3GPP TSG-SA WG3 Meeting S3#37
Sophia Antipolis, France, 21-25 February, 2005

Tdoc ⌘S3-050068

CR-Form-v7.1

PSEUDO-CHANGE REQUEST

⌘ CR xxx ⌘ rev - ⌘ Current version: ⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: UICC apps⌘ ☐ ME ☐ Radio Access Network ☐ Core Network ☒

Title:	⌘	Update for Access Security Enchancements Feasibility Study
Source:	⌘	Ericsson
Work item code:	⌘	GERAN
Date:	⌘	14/02/2005
Category:	⌘	
Release:	⌘	Rel-7

Use one of the following categories:
F *(correction)*
A *(corresponds to a correction in an earlier release)*
B *(addition of feature),*
C *(functional modification of feature)*
D *(editorial modification)*
Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use one of the following releases:

Ph2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
Rel-4	*(Release 4)*
Rel-5	*(Release 5)*
Rel-6	*(Release 6)*
Rel-7	*(Release 7)*

Reason for change:	⌘	Update of document
Summary of change:	⌘	
Consequences if not approved:	⌘	

Clauses affected:	⌘	

		Y	N		
Other specs Affected:	⌘		N	Other core specifications	⌘
			N	Test specifications	
			N	O&M Specifications	

Other comments:	⌘	

Title: Vulnerabilities and Enhancements for GERAN/UTRAN Access Security ~~Review~~and GSM/UMTS Security Context

1 Introduction

In a previous contribution, [15], Ericsson proposed a new work item to study long-term security enhancements to GERAN and UMTS access security. The following is a draft TR *[ed note: currently on "outline" level]* for discussion and an invitation to further contributions towards finalizing the study.

SA3 has agreed on short-term solutions to mitigate the worst effects of discovered A5/2 vulnerabilities. SA3 has also agreed that long-term security enhancements are needed to protect GERAN Access Network in the future. A deeper study of GERAN security weaknesses, in particular security dependencies between various uses of the GSM security context, and consideration of potential future attack scenarios is needed, to decide on suitable long-term enhancements of security for GERAN Access Network and other access types relying on GSM security context. Similar considerations for UMTS access security are also taken into account in order to evaluate and re-assess UMTS security features for future attack scenarios, not originally considered.

2 Definitions and Terminology

~~**GERAN security**: tbd~~

~~**UMTS security:** tdb~~

GSM security context: see [19].

UMTS security context: see [19].

AG: Access Gateway. A node on the border between the access network and the Core Network with the property that it is trusted to terminate the access security. E.g. for UMTS the AG is the RNC, for GSM it is the BTS, etc. *[ed note: should we be even more general and open up for terminating GSM security in another place? Seems a quite tough change…]*

PDG: Packet Data Gateway

AN: Access Network.

CN: Core Network.

DoS: Denial of Service.

One-way function: a function easy to compute but infeasible to invert.

SSO: Single Sign-on.

TE: Terminal equipment. This consists of the subscriber's 2G MS/3G UE together with SIM/UICC, as well as any other device that can access and use GSM/UMTS security context information such as RES/SRES, KC/CK/IK, etc. Thus, a laptop with a SIM card reader is considered TE, even if no mobile phone is used.

GERAN security: Any and all security and privacy aspects related to the protection of GSM security context and Layer 2 traffic (user plane CS/PS, and signaling) carried in GERAN between the TE and the CN, and any other security function (e.g. application layer) building on these.

UMTS security: As above, but for UMTS/UTRAN.

2.1 Network Model

Since the study covers GERAN, UTRAN and any other access technology, interworking with GSM/UMTS security context, we shall use the following abstract network model.

<Ed note: insert a figure showing a TEs with "SIM", and three access networks; GERAN, UTRAN, and "other access", together with the corresponding AGs>

3 Scope

<Editor's note: this section should define the scope of the study>

The high-level objective is to analyze the potential vulnerabilities and threats coming from the re-use of security context between ~~GSM,~~GSM and ~~GPRS~~ UMTS (and other access networks) in the absence of security features such as strong algorithms, network authentication, key separation, etc. Interaction between GERAN/UMTS/other access during hand-over is also to be considered. ~~Finally, the security objectives under which UMTS security was designed are to be re-evaluated to assess the long-term security of UMTS in new attack scenarios and threat models, and effects of re-use of UMTS security context~~.

Details in the scope of the study are ~~to~~

- Re-assess the security objectives for GERAN ~~and UMTS~~ security, i.e. consider whether the security objectives that were deemed required at the time GERAN~~/UMTS~~ security was designed is still sufficient or not.
- Perform a threat, risk and vulnerability analysis of GERAN and UMTS access security. This should in no way be limited by e.g. A5/2 cipher vulnerabilities, but should rather look at (at least) those issues raised in [15].
- The study should take into account known potential threats and vulnerabilities, and should also try to identify new ones with a clean-sheet approach.
- Provide a survey of long-term countermeasures to limit these threats and risks. A possible countermeasure should not (at this point) be ruled out just because it would imply major changes, such as e.g. phasing out legacy SIMs. (In other words, no part of the GERAN/UMTS "security context" is by default left out from the study).
- Study the feasibility of the introduction of these countermeasures in the time-frame of 3GPP Release 7~~Y~~. This includes not only cost of implementation, but also migration and backwards compatibility issues.
- Suggest a set of feasible to implement, long-term security enhancements to GERAN (and possibly UMTS) that reduces relevant risks/realistic threats.

~~Specific issues to consider include (but are not limited to):~~

- ~~The need and feasibility for network authentication, replay protection and key separation~~
- ~~Need and feasibility for integrity protection of important signaling messages~~
- ~~Effects of a near-future break of A5/1, GEA1 and/or other algorithms.~~
- ~~Risk assessment of implications of "two-time pads"~~
- ~~Ensure protection both for the PS and CS domains, in particular that possible insecurity does not spread across domains.~~
- ~~Study effects relating to inter-system handover and security context re-use or re-mapping.~~

- ~~Consider new threats, e.g. caused repudiation scenarios and effects of using GSM/UMTS security context for other accesses, e.g. WLAN~~
- ~~Consider security "bottlenecks" arising from different sizes of keys and other security parameters in the various access types, in particular enhancing the GERAN radio interface ciphering mechanism so that it supports key lengths of up to 128 bits.~~
- ~~Study the possibility of using AKA and AKA based applications for enhancing security.~~

3.1 Non-issues

The following issues are explicitly left outside of the scope:

- DoS attacks of pure radio interference or "jamming" nature.
- Cryptographic analysis of individual algorithms.
- ~~…~~
- While it is possible for operators to define their own AKA algorithms, we shall not consider possible desire to maintain the secrecy of these algorithms as part of the scope. Indeed the study shall be based on the assumption that all algorithms (including COMP and GEA variants) are publicly known.
- …

4 Threat and Risk Analysis Methodology

Every threat/risk analysis starts with *a system description*. In this case the system is rather well known, so the main purpose is to define which parts of the ~~GSMGPRS//UMTS~~GSM/GPRS/UMTS networks that are part of the study. Also, we may need to make *assumptions* about changes that may have been introduced in the time frame of Release ~~Y~~7, e.g. the disabling of A5/2 in R6.

Next, we define which *assets* that are desirable to protect and classify them according to sensitivity/value.

The consequences of the attack on A5/2 are highly dependent on the resources of the attacker. For instance, casual eavesdropping requires modest resources, whereas the active attacks (false base stations etc) require substantially larger resources. Therefore, we define which *attackers/threat agents* we consider relevant, and classify them into categories.

~~Finally,~~After this, we define a *trust model* reasonable for use in Release ~~Y~~ 7 time frame. It is clear that with public WLAN access, re-use of (U)SIM authentication, etc, the trust model may be quite different than that used in the original design of GSM.

Then, *threats* to these assets are identified after which i~~t~~t is then investigated which threats ~~against the assets~~ that seem practically possible to be realized. During this investigation there is only a coarse-grained attempt to qualify how probable a particular threat is.

As the next step, the *risks* posed to the assets are evaluated. The risk is measured as a function of the probability that the threat is instantiated and the cost of damages, specifically, the risk is the expected damage:

RISK = f(PROBABILITY_OF_THREAT_REALIZED, DAMAGE),

for some function f.

The PROBABILITY_OF_THREAT_REALIZED, in turn, is the total probability over all attacks leading to the threat's realization. We will use a scale of 1-5 for *seriousness*, 5 being the most serious, and we similarly estimate probabilities on a 1-5 scale, 5 being the most probable, as follows:

	Threat Seriousness	Attack Probability
1	**Minimal** Example: ~~Attacks that only causes annoyance for a single user during a short period of time.~~Threats that would not imply anything for user privacy, QoS, or charging, e.g. being able to occasionally increase a phone's transmit power.	**Negligible** Example: ~~Threat realized~~Attack successfull with a probability comparable to guessing/breaking an (at least) 80-bit key, or requiring resources equivalent to breaking such a key. Alternatively, requiring full control of some critical function e.g. the AuC, from the "outside". (Note: 80-bit is marginal if one considers attacks by "national agencies".)
2	**Small** Example: Threats that, if realized, only causes very small annoyance for a single user during a short period of time.	**Unlikely** Example: Organized crime with considerable resources would only occasionally be able to mount a successful attack.
3	**Medium** Example: Local ~~attacks~~threats, e.g., DoS targeted at a small set of BTSes under a single BSC. Could occasionally lead to single instances of incorrect charging data.	**Medium** Example: Organizations, capable of erecting rogue network GERAN/UTRAN equipment, e.g. base-stations, are likely to be able to ~~realize the threat~~succeed.
4	**High** Example: Something that, if realized, would be mentioned in IT/telecom media.	**High** Example: Qualified/resourceful individuals or small groups, e.g. capable of manipulating consumer products on a limited scale, could ~~realize the threat~~succeed.
5	**Very high** Example: Something that would make front-page news, seriously damaging the trust in mobile networks, either from users' or operators' point of view, e.g. complete loss of privacy and/or robust charging.	**Almost certain** Example: The ~~threat~~attack is ~~easily~~performed realized by single, averagely skilled "hackers" with standard PC/phone resources, possibly using "attacking tools" developed by someone else, found on the Internet. Cryptographic complexity: 40-bits or less.

Note that there is no correlation between the seriousness and the probability columns in the table above, i.e. a threat's seriousness can in principle be completely independent of the probability that it is realized.

5 System Description

5.1 Assumptions

<Editor's note: list assumptions, e.g. that A5/2 have been removed in this time-frame>

We shall make the assumption that the following holds for 3GPP Release 7~~Y~~:

1. A5/2 has been disabled from TEs.
2. Any possible new access technology that uses GSM/UMTS security context information has a well-defined AG.
3. All security algorithms are known, and *can* be analyzed by the public.
4. The Lawful Intercept systems are working properly and cannot be used by attackers to circumvent protection.
5. …

5.2 System

The system under study consists of

- the AN user and control plane traffic (GERAN/UTRAN/WLAN,…), from TE to the AG and CN,
- the security processing in AuC, MSC/VLR, BSS, AG, PDG and TE,
- any application service relying on GSM/UMTS security context, e.g. a server using SIM based SSO, GAA/GBA, etc,
- the (U)SIM and its communication with external entities such as TE,
- …

5.3 Assets

<Editor's note: what are the assets we may want to protect>

User data: user payload (CS or PS) in the AN.

Security context data:

- the subscriber key, Ki,
- replay counter, key sequence number (where applicable),
- SA data (Kc, CK, IK, etc),
- user identity, IMSI/TMSI,
- …etc

Control signalling: ~~any other~~ signalling in the AN/CN:~~, e.g.~~

- radio resource management (including AKA procedure, cipher mode command, etc)

- ~~management,~~ mobility/hand-off signalling (including triplet/quintuplet transport etc),
- call set-up~~connect/disconnect~~ signalling,

~~etc.~~ *[ed note: should this be further classified, e.g. signalling "releasing" the phone from the network ?]*

Security signalling: higher layer signalling, directly related to security context:

- IPsec tunnel establishment for integrated WLAN or other interworking access,
- GAA/GBA related signalling,
- …etc.

<Editor's note: a "value" classification is ~~missing~~TBD in connection to the risk analysis>

5.4 Actors and Threat Agents

<Editor's note: who is the attacker (mafia, terrorists ,what resources?)>

The following are the main actors, which to varying extent (see next section) are trusted by each other:

Subscriber: ~~…~~The TE user who has a subscription with an operator.

Home ~~network:~~ operator: The operator with whom the subscriber has a contractual agreement for the access service.

Home network: The network used by the ~~h~~ome network operator.

Visited (access) network: A network to which the subscriber is attached, that is owned by an operator different from the subscriber's home network operator.

Visited operator: The operator of a visited network.

…

The (untrusted) threat agents are classified as follows:

Insider: Dishonest p~~P~~erson working for operator and/or manufacturer of (U)SIM.

Outsider: Any of the following.

Pedestrian hacker: a single (or a small group of) individuals which are assumed to be able to launch passive attacks on the radio interface and with computing power equivalent of a small number of workstations/PCs connected to the Internet. This type of attacker can however be assumed to be able to transmit in unlicensed spectrum using off-the-shelf equipment such as WLAN cards.

Organized crime: "cyber terrorists" or resourceful organization, powerful enough to put up false 2G/3G base stations, large computing power, etc. Such an organization could potentially bribe an **insider**, but in that case we consider the attack as mounted by the **insider**. Note that an operator performing an attack against another operator is considered as an **Organized crime** unit.

Agency: an extremely resourceful organization, e.g. a national agency.

We shall, however, not consider attacks be agencies in this study.

…

5.5 Trust Model

<Editor's note: in the time-frame of Release ~~Y~~7, how much do operator trust subscriber, does home trust visited,WLAN access operator, UMA access,… etc>

TBD.

6 Security Objectives

<Editor's note: list the "standard" security objectives, then those that were considered when designing GERAN/UMTS, also list those that may now have shown up as new requirements>

In the following, we ~~re-asses the need for~~briefly survey the most common security objectives, some of which were considered irrelevant or found to be met implicitly when designing GSM security.

6.1 Confidentiality

Due to the nature of wireless communication, the need for confidentiality protection of the access has never been questioned, and it is obvious that future mobile networks must strive to meet this security objective.

6.2 Integrity

From 3G systems and onwards it has been deemed necessary to provide integrity for signalling but not for user data. However, there is clearly a big difference in difficulty between injecting/forging traffic on WLAN access respectively GSM access. The need for more robust charging may be reason to re-assess this requirement.

6.3 Authenticity

Subscriber authentication has from the start been an obvious security objective, if for no other reason to ensure robust charging. 3G and newer accesses have identified the need for strong authentication (mutual authentication with replay protection). Note that unless integrity protection is used, the reliability of authentication depends on the frequency of re-authentication. In fact, in scenarios where pairwise shared keys are used, authenticity and integrity are in direct correspondence; you cannot have one without the other

6.4 Non-repudiation

In both GERAN and UMTS access, the visited network is trusted to authenticate the user and to produce correct charging data. This means that a user who complains about a phone bill currently has no "cryptographic" evidence speaking either for or against him. Nor does the visited network have any "proof" of the user's presence in the network. This model has changed slightly in IMS access, where the home network performs the authentication, and there may be need to re-assess also if this objective should be more strongly enforced.

6.5 Availability

~~TBD.~~While we do not consider attacks of "radio jamming" nature, other aspects are of importance for the study. For example, the subscriber should not loose network attachment, except if radio contact is lost/degraded. If the TE is handed over to another base station, there should indeed be a base station there to continue the service, etc.

6.6 Privacy

On the “access level”, the important aspects of privacy are: protection of subscriber identity and location, protection against unsolicited paging, and privacy of user traffic, the latter being considered a confidentiality issue for the purpose of this study. The use of temporary identities in GSM gives some anonymity, since the real identity is only used when the MS gets connected to the network. Strong confidentiality protection (Section 6.1) provides privacy to the subscriber’s communications.

7 Known Vulnerabilities

<Editor’s note: list the known GERAN/UMTS vulnerabilities and possible impact>

7.1 Cryptographic Algorithm Vulnerabilities

7.1.1 Weak ciphering algorithms

Any access or application security solution which uses GSM/UMTS security context and a weak algorithm potentially jeopardizes confidentiality and possibly also a spread of this problem to other accesses using these contexts. Even if A5/2 has been removed in this time-frame, it can not be ruled out that some other algorithm (A5/1 and GEA1 being the most likely victims), are also broken. Indeed, recent attacks on A5/1 (e.g. [4]: about 20 seconds of known plaintext, and a ten minutes computational effort) raises the question how long we can trust A5/1. The main thing that protects GEA1 is probably the fact that the algorithm is still not known to the general public.

7.1.2 Key size

The 64-bit key size of GSM’s A5/1-3 is marginal. The RC5-64 project [16], retrieved 64-bit keys by brute force in about 3 years using distributed Internet computing, which today (assuming Moore’s law) could be done in less than a year. Even the pedestrian hacker type attacker could ~~possible~~possibly launch such an attack by “stealing” CPU cycles from a large number of users by a large scale ”malware” attack (in fact, several Internet “Worms” have been designed for this purpose [18]). Organized crime or other resourceful attackers can build special purpose hardware that would retrieve such keys in a matter of hours, extrapolating from [17]. A generally recommendation for secure key size for the foreseeable future would be around 100 bits, and 128 bits may be a practical choice.

7.1.3 Weak AKA algorithms

Weak (GSM or UMTS) AKA algorithms could make responses or cipher keys predictable or even reveal parts of the subscriber key, Ki. Though the AKA algorithms are not standardized, effects of proprietary weak AKA algorithms (e.g. COMP128) needs consideration.

7.2 Cryptographic Protocol Vulnerabilities

7.2.1 Lack of network authentication and replay protection

GSM has no network authentication and this is part of the reason that A5/2 weaknesses spreads to other GSM algorithms. UMTS does provide replay protection, yet as noted in [20], it is possible to set up false base stations. This can be seen as a “pre-play” attack. Though the RAND/SQN has not been seen before by the TE/USIM, it is still *not* the RAND/SQN that the TE would have received, had it been communication with the home network. To guarantee freshness in this sense, the protocol would require the use of time-stamps and clock synchronization, or preferably, exchanging RAND values both TE-to-network, and network-to-TE.

7.2.2 Lack of integrity protection

<Editor's note: e.g. signaling/algorithm selection>

As mentioned, without integrity (as in GSM), strength of authentication is weakened since it is theoretically possible to hijack the session after authentication has taken place. The encryption only provides limited protection, in particular the encryption may be switched off from time to time, and we have a situation where the strength of authentication depends on confidentiality, an undesirable dependence.

We also note that the termination point of integrity may be of importance. For instance, in WLAN access, even if stronger TKIP or AES based WLAN mechanisms are used, the L2 integrity terminates in the access point, which typically in a potentially "hostile", public environment. Therefore, WLAN L2 integrity (alone) does not provide sufficient means for e.g. robust charging.

7.2.3 Key (in)separation

<Editor's note. Also WLAN use of SIM etc>

By key separation we mean the property that the same key can never be used for the different purposes, e.g. both for integrity and confidentiality, or even for confidentiality using two different algorithms. Key separation requires either guaranteed replay protection, or, an algorithm/access type specific conversion of the key using a one-way function. Without this, a weak GSM algorithm will threaten the confidentiality of other GSM algorithms and there can also be inter-access security dependencies, e.g. GPRS or WLAN implications on GSM. Due to the use of exactly the same procedures and authentication functions in GSM/GPRS, it is of special importance to consider interaction between these two systems.

7.2.3.1 UMTS/GSM Hand-over and algorithm similarities

When performing handover from UMTS to GSM, the TS [19] specifies a key-conversion function. Specifically, the 128-bit CK/IK are turned into 64-bit GSM KC by XOR:ing the four "halves". This means that if Kc is used with a weak GSM algorithm, 64 bits of information about the (CK,IK) pair leaks. This is not directly devastating, but shows that the choice of key derivation function is not an arbitrary one. One could consider a worse potential problem as follows.

Suppose that the 128-bit A5/4 algorithm has been introduced in GSM and that the following (quite natural) key conversion function would ~~had~~has been specified:

Kc = CK XOR IK. (Eq. 1)

Now, GSM A5/4 is essentially identical to UMTS UEA1. This means that in the (unlikely) case that UEA1 is broken, so is A5/4 and vice versa. Now, per se this means that UMTS confidentiality is essentially lost. However, thanks to the integrity protection of UMTS it is (unlike the GSM case) still not possible to hijack the session since integrity is based on IK which cannot be deduced from CK. However, suppose an active attacker fools the TE into making a~~n~~ hand-over to GSM. The ciphering there will take place using Kc as in (Eq. 1) above, which can similarly be retrieved by breaking A5/4. ~~However,~~But, this now means that the attacker knows CK and (CK XOR IK), from which also IK can be deduced. By handing over back to UMTS, the attacker can now also hijack the UMTS session.

Admittedly, this is a highly hypothetical example, but it again shows that key ~~derivation choices are not arbitrary.~~

derivation/conversion functions cannot be arbitrarily chosen. The ~~paper~~specification [20] lists the cases that could occur when a UE is authenticated to GERAN/UTRAN (including all combinations of GSM/UMTS capable MSCs and SIM/USIM) and then is moved over the other type of access network. The conclusion is (under the assumption that the GSM encryption can be broken) that GSM subscribers who ~~are~~perform hand-over from UTRAN to GERAN reveals information on both IK and CK for all UTRAN communication, both for keys used before the handover and keys used when moved back to UTRAN. UMTS subscribers will have 64 bits of the key-material revealed -(if handover to a UMTS capable MSC) or both IK and CK if the handover is to a GSM only capable MSC.

Also, one could argue that since UEA1 is somewhat similar to UIA1, the fact that UEA1 is broken could have implications also for UIA1 and vice versa. It may thus be desirable to consider the addition of new UMTS UEA/UIA algorithms that are more "independent" of each other and of UEA1/UIA1.

7.2.4 Two-time Pads

<Editor's note. GPRS PS h.o. issues etc>

GSM/UMTS (for good reasons) relies on stream ciphers. These are vulnerable to replay attacks, causing so-called two-time-pads. On could imagine an attack as follows. An A5/1 (say) session is recorded. Later, the victim is (somehow) fooled into sending a known message (e.g. ~~email)~~responding to an email, a form of "phishing" attack) using the same replayed RAND. This enables the attacker (using a false base station) to decrypt the recorded traffic. Even if *this* attack is not considered realistic, it shows an "unsoundness" in allowing replay that could potentially be exploited also in other ways.

Network authentication (7.2.1) is typically a pre-requisite to obtain replay protection.

In [13,14] issues were raised concerning potential loss of security in connection to PS handover. The security of the GPRS ciphering depends on the uniqueness of a 32-bit IOV value; in case of collision (which may occur in such hand over situations) a two-time-pad is generated, revealing *at least* the XOR of the corresponding plaintexts. With the coming 128-bit GEA4 algorithm, the overall security will potentially depend on accidental collisions between 32-bit values, and may not reach the expected 128-bit level.

7.3 Repudiation scenarios

<Editor's note. Access network falsely claims it has a roaming subscriber>

There is a trend towards decreased trust in the visited network. E.g. in IMS, authentication is done in the home. Consider the following "repudiation" scenario, which might be a WLAN access scenario. A somewhat dishonest visited network, X, claims that that home network Y's subscriber, S, is roaming in X. Y will happily (?) provide authentication vectors but will really not have any chance to determine if S is really in X's network. Later S might claim he never was. It is impossible to (robustly) decide if S was in X's network (or if X is lying in an attempt to get compensation) with current AKA mechanisms. However, it would be very easy to solve this cryptographically by introducing non-repudiation mechanisms. Note that non-repudiation can in this case be achieved with lightweight symmetric (SIM based) techniques without the need for PKI.

7.4 Potential Vulnerabilities with Suggested Enhancements

<Editor's note. Some problems with special RAND etc>

A number of suggested countermeasures to the A5/2 attack has been proposed, some which if implemented, *may* have security issues that needs consideration.

7.4.1 Special RAND

The special RAND solution decreases the maximum entropy of the RAND from 128 to about 80 bits. Thus, it also decreases the theoretically effective key-space of Kc by the same amount. However, assuming a secure A3/A8 implementation, it cannot be exploited in practice. The decrease of entropy also means that off-line pre-computation attacks against Ki are reduced in complexity from 2^{128} to about 2^{104}. Still, this is more than enough to rule out the practical feasibility of such attacks. SAGE has estimated that the entropy of RAND could be reduced even to 64 bits without making practical, non-trivial attacks more likely to succeed.

7.5 SIM cloning

What would happen if two identical (same IMSI, Ki) were used in parallel? As far as we understand, there is nothing built into the SIM/USIM standard that prevents/detects this. It is assumed that it is not possible to reverse engineer a

SIM. However, as we have seen, some COMP versions were weak and allowed retrieving Ki. Also, the population fo Ki values into the AuC is a potential weak link in the security chain.

7.6 Other potential vulnerabilities

A potential threat scenario is discussed in [11]. TBD.

8 Threat and Risk Analysis

<Editor's note: pretty standard>

8.1 Threat Analysis

For each of the assets, we perform a threat analysis against each of the security objectives relelvant for that asset. For each threat, we list possible attacks. We also identify the most important "sub-assets", comprising the "total asset".

<Editor's note: most sections currently TBC, including those where some contents exist>

8.1.1 User payload

No sub-asset.

8.1.1.1 Threats to confidentiality/privacy

Threat: sensitive user conversation/packet data is revealed.

Attack(s):

- The TE is fooled to re-use a previously compromised key.
- The TE is/will be fooled to re-use the same key with an insecure algorithm (see Section X.Y). *<Editor's note: this is intended to be a reference to threats to security context data>*
- The key is disclosed by other means (see Section X.Y).
- The TE uses a stream cipher and re-uses a non-compromised key (and other data) that was earlier used to protect data known to the attacker.
- The TE uses a stream cipher and later re-uses the same (non-compromised) key (and other data) to protect data known to the attacker.
- The TE is fooled into switching off ciphering (see Section …).

8.1.1.2 Threats to integrity/authenticity/non-repudiation

Threat: a subscriber generates traffic on behalf of another subscriber.

Attack(s):

- Attack on Ki (see Section…).
- Cryptanalysis of AKA algorithm, enabling response to be predicted.

Threat: A subscriber's payload data is received incorrectly by a service (e.g. a credit card number sent over GPRS) or by another subscriber.

Attack(s):

8.1.1.3 Threats to availability

This is either a radio DoS attack (outside scope), or faked signalling (e.g. faked "detach", "hand-off", etc), which is handled below.

8.1.2 Call set-up signalling

Sub-assets: TE/NW control messages and "identifiers" (e.g. MSISDN).

8.1.2.1 Threats to confidentiality/subscriber privacy

Threat: Someone can get information on who calls who.

Attack(s): Attacker is able to eavesdrop on call setup traffic and retrieves the MSISDN of at least one of the two parties.

8.1.2.2 Threats to integrity

Threat: Calls are redirected.

Attack(s): Attacker changes the destination MSISDN of the call in the signalling (requires MITM).

Threat: Calls are dropped.

Attack: Send faked "hang-up" or "call reject" signalling in the middle of a call (requires MITM).

8.1.2.3 Threats to availability

8.1.2.4 Threats to non-repudiation

Threat: A subscriber denies making a call he/she did make.

Attack(s):

Threat: A subscriber gets charged for call-time he did not use.

Attack(s): A session is hijacked; making call is longer than user think it is.

8.1.2.5 Threats to authenticity

See "Threats to integrity" and "non-repudiation".

8.1.3 Mobility signalling

Important sub-assets:

- MAP signalling,
- Access network discovery signalling.

8.1.3.1 Threats to confidentiality

8.1.3.2 Threats to integrity

Threat: TE is forced to use a certain network.

Attack(s): Send faked “PLMN not available”, force TE to look for another one.

8.1.3.3 Threats to availability

8.1.3.4 Threats to non-repudiation

8.1.3.5 Threats to authenticity

8.1.3.6 Threats to subscriber privacy

8.1.4 Radio resource management signalling

Important sub-assets:

- TE cabability (“Classmark”) info,
- location/Cell-ID where TE is located,
- security setup signalling,
- radio measurement data,
- NW detach signalling.

8.1.4.1 Threats to confidentiality/subscriber privacy

Threat: Outsider can deduce information about a subscriber’s location.

Attack(s): Eavesdropper retrieves the Cell ID from the signalling from the UE to the NW. Note: seriousness depends on also compromising subscriber ID (see next).

Threat: A subscriber’s ID is revealed/tracked.

Attack(s):

- Signalling is tracked from the start (“TMSI” does not help).
- Fake “ID request” from NW.

Threat: Outsider can deduce information about the TE capabilities.

Attack(s): Similar to above.

8.1.4.2 Threats to integrity/authenticity

Threat: Outsider may trick TE into using no (or weak) encryption.

Attack: MITM fakes capabilities of the TE. E.g., the TE and NW is tricked into using GSM security even if both are capable of UMTS security.

Threat: A TE is illegitimately moved to another NW.

Attack(s): Forge radio measurement data signalling, causing handover to another NW.

Threat: TEs are made to hand over to non-existing/faked base station.

Attack(s): Faked h/o signalling.

Threat: One or more TE is illegitimately detached from NW (or are never able to attach).

Attack(s): Fake “Release” command from the NW to one or more TEs (e.g. “group release”).

8.1.4.3 Threats to availability

8.1.4.4 Threats to non-repudiation

8.1.4.5 Threats to authenticity

Threat: False base station.

Attack: Attacker destroys real basestation, puts up a false basestation, faking a basestation (e.g. over non-authenticated microvawe link) towards the NW and fakes a NW towards the TE.

Threat: TE claims other identity, pulling challenges from the NW, AVs from Home Network.

Attack(s): A TE sends many attach request for random/selected IMSIs.

8.1.5 Security context data

Important sub-assets:

- Long-term subscriber key (Ki),
- Identifier, TMSI,
- session confidentiality/integrity key(s) (Kc, CK, IK, etc),
- replay information (SQN),
- context identifier (information on in which “other” context, if any, the security context is being used).

8.1.5.1 Threats to confidentiality

Threat: Ki is disclosed:

Attack(s):

- Ki is disclosed by passive cryptanalysis of the AKA algorithm.
- Ki is disclosed by active cryptanalysis of the AKA algorithm.
- Ki is disclosed by physical tampering with SIM/UICC.
- Ki is disclosed by injection (see threats to integrity/authenticity).
- Ki is leaked from manufacturer.
- Ki is leaked when installed in AuC.

Threat: a session key is disclosed.

Attack(s):

- The key is disclosed by cryptanalysis of the encryption/integrity algorithm using it.
- The key is disclosed by cryptanalysis of the AKA algorithm.
- The key is disclosed by attacking Ki (see above).
- A known value is “injected”/replayed in the protocol (see threats to integrity).
- The key is disclosed by cryptanalysis of a hand-over key conversion function.
- Key is exposed during NW transport (MAP signalling).
- Key is disclosed by physical tampering of AG.

8.1.5.2 Threats to integrity/authenticity

Threat: Ki is modified.

Attack(s): A known value is injected in SIM/UICC and AuC.

Threat: Session key(s) are modified.

Attack(s): A known key is replayed.

8.1.5.3 Threats to availability

Only DoS aspects.

8.1.5.4 Threats to non-repudiation

All threats related to disclosure of keys open up repudiation scenarios, No other threat has been identified.

8.1.5.5 Threats to subscriber privacy

See threats to confidentiality.

8.1.6 Security signalling

8.1.6.1 Threats to confidentiality

8.1.6.2 Threats to integrity

8.1.6.3 Threats to availability

8.1.6.4 Threats to non-repudiation

8.1.6.5 Threats to authenticity

8.1.6.6 Threats to subscriber privacy

8.2 Risk Analysis

<Editor's note: This section will assign "seriousness" and" probability" to the threat found above.>

8.2.1 Risk assessment

<Editor's note: This section will draw the line between which risks we accept and which we will look at countermeasures for>

9 Overview of Possible Enhancements

<Editor's note: This section will discuss protection mechanism to counter the identified risks>

10 Feasibility Study

<Editor's note: This section will study feasibility of the Possible Enhancements>

11 Conclusions and Proposal

12 References

<editor's note: should be set in alphabetical order>

[1] Elad Barkan, Eli Biham and Nathan Keller, "Instant Ciphertext-Only Cryptanalysis of GSM Encrypted Communication", Proceedings of Crypto 2003, Springer LNCS 2729.

[2] Vodafone, "Cipher key separation for A/Gb security enhancements", S3-030463, S3#29, 15 – 18 July 2003, San Francisco, USA.

[3] Ericsson, "Enhanced Security for A/Gb", S3-030361, S3#29, 15 – 18 July 2003, San Francisco, USA.

[4] A. Maximov, T. Johansson and S. Babbage, "An improved correlation attack on A5/1", Proceeding of SAC 2004.

[5] Ericsson, "On the introduction and use of UMTS AKA in GSM", S3-040534, S3#34, 6 - 9 July 2004, Acapulco, Mexico.

[6] Vodafone, "Analysis of the authenticated GSM cipher command mechanism", S3-040262, S3#33, 10-14 May 2004, Beijing, China.

[7] Vodafone, "Evaluations of mechanisms to protect against Barkan-Biham-Keller attack", S3-040263, S3#33, 10-14 May 2004, Beijing, China.

[8] Ericsson, "Comparison of Suggested A5/2 Attack Countermeasures", S3-040341, S3#33, 10-14 May 2004, Beijing, China.

[9] Qualcomm Europe, "An observation about Special RAND in GSM", S3-040572, S3#34, 6 - 9 July 2004, Acapulco, Mexico.

[10] Ericsson, "Enhancements to GSM/UMTS AKA", S3-030542, S3#30, 6 – 10 October 2003, Povoa de Varzim, Portugal.

[11] Lucent, "Eavesdropping without breaking the GSM encryption algorithm", S3-040360, S3#33, 10-14 May 2004, Beijing, China.

[12] C. Brookson, "Authentication: A mechanism for preventing man-in-the-middle attacks", S3-040036, S3#32, 9 - 13 Feb 2004, Edinburgh, Scotland, UK.

[13] Ericsson, "Generation of IOV-UI/IOV-I values during PS Handover", GP-041987, GERAN#21, 23 – 27 Aug 2004, Montreal, Canada.

[14] Nokia, "Handling of ciphering during PS Handover", GP-042046, GERAN#21, 23 – 27 Aug 2004, Montreal, Canada.

[15] Ericsson, "Future of GERAN Security ", S3-04xxxx, S3#35, 5 - 8 October 2004, St. Paul's Bay, Malta.

[16] Project RC5, http://www.distributed.net/rc5/

[17] Electronic Frontier Foundation, "Cracking DES", O'Reilly.

[18] E. Skoudis and L. Zeltser, "Malware: Fighting malicious code", Prentice Hall, 2003.

[19] 3GPP TS 33.102 V6.2.0, "Technical Specification Group Services and System Aspects; 3G Security; Security architecture (Release 6)".

[20] U.Meyer and S. Wetzel, "On the impact of GSM encryption and man-in-the-middle attacks on the security of interoperating GSM/UMTS networks", 2004.