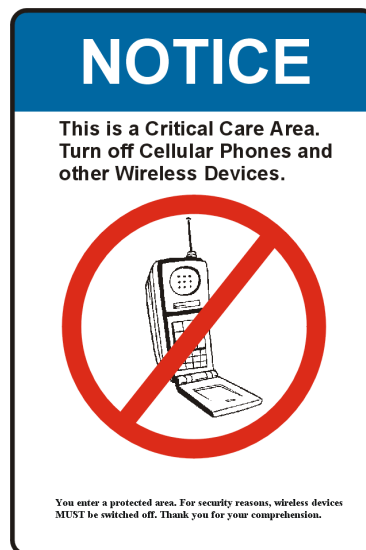

UMTS security

ESIEA - TOWARDS 3G NETWORKS

Pierre **BETOUIN** <betouin@et.esiea.fr>
<http://securitech.homeunix.org/>

June 20, 2006



Contents

	4	Attack vectors and entry points	6
1	Introduction		
2	Were older protocols so insecure ?	5	UMTS encryption enhancements
			7
3	UMTS security overview	2	6
			Conclusion
			9
	4		

1 Introduction

UMTS, which stands for *Universal Mobile Telecommunications System*, is one of the new third generation mobile cellular communication system, also called **3G networks**. It was built within the common "framework" defined by the ITU (International Telecommunication Union) in 1998. GSM technology, which could also be seen as the UMTS predecessor, is perhaps the most currently used technology, with approximately 650 million customers all over the world.

Mobility and compliant all-in-one cutting edge devices are becoming more and more present for everyone and require nowadays a high level of security : who wouldn't care about be eavesdropped, recorded and traced everywhere ? More than just a whim, security must be considered as a main goal for every project, since their beginning. Mobility introduces numerous new stakes towards new threats emerging. 3GPP — 3rd Generation Partnership Project — (eg. [3gp06]), is a collaboration agreement which develops new telecommunication standards, of which UMTS. This group has to deal with security as they bring new standards implemented in mobile devices. All modern technologies lead to security issues, as seen recently, for instance, with the Bluetooth protocol (eg. [BET06]).

UMTS will be surely one of the most audited protocols in the next ten years... A lot of security researchers will spend time and money testing this technology and maybe find security flaws (which could lead to serious threats in the future).

By the way, the race already began : @stake company (<http://www.astake.com>) , which was purchased by the famous Symantec one, was one of the first investigating security in UMTS technology (eg. [Whi04]).

This report is relative to Drago Hercog's course we had in 5th year at ESIEA school (eg. [Her06]). It was written with L^AT_EX.

2 Were older protocols so insecure ?

1G systems (NMT, TACS, AMPS) were almost deprived of any security mechanism and were thus vulnerable to numerous kinds of attacks : subscription spoofing, MiTM (Man in The Middle), etc. 2G GSM and 2.5G GPRS technologies came with these threats in mind and tried to avoid them using cryptography mechanism in order to provide integrity, confidentiality and authenticity through cypher algorithm. Authentication was provided with a one-way challenge-response handshake, which suffered of serious lacks (RAND, SRES were sent in clear text, as described in 5). As a consequence, the base station is not authenticated and therefore can not guarantee its identity to the mobile device (eg. [Koi02]).

Another serious flaw is due to the ability of the network to downgrade encryption, or

straightforwardly disable it...on the fly ! An attacker could then easily use this property to change this behaviour to fit his own requirements... Moreover, it is impossible for a mobile device to force encryption in a communication, the base station is the only one able to activate or disable it, so the user can not know, at any moment, if his communication is cyphered or not.

All these drawbacks had to be corrected and were taken into account since the early beginning of 3G networks.

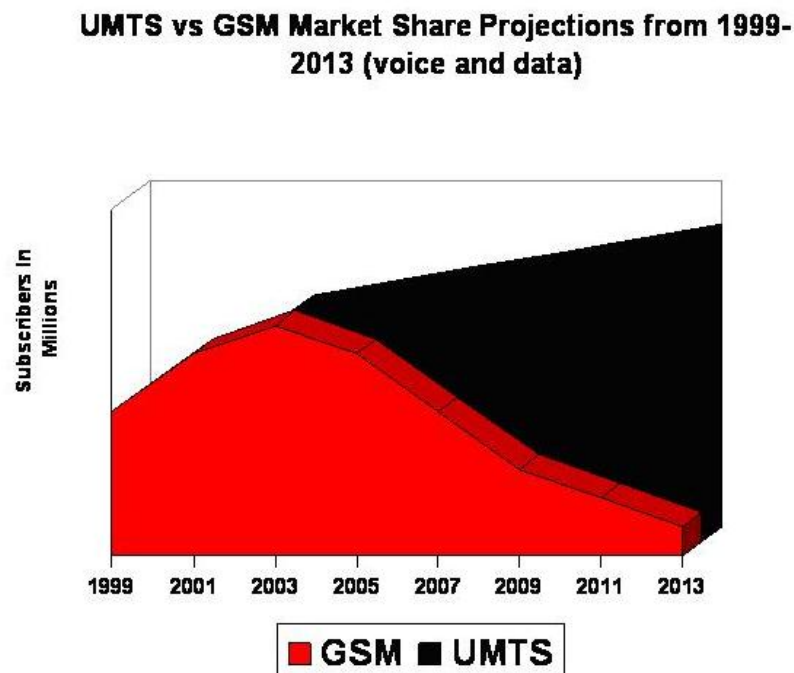


Figure 1: UMTS and GSM evolutions

As described on illustration 1, UMTS technology spreads very quickly since 2005. It is expected to be more used than GSM in the next five years. But as long as GSM will still exist, it will be possible to launch attacks using degraded modes. As all base stations do not support both technologies, devices use the best available and compliant mode. Therefore, a *Man in The Middle* attack through GSM mode (considered as degraded mode) could allow a malicious user to hijack the mobile device flow. As a matter of fact, it is then possible to silently forward packets, interrupt them, or even inject traffic (voice or data).

3 UMTS security overview

The major evolution concerning security in UMTS is, without any doubt, the "transparent" migration of the mobile technology towards IP networks, although lots of other additional changes occurred, like the radio media called UTRAN (*UMTS Terrestrial Radio Access Network*). It's indeed a major low level change in comparison to the GSM access to media method, but with less impacts on security than other upper protocols changes.

UMTS therefore introduces IP networks : "standard" security flaws are, nowadays, actively linked to this technology. If it could be expensive, a few years ago, to abuse of mobile technologies — using fake base stations for instance — it's now a common threat which must be taken into account. A such widely open protocol allows numerous kinds of attacks : it is clear that an unknown protocol (we should rather say "undocumented") is less targeted than an open one because it requires much more investigations. Some proprietary ones are moreover voluntarily obfuscated : the famous VoIP (Voice over IP) software Skype (<http://www.skype.com>), for instance, uses obfuscated binaries and protocols. Security analyses were slowed down a lot but security researchers (from EADS company) recently discovered many critical bugs which could lead to remote compromission, information disclosure. This is a great example to illustrate the fact that "security by obscurity" (which is a well known concept in IT security) is not reliable at all. It could be compared with cryptography algorithms: a reliable algorithm will never be considered as strong if the secret is based on the its own mechanisms. They must be instead based on the knowledge of a third information such as a secret key for instance.

Common sources of security related threats are located :

- In **Software security** : with development mistakes : memory concens (heap & stack overflows), format string bugs, design errors, race conditions, insane input data, escape characters, and so on. A non-patched Windows NT server in front of a UMTS device, for example, will be vulnerable to the same kinds of attacks as if it was located on an intrusted network, such as Internet ;
- In **Network topology** : known threats like flow redirections and modifications, MiTM attacks (*Man in The Middle*), or also passive sniffing : devices using UMTS are now part of a classical heterogeneous network ;
- In **Protocols** : clear-text exchanges (or weak encryptions), default passwords, replay attacks, session stealing, and so on.

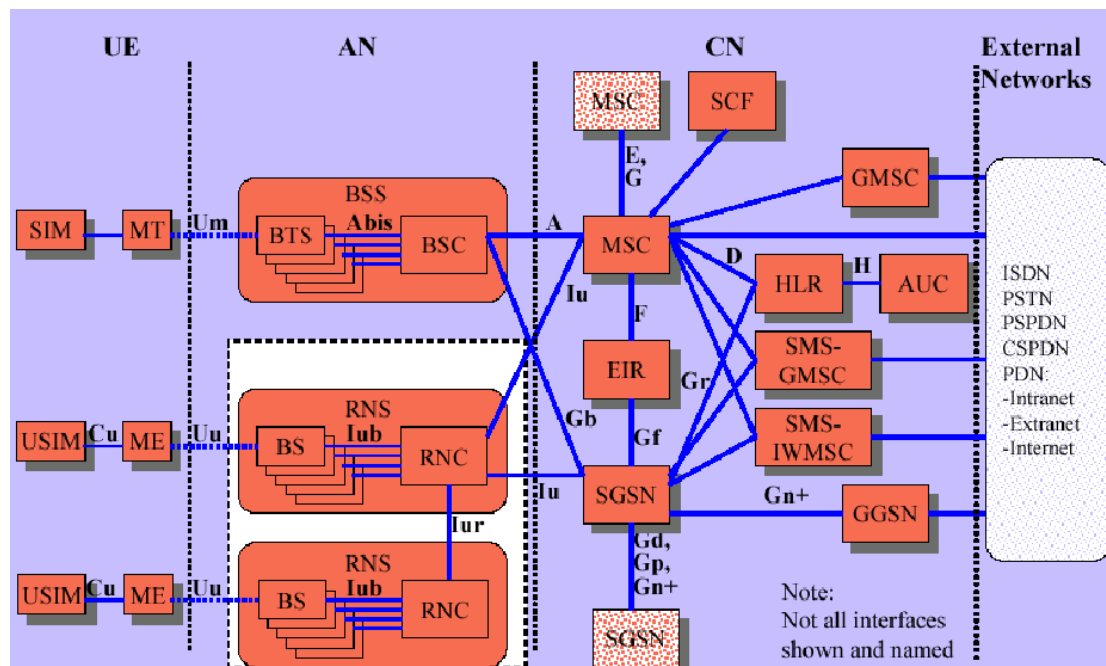


Figure 2: UMTS network design

Several “domains” are illustrated on 2:

- **UE** represents the remote device connectivity with the SIM card (containing cryptographic routines) ;
- **AN** could be seen as the *physical layer* (also call radio sub-system) of the wireless part with the BTS (Base Stations), which deal with electronic and transmission properties: transmission, modulation, coding, integrity checks...). The RNC (Radio Network Controller) works on a higher level and manages quality of service. It replaces the old GSM “Base Controller” (BSC) which had nearly the same function. It is also used to regulate the transmission power (and thus always try to keep a clean and standardized signal) .
- **CN** domain is, on the other hand, located beside the top level layer of the UMTS network. The MSC (Mobile Services Switching Centre) is responsible of conversions, handover between different BTS and also checks for subscribers’ features during outgoing call. The HLR (Home Location Register) is a kind of user database which records the “international user identity” (useful to recognize him in roaming conditions). The AuC (Autentication Center) is considered as the security backbone of the UMTS network, managing user credentials (secret keys), described in [?] ;
- **External networks** are linked through different protocols such as standard telephony PSTN, ISDN, LAN/WLAN...

Standard attacks, already existing on large and deployed networks, are in fact still possible. Even if mobile targets have some minor differences (almost on their architecture and operating systems, often proprietary), malicious exploitations must no longer be considered as fiction. UMTS devices, either for voice call or data purposes, have several specific stakes such as :

- **Anonymity and authenticity:** As a default behaviour, for instance, a phone number should not be revealed if the proper option had been set by the user. Even with anonymity constraints, authenticity should also be guaranteed to ensure that the calling number (if not restricted) is the real remote user number. These two properties (both anonymity and authenticity), needed at the same time, are not so common in security ;
- **Confidentiality:** a conversation between two users (or even a data communication) should be kept secret and remain confidential. Third party attacks must not occur in any case ;
- **Integrity:** End-to-end communications should not be modified. This feature could be managed towards cryptographic mechanisms. Hash functions do not need to be used on a tunneling context (full ciphered tunnel) when relevant cryptographic choices and implementations have been made (padding, strong algorithms and credentials...).

As this technology also deals with wireless issues, it is therefore especially vulnerable to eavesdropping attack schemes.

4 Attack vectors and entry points

- **GTP** (*GPRS Tunneling Protocol*), which enables GPRS support nodes in a GPRS network (both GSM and 3G) to communicate with each other uses UDP (User Datagram Protocol) as transport layer. A such compromise would be full of consequences : imagine the case where a malicious user, after having compromised the remote GTP server, installs a backdoor which would be automatically deployed on other remote devices (eg. [Fle05]) connected to the network ;
- **SS7** (*Signalling System 7*), is a kind of "gateway" protocol which translate a computed PSTN traffic to a IP compliant one using NAT techniques (Network Address Translation). This is also called "soft switching". Specific crafted buggy packets (buffer overflows, integer overflows, etc.) could affect a gateway, depending on its SS7 implementation (remember the recent ASN.1 bug) ;
- **SIP** (Session Initiation Protocol), **IAX** or **H323**, voice signalization protocols, could also be affected to these attacks ;

- **WAP** (Wireless Application Protocol), and any other kind of application server. WAP uses tags (as HTML does) and is therefore victim of numerous application flaws ;
- **Off the shelf components vulnerabilities**, which could be easily adapted to mobile devices (handhelds, smartphones, laptops...). *Full disclosure* mailing-lists, such as Bugtraq (eg. [Bug06]) for instance, often release vulnerability exploits (*Proof of concept*). 0-days — non-public exploits — are also in the wild!

5 UMTS encryption enhancements

2G mobile Networks were designed with a 64 bits A5 symmetrical algorithm, but most of operators used only 54 bits for performances reasons and law issues : some countries indeed used to restrict symmetrical cipher key lengths (eg. [BHHN05]) : the top 10 bits of the cipher key being often set to zero.

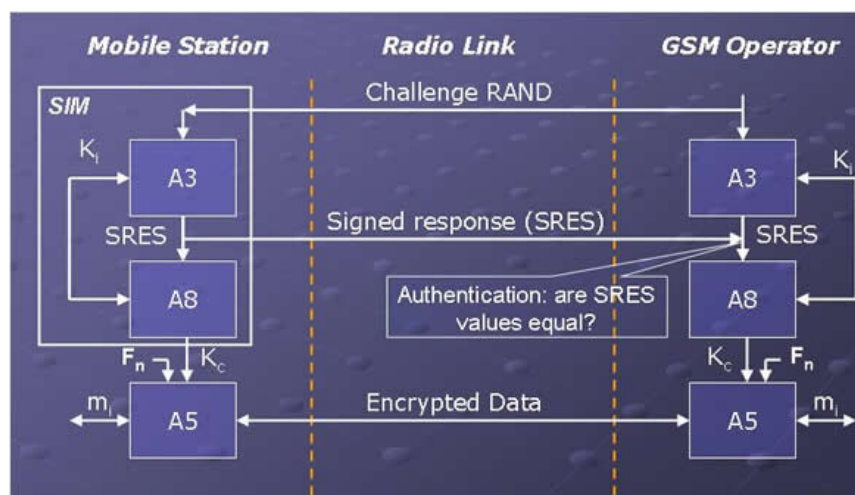


Figure 3: 2G A5 cipher algorithm

The "challenge/response" mechanism is still used in UMTS (SRES is the ciphered random challenge : RAND).

A5 algorithm, having several famous weaknesses (it could be broken within only 5 hours on a standard hardware configuration), was replaced by KASUMI (containing GEA, GEA2, and GEA3 128 bits sub-algorithms) for encryption and MILENAGE for authentication in UMTS technology, which is considered as a much stronger one. UMTS also provides

mutual authentication between the subscriber and the network with X509 signed certificates. Authentication's aim is to ensure that both client and remote nodes are allowed to initiate a communication and are what they claim to be (thus avoiding rogue station or client spoofing). This last feature enhances considerably mobile network security. GSM and other older technologies were indeed vulnerable to rogue base stations. This attack lets a malicious user to hijack a communication between a mobile device and a legitimate base station. A stronger signal (for instance using a more powerful antenna or being very close to the target), claiming to be the legitimate base station — with an equivalent configuration — will force the device to use it as new base station. This is due to roaming functions (dynamical base station switching), which are very useful when a mobile device is moving from one cell to another (eg. 2).

6 Conclusion

UMTS made a major breakthrough in mobile telecommunications. Security, which is more and more required nowadays, was clearly integrated to this technology since its beginning. As a matter of fact, UMTS provides a strong level of authenticity, integrity and confidentiality for end users. Thereby, added to many new kinds of services (Voice over IP, multimedia services, realtime streaming...), UMTS should replace so quickly older technologies in the next coming years. Prices, inevitably high when new products are sold, will decrease and then allow a large number of users to get rid of their old cellular phones.

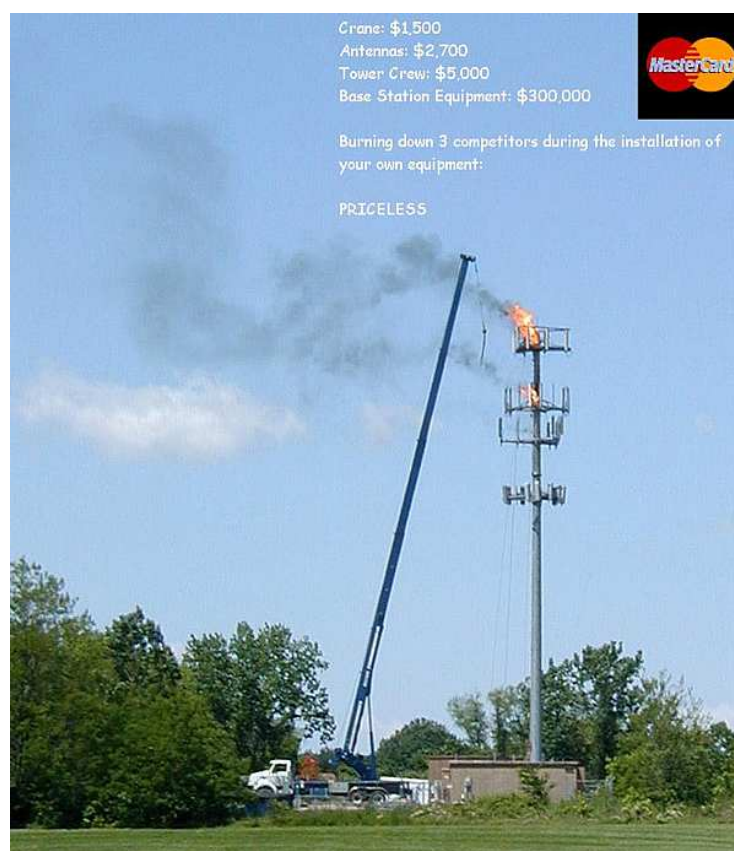


Figure 4: When physical security interferes with logical issues...

References

- [3gp06] 3GPP. – Shaping the future of mobile communication standards. – 2006. <http://www.3gpp.org/>.
- [BET06] BETOUIN (PIERRE). – Bluetooth (in)security. – 2006. <http://securitech.homeunix.org/blue/>.
- [BHHN05] BOMAN (K.), HORN (G.), HOWARD (P.) et NIEMI (V.). – Umts security. – 2005.
- [Bug06] BUGTRAQ. – Full disclosure mailing-list. – 2006. <http://www.securityfocus.com/>.
- [Fle05] FLEXTRONICS. – Gtp overview. – 2005. http://www.hssworld.com/mobile/stacks/GPRS_TUNNELING_PROTOCOL/overview.htm#gtp.
- [Her06] HERCOG (DRAGO). – Towards 3g networks. – 2006. <http://protokoli.fe.uni-lj.si/~esiea/>.
- [Koi02] KOIEN (GEIR M.). – An involved umts network domain security. – 2002.
- [Whi04] WHITEHOUSE (OLLIE). – Attacks and counter measures in 2.5g and 3g cellular ip networks. – 2004. http://www.blackops.cn/whitepapers/atstake_cellular_networks.pdf.

List of Figures

1	UMTS and GSM evolutions	3
2	UMTS network design	5
3	2G A5 cipher algorithm	7
4	When physical security interferes with logical issues...	9