3GPP TSG SA WG3 (Security) — meeting #11 **S3-000137**
Mainz, Germany, 22-24 February, 2000

Source: Siemens

Title: GPRS encryption

Document for: Discussion and decision

Agenda item:

---

1 Introduction

With appropriate equipment it may be possible to perform **hijacking attacks** on a not-ciphered GPRS radio link. Appropriate equipment consists of a combination of a modified base station and a modified mobile station. Hijacking attacks are attacks whereby an intruder inserts his packets on radio resource allocated to a genuine user.

As an effective countermeasure, SMG10 (Oct. '97, and again in Jan. '00) have proposed to make encryption mandatory for GPRS. Mandatory encryption however would **prevent world-wide deployment** of GPRS (without any non-standard additions), as some countries restrict the use of encryption and to other countries the export of network equipment with the appropriate algorithms is restricted, **or** – which is more likely due to the importance of the market that is involved – it would make vendors build in there equipment a **"back-door"** which would result in the fact that encryption is only mandatory "in the specification" but not in reality. We're burying our heads in the sand if we follow this proposal.

Therefore in this contribution we describe **an alternative set of countermeasures** that prevent hijacking attacks on the GPRS radio link in those networks that are allowed to use encryption and have access to the appropriate encryption algorithms, while at the same time taking into account that in some networks encryption cannot be used.

2 Alternative set of countermeasures

We propose:

- the use of encryption be recommended for GPRS and that the signalling provides in the means to negotiate "no encryption";

and as essential countermeasures

- the GSM Association explicitly recommends its members, where possible, to enable encryption;
- there is a mandatory set of ciphering algorithms (GEA1 and GEA2) that all UE have to support; such that all SGSN that have an encryption algorithm GEA1 or GEA2 can establish ciphered connections;

and as supplementary measures

- there is a ciphering indicator in the UE, such that the user is informed when ciphering is not enabled, and that his connection is vulnerable for eavesdropping and channel hijacking;
- there is the ability to configure the UE such that the user can make the UE refuse non-ciphered connections or be prompted to explicitly allow a not-ciphered connection.

3 Consequences

3.1 Application of encryption where possible

Channel hijacking is prevented in all networks that are allowed to use encryption and have access to GEA1 or GEA2 and follow the recommendation of the GSM Association.

There is no reason for operators not to follow that recommendation. There were suspicions that in some cases ciphering is disabled temporarily for technical reasons, such as disturbances on the radio interface. However, if operators would really experience such technical problems, they would not be confident to support mandatory ciphering, as they are.

At the same time the solution provides the ability to deploy not-ciphered GPRS, especially in those countries where ciphering is forbidden or where the network equipment has no access to the ciphering algorithms.

3.2 Visibility of encryption being disabled

When a user roams from a country with encryption to a network without encryption, his ciphering indicator will indicate that ciphering is not enabled and that his connection therefore is less secure. This may be considered a bit user unfriendly, but having no GPRS system in the visited country is hardly any better.

Note that in his home country and in other countries where networks can follow and do follow the GSMA recommendation, all connections will be encrypted, and the user is not bothered.

3.3 Configurability of terminal attitude towards attempts to establish not-ciphered connections

In addition, the UE may be configurable, in a way that it either is in state where

1. when the network attempts to set up a not-ciphered connection, that connection is refused, without the user being informed;
2. when the network attempts to set up a not-ciphered connection, the user is prompted;
3. when the network attempts to set up a not-ciphered connection, the connection is accepted, with the ciphering indicator informing the user of the event.

A user from a network with encryption may have his phone set to state 1 or state 2. While roaming in his own country and other countries with encryption enabled, he would never be bothered with indications, and the feature would not be unfriendly after all. When in other countries, he may remain in state 2, or – deliberately – go to state 3.

Note however that the visibility feature (the ciphering indicator) and the configurability feature are not essential to the prevention of channel hijacking in those network that enable encryption: all that is required to prevent channel hijacking in a network is the network enabling encryption and not allowing not-ciphered connections. All that is required to prevent channel hijacking for your customers when roaming abroad in a particular network is the visited network applying encryption. This can be a part of the roaming agreement.

4 Enhancements for UMTS subscribers

The above proposal is weaker only in the sense that a network operator must trust another network operator to enable encryption when his users are roaming in that network. If part of the roaming agreement, he must trust his roaming partner network to honour the roaming agreement and/or follow the recommendation of the GSM Association.

In UMTS however, the challenge is accompanied by a network authentication token (AUTN) that provides by means of the authentication management field (AMF) an authenticated signalling channel from the HLR/AuC to the UE/USIM. The use of the AMF is up to the discretion of the HE; it is completely transparent to the serving network. The HE could use the AMF to signal to the UE/USIM whether it should allow not-ciphered connections, and this for the duration of a connection. In other words, the HE could send quintets that do not allow not-ciphered calls as a default, but when a network that cannot apply encryption requests for quintets, it could send quintets that allow the UE/USIM to accept not-ciphered connections. In this way, the home environment can enforce that ciphering is applied in those network where it is possible, while also allowing their users to roam to other countries.

5 Conclusions

Mandatory encryption is not required to prevent channel hijacking attacks, the application of encryption where possible and the mandatory implementation in the UE of GEA1 and GEA2 are sufficient countermeasures.

The situation can be improved even with visibility of encryption being disabled and further by providing the user with the ability to configure the terminal attitude towards attempts to establish not-encrypted connections.

Finally, for UMTS subscribers, the home environment will have the ability to control the use of encryption for its users, even when they are roaming abroad.