3GPP TSG SA WG3 Security — S3#32 **S3-040009**
09 - 13 February 2004
Edinburgh, Scotland, UK

Source: **BT Group**
Contact: **Colin Blanchard colin.blanchard@bt.com**
Title: **Protecting GSM/GPRS networks from attacks from compromised WLAN networks when interworking**

Document for: **Discussion and decision**
Agenda Item: **TBA**

1. Introduction

At SA3#31 some concern was expressed that the A5/2 vulnerability can spread from the GSM network to the WLAN network. An even greater concern is that any vulnerability exploited in the WLAN access network or end user devices can spread to from the WLAN network to the GSM network. There was no time during the meeting to explore these concerns and this paper attempts to document with the full expectation that it may be a case of “that is not how WLAN interworking works” or “Yes but nobody would deploy it like that”. However, while additional protection measures for GSM and WLAN are being developed it would worth seeing if a small enhancements now e.g. to the special RAND mechanism may save much effort and rework in the future

2. Background

In GSM/GPRS the use of a specific algorithm can be blocked by the use of the special RAND mechanism. Ericsson has also proposed, *“that those requirements shall also apply to WLAN and 3G interworking for consistency reasons. So, for example, if the special RAND mechanism is adopted then special RANDs should be sent to WLAN AAA servers to prohibit the use of all A5 and GEA algorithms. When the GSM device implements the special RAND mechanism, this will protect against a man-in-the-middle exploiting a weakness in any GSM algorithm in order to masquerade as a WLAN client or eavesdrop the WLAN communications”*. [1].

The special RAND mechanism protects WLAN access from weaknesses in the GSM access. This paper is looking also at the opposite case i.e. protecting GSM/3G access from weaknesses in WLAN access.

For example: -

1. WLAN access networks may also use encryption algorithms that turn out to be weak. However, SA3 have agreed not perform a security analysis of the mechanisms proposed by IEEE. SA3 could disallow the use of certain algorithms, but the current SA3 view is that this is not necessary, since the encryption keys used with these encryption algorithms cannot be used to infer information on any GSM or UMTS keys, due to the use of the key derivation functions in EAP/AKA and EAP/SIM.

2. EAP/AKA and EAP/SIM may use key derivation functions, which turn out to be weak. Currently this is not an issue as only one mandatory mechanism, based on SHA-1, is

specified in the EAP/AKA and EAP/SIM specifications. It is assumed that is fully specified and secure.

3. The AAA server may not be fully trusted or reside in a network that is not completely trusted. This may not be a concern, if the assumption that the AAA server resides in the home network, holds for all deployments.

4. The WLAN access points may not be fully trusted or reside in a network that is not completely trusted. While this lack of trust is a concern for GSM/3G operators it is has been assumed no information present in the AP can be re- used with a GSM 3G UE eg RAND or the link layer keys. For example, the WLAN link layer keys do not give any information on the GSM/3G session keys.

5. The WLAN terminals may not be fully trusted or could be operated by a user who is not completely trusted. The UE functionality split scenario is a specific example of this concern.

SA3 needs to determine if it is possible to:

- Deploy a false base station replaying a RAND obtained from a WLAN network to a 3G/GSM/GPRS mobile which having not seen it before, accepts it as genuine.
- Deploy a false base station reusing CK, IK or kc on the link between the GSM/GPRS mobile and the false base station, with a genuine session (from the perspective of the mobile network) from the false base station to the GSM/3G network.

An initial analysis suggests that for UMTS, this would be possible only if

- The HSS was compromised
  OR
- The AAA server was compromised

However, a compromised 3G WLAN UE allows impersonation of a 3G user accessing UTRAN if the compromised part of the UE can communicate with the attacker's UE, used for UTRAN access, in real time.

If the WLAN UE (e.g. the TE in a UE functionality split scenario) is compromised, then no false base station attack against UMTS is possible because the compromised part of the UE can obtain CK, IK only from the USIM, hence the USIM must have seen RAND before and will not allow this RAND to be re-used.

It is essential that the introduction of WLAN interworking with 3GPP does not reduce the security currently available to GSM/GPRS/3G users.

3. Solutions

If SA3 agree that there is a potential vulnerability, that can be exploited and there is a motivation for this exploit then 4 solutions are described below which may be used individually or in combination.

3.1 Segregated HSS and UICC applications

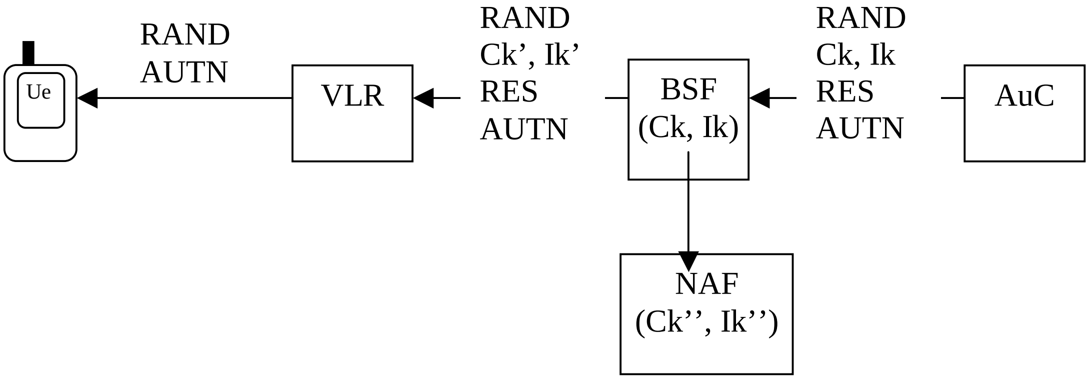
The most effective solution would be to ensure that the HSS/HLR contains a completely separate database of triplets or quintets computed from a separate range of authentication keys (K for 3G and Ki for GSM/GPRS). This will of course mean that the UICC will have to contain two separate applications, a USIM for 3G and an (yet to be named) application for WLAN access. It is recognized that this may conflict with the fact that that Rel99 UICC are allowed to be used in Rel6 UEs for WLAN access and that only one USIM application can be active for Rel99 UICCs, The restriction to have only one USIM application active goes away for Rel4+ UICCs.

It will be important to ensure that any solution suits the (most common) business model where the WLAN access network operator and GPRS operator are separate companies and also the model where 3G WLAN interworking is used to ensure that users use their subscription (and USIM) to get access also over WLAN, and in this way bind users to one operator.

3.2 Key separation function in HSS

An alternative solution proposed by Ericsson in [2] would be to introduce a key separation function ***before*** the VLR or AAA server, which is ***under the control of the 3GPP operator***

In that contribution, Ericsson *"Propose to introduce a general function for key separation in the terminal admittedly require more changes in the terminal and in the network. But it also offers greater possibilities and it might be seen as a more long-term solution and not a quick fix. To support this view we would like describe a possible use case related to GBA. Assume that the key separation mechanism isn't only used to separate keys between encryption algorithms but also to derive other service specific keys. One such service specific key might be a key shared between the BSF and the terminal. Another key could be for WLAN access and a third for presence. However, to guarantee home control an additional layer of key separation is required as indicated in the figure below. The primed and double primed keys are derived from the original data coming from the AuC by application of a key separation function. The figure below shows this idea in a UMTS setting. One immediate conclusion is that there is no need for a separate authentication to load the BSF in GBA with the required keying material.*



When quintets are delivered from the AuC they are first passed to a node, here called BSF, which stores the keys in the quintet together with a hash of it and the identity of the "user". The hash will serve as a reference to exactly this quintet for the given user. The BSF then applies a key separation function using a service name, which could be UMTS authentication as differentiation. "

3.3 Separate range of RAND for each access network type

This is an extension to the special RAND proposal [3]

Where. in addition to reserving 16 bits of RAND for Encryption Algorithms Restriction Vector (EARV), to describe restrictions on the set of encryption algorithms the MS is authorized to use with the ciphering, additional bits of RAND are reserved to describe the restrictions on the set of access devices the RAND can be used with.

This assumes that we have a device that can be trusted to interpret the information correctly ie a traditional GSM/GPRS 3G PS and CS mobile phone issued by the Home Network Operator

3.4 Appropriate functionality split of EAP-AKA and EAP-SIM over UE devices

This was proposed by Siemens [4]. Assuming a UE functionality split scenario, in which the WLAN access device is attacked, but not the card holding device (an assumption similar to the one made for the separate ranges of RAND in section 3.3 above), then attacks on WLAN access can be prevented to affect GSM or UTRAN access by computing at least the EAP-AKA and EAP-SIM master keys on the card holding device.

4. References

[1] S3-030733, Implications of the A5/2 Attack for 3GPP WLAN Access Ericsson, TeliaSonera
[2] S3-030754, Enhancements to GSM/UMTS AKA Ericsson,
[3] S3030698 CR Introducing the special RAND mechanism Orange, Vodafone
[4] S3-030747 Pseudo-CR to TS 33.234 on Requirements on UE split, Siemens