for COMP-128 is readily available on the Internet. This has led to new versions of COMP-128 coming out.

The A5 algorithm is a stream cipher. It is implemented very powerfully in hardware and the design was never made community. There are 3 different versions of A5: A5/1 a strong versions, A5/2 a weak version and A5/3 based on algorithms used n 3G phones. There is also A5/0 but it has no encryption.

These algorithms can also be split quite simply. By analysing the output of A5/1 for 2 minutes it can be broken in less than a second. The weaker A5/2 algorithm can be cracked in milliseconds and attacks against A5/3 have been described.

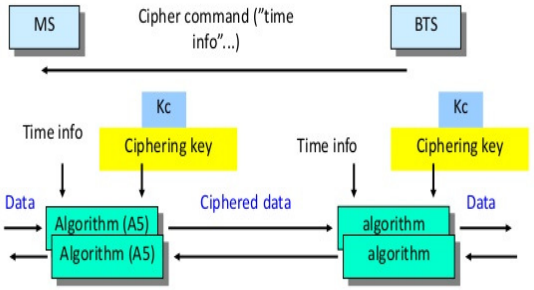
Equipment Security:

All handsets have an International Mobile Equipment Identity (IMEI) number that is stored in the Equipment Identity Register (EIR). This number is fully free of the SIM and completely matchless. The EIR has classifications for every IMEI number: White: Valid phone. Grey: Phones to be tracked. Black: Barred phones. (Lost or stolen)

User Security:

persons can be recognized by the International Mobile Subscriber Identity on their SIM. To avoid people listening for this a temporary IMSI is sent when communicate with the base station, when the phone is switched on or a call is being initialised.

Ciphering in GSM



For each call, a new ciphering key (Kc) is generated during authentication both in MS and MSC (in same way as authentication "response").

It used to provide over-the-air communication privacy in the GSM cellular telephone standard.

GSM security notes:

- focused on the defense of the air boundary
- no protection on the restless part of the network (neither for privacy nor for confidentiality)
- the visited network has access to all data (except the secret key of the end user)
- generally robust, but a few successful attacks have been reported:
- faked base stations
- cloning of the SIM card

UMTS - Introduction, History and How It Works

We live in scientific age where modern techniques in telecommunications maintain to allow us to move forward into a mobile world, allowing natural portability of information. Since the early 1990's market leaders such as Siemens have been increasing and humanizing 3rd

generation (3G) telecommunications values in order to provide bandwidths that would allow high quality video transmission. One of their aims was to define a worldwide traditional normal to give users international wireless treatment area of service. The result of this gave rise to UMTS (Universal Mobile Telecommunications System), as defined by the International Telecommunications Union (ITU).

UMTS technology is a further growth of the second generation GSM (Global System for Mobile) communication standard. It uses a new transport system for wireless data transfer between a mobile phone and a base station. UMTS aims to present a broadband, packet-based service for transmitting video, text, digitized voice, and multimedia at data rates of up to 2 megabits per second while remaining cost effective.
UMTS is built on top of the existing GSM infrastructure and integrates both packet and circuit data transmission. The design allows UMTS to be used in parallel with GSM therefore allow reception in areas where UMTS has not yet been completely implemented. Integration of these two workings leads to a smooth conversion into UMTS, so GSM is still very important and will continue to run in parallel for some years to come (as shown in the graph below). UMTS separates itself from GSM by using different occurrence bands. With its fast communication rates UMTS offers a wide array of multimedia services and parallel applications such as surfing the web while still talking on the phone.

The worldwide roving access provided by UMTS is implemented using a grouping of cell sizes, giving service to the isolated regions of the world. The cells are "In building" **Pico** cells, "Urban" **Micro** cells, "Suburban" **Macro** cells and "Global" **World** cells. FDD (Frequency Division Duplex) and TDD (Time Division Duplex) are the two in commission modes that allow users to avail from this wide range of usage. The FDD mode is apposite for general urban and rural areas and use W-CDMA to offer data rates of up to 384 Kbit/s with high mobility. TDD is suited for hot spots and common urban areas. It uses TD-CDMA, and operates in Pico and Micro cell environments. Mobility is low but data charge are high (2 Mbit/s). As TDD allows for asymmetric access mobile operator can offer portable broadband records service in areas of high density such as office complexes.

CDMA (Code Division Multiple Access) is an contact process that enables multiple participant to telephone consecutively via a single base station, while their conversation are kept separate. UMTS utilizes CDMA as it is far better suited for fast data stream transport.

UMTS Security:

The security Method of UMTS are based on what was implemented in GSM. Some of the protection functions have been additional and some existing has been enhanced. Encryption algorithm is stronger and built-in base station (NODE-B) to radio network controller (RNC) edge , the submission of validation algorithms is stricter and subscriber in secret is tighter.

The main security elements that are from GSM:

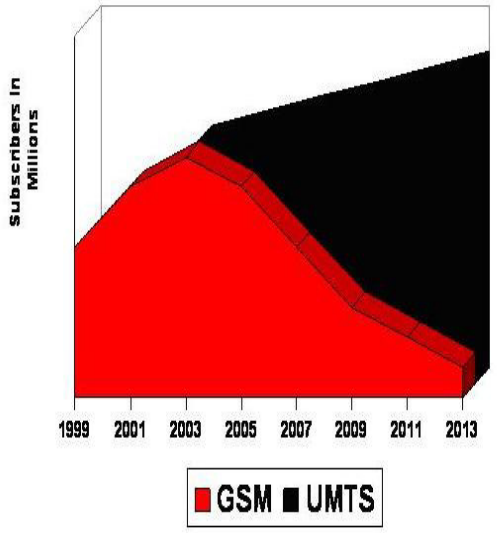
- verification of subscribers
- Subscriber identity confidentially
- Subscriber Identity Module (SIM) to be removable from terminal hardware
- Radio line encryption

Additional UMTS security features:

- Security against using false base stations with mutual verification
- Encryption extended from air interface only to include Node-B to RNC link
- Security data in the system will be secluded in data storages and while transmit ciphering keys and verification data in the system.
- Mechanism for improvement security features.

Core system traffic between RNCs, MSCs and additional networks is not ciphered and operator can to realize protection for their core network communication links, but that is unlike to happen. MSCs will have by drawing a lawful interception capability and access to Call Data Records (SDR), so all switch will have to have security procedures against unlawful right to use.

UMTS vs GSM Market Share Projections from 1999-2013 (voice and data)



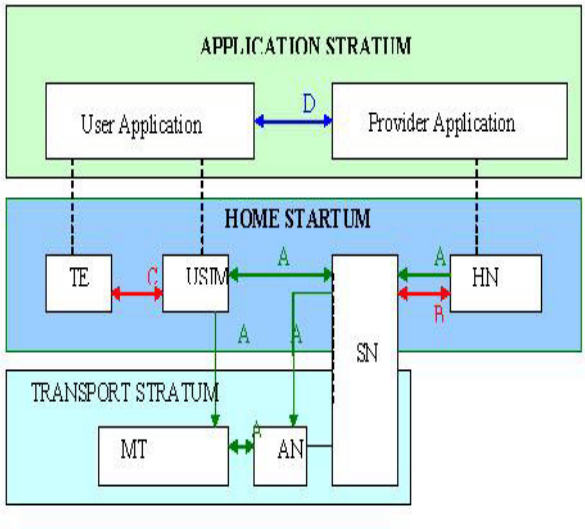
UMTS specification has five security feature groups:

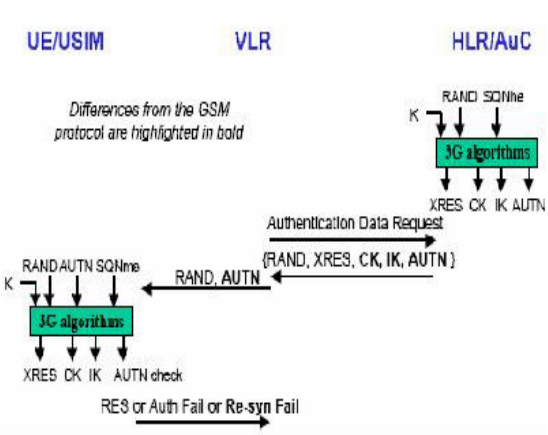
- **Network access security:** the set of protection features that give users with protected access to 3G services, and which in exacting protect against attacks on the (radio) access link;
- **Network domain security:** the set of protection features that enable nodes in the giver domain to securely exchange signaling data, and protect beside attacks on the wire line system;
- **User domain security:** the set of security features that secure access to mobile stations
- **Application domain security:** the set of protection features that enable application in the user and in the giver domain to strongly switch messages.
- **Visibility and configurability of security:** the set of features that enables the user to update himself whether a protection quality is in operation or not and whether the use and terms of services should depend on the protection feature.

UMTS specification has the following user identity confidentiality security features:

- **User identity confidentiality:** the property that the permanent user identity (IMSI) of a user to whom a forces is delivered cannot be eavesdropped on the radio access link;
- **User location confidentiality:** the property that the existence or the entrance of a user in a certain area cannot be firm by eavesdropping on the radio access association
- **User untraceability:** the property that an intruder cannot deduce whether unusual services are delivered to the same user by eavesdropping on the radio access link.

Air interface ciphering/deciphering in performed in RNC in the network side and in mobile terminals. Ciphering in function of air interface procedure Radio Link Control (RLC) layer or Medium right to use control (MAC) layer.





TE: Terminal Equipment
USIM: User Service Identity Module
SN: Serving Network
HN: Home Network
MT: Mobile Termination
AN: Access Network

Unlike GSM, which has verification of the user to the network only, UMTS uses mutual confirmation which resources the mobile customer and the serving system confirm each other, provided that safety against false base stations. This mutual confirmation uses an authentication quintet which helps to ensure that a bill is issued to the correct person. The confirmation quintet consists of the user challenge (RAND), expected user response (X(RES)), the encryption key (CK), the integrity key (IK) and the substantiation token for network authentication (AUTN). Also UMTS provides a new data integrity mechanism which protects the communication being signalled between the mobile station and the radio network controller (RNC). The user and system negotiate and agree on cipher and integrity algorithms. Both the integrity machine and enhanced confirmation combine to provide protection against active attacks on the radio interface.

K: Subscriber Authentication Key
SQNms: Sequence number information at user
SQNhe: Sequence number information at home system
UE: User Equipments / SIM
VLR: Visitor Location Register
HLR/AuC: Home Location Register/ Authentication Centre

UMTS provide improved encryption which ensures that communication is not available to not permitted users. With UMTS, encryption is completed in the radio network controller (RNC) rather than the base station, as is the case with GSM. The enhanced privacy has come about by using longer encryption key lengths, which (along with other UMTS safety functions) are easier to promote than the GSM counterpart. Also, as GSM's ciphering keys were not protected, UMTS added a privacy algorithm.

UMTS also provide diverse safety features for maintain identity confidentiality.

1) User identity confidentiality is maintained by ensuring the permanent user identity (IMSI) of a user using the service cannot be eavesdrop on the radio link.

2) User location privacy means that one cannot establish whether the occurrence of a user by eavesdropping on the broadcasting access link.

3) User unteachability ensures that it cannot be determined if special services are accessible to the same user by eavesdropping on the radio admission link.

It is clear to see UMTS boasts many safety compensation over GSM counting a data integrity mechanism, improved confirmation and encryption, identity confidentiality, a potential for secure roaming and superior facilities for upgrading. However UMTS also has security troubles. For example the whole lot that could happen to a preset host attached to the internet could also happen to a UMTS terminal. Also if encryption is disable hijacking calls is potential. And if the user is drawn to a false base station, he/she is ahead of reach of the paging signals of the allocation system. Finally when the user is registering for the first point in the serving network the permanent user identity (IMSI) is sent in cleartext.

UMTS,

- Inherits good practices from GSM
- UMTS R99 offers better subscriber safety than GSM
- New features are bilateral authentication and signalling integrity check
- Algorithms are public and longer keys are used
- Safety mechanisms between networks standardized in UMTS R4/R5

- Subscriber safety in IP Multimedia systems
- IPSEC is new mechanisms in IP-based networks
- Independent from radio technology
- Utilized methods that are already in use

CONCLUSION

We discussed GSM Mechanism, and later UMTS device and its capability over GSM. The access security mechanism in UMTS now protects against the false base position attacks which are not secluded in GSM. The privacy algorithm is stronger than its GSM antecedent. UMTS builds upon safety mechanism of GSM, and in adding provides subsequent enhancement,

- Encryption terminates at the radio network controller
- Mutual authentication and integrity protection
- Longer key lengths (128-bits)
- Network domain security using MAPSEC or IPSec

REFERENCES

(1) http://www.slideshare.net/Garry54/gsm-and-umts-security

(2) http://ntrg.cs.tcd.ie/undergrad/4ba2.05/group7/

(3) http://www.umtsworld.com/technology/security.html

(4) “Security of communication protocol” article and presentation by P.Perttula of Helsinki University of Technology.

(5). Images courtesy www.google.com