3GPP TSG SA WG3 Security#34 **S3-040574**
5-9 July, 2004
Acapulco, Mexico

Agenda Item: **7.6**

Source: **Vodafone**

Title: **Comments on Orange/Nokia contribution S3-040528 regarding domain separation**

Document for: **Discussion**

1 Introduction

In section 3 of [S3-040528], "domain separation" is listed as one of the advantages of the special RAND mechanism:

> *"Separation of domains (GSM, GPRS, WLAN but possibly others) can be ensured: the derived key can be used only in a certain context. Then, vulnerabilities cannot spread from one context to another. For instance, if an attacker retrieves a triplet in WLAN environment, he cannot use it in the GSM context."*

Furthermore, the conclusion section includes the following statement:

> *"The key separation provided by special RAND does not only allow to counteract Barkan-Biham-Keller attack but it also provides with context separation with other domains."*

We believe that it is important to have a more detailed understanding about what threats domain separation actually protects against. In this document we attempt to do this by elaborating upon some of the attack scenarios that domain separation using special RAND might address. We also evaluate the effectiveness of both the special RAND mechanism and the authenticated ciphering instruction, described in [S3-040262], against these attack scenarios.

2 Discussion

It this section we discuss two attack scenarios.

2.1 Preventing the spread of the Barkan-Biham-Keller attack to the WLAN environment

In this scenario the attacker eavesdrops the RAND values sent over the air to the target customer's WLAN device and using them to mount a Barkan-Biham-Keller attack against the target customer's GSM device in order to discover the corresponding RES/Kc values. The attacker can then use the resulting triplets (RAND, RES, Kc) to determine the WLAN link layer encryption key for eavesdropping purposes, or he may be able to use the triplets to conduct dynamic cloning against the WLAN network. The attack assumes that the target customer has a device that is capable of both GSM and WLAN communications, and that the same Ki value is used for both WLAN and GSM authentication. The special RAND mechanism can protect against this attack because the target GSM mobile will reject the cipher instruction from the false GSM network if the RAND values sent to the WLAN network are configured to prohibit the use of any GSM encryption algorithm.

Note that the authenticated cipher instruction mechanism also protects against this attack. This is because the attacker's false base station is unable to perform the Barkan-Biham-Keller attack because it cannot calculate the correct MAC for the cipher start instruction that is sent to the GSM device. Therefore the "domain separation" entry in the table in section 2 of [S3-040528] is incorrect as far as this attack scenario is concerned.

2.2 Preventing the misuse of WLAN triplets in a GSM context

In this scenario an untrusted WLAN visited network requests triplets from the home network and misuses them to mount a man-in-the-middle attack using a false base station to eavesdrop mobile-originated GSM calls. The attack works even if the customer checks that ciphering has been enabled, because the attacker is able to turn on ciphering using a known cipher key. The special RAND mechanism successfully prevents this attack because the target GSM mobile will reject the cipher instruction from the false GSM network due to the fact the RAND value prohibits the corresponding Kc from being used with any GSM encryption algorithms. Note that this attack is totally independent from the Barkan-Biham-Keller attack.

While the special RAND protects against this specific attack, it should be noted that special RAND does not protect against a false base station that eavesdrops mobile-originated GSM calls by simply omitting the instruction to start ciphering. Such attacks can be detected by the target customer, but this is only possible if the target's mobile implements the GSM cipher indicator, his SIM enables the indicator, and the customer actually checks the indicator before proceeding with each and every call[1]. Therefore, it is considered much more important to protect against false base station attacks which simply omit the instruction to start ciphering, before considering more sophisticated attacks which involve an untrusted visited WLAN network misusing triplets.

A further issue regarding this type of attack is that a WLAN visited network, which is so untrusted that it misuses triplets to mount the GSM eavesdropping attack as described above, would also be likely to carry out other potentially more serious attacks against the home network and/or the home network's subscribers. For example, an untrusted WLAN visited network could overcharge the subscriber or eavesdrop all user traffic that is sent over the WLAN network.

While the basic authenticated cipher instruction mechanism does not protect against the abuse of WLAN triplets in a GSM context, it does protect against the more fundamental false base station eavesdropping attacks which involves simply omitting the instruction to start ciphering.

3 Conclusion

We believe that the claim in [S3-040528] that the authenticated ciphering instruction mechanism does not provide any domain separation is misleading due to the fact that the authenticated ciphering instruction mechanism protects against the spread of the Barkan-Biham-Keller attack as described in section 2.1 above. Furthermore, based on the discussion in section 2.2 above, we believe that special RAND does not offer any significant advantages over the authenticated ciphering instruction mechanism with regard to domain separation.

In summary, we believe that the conclusion of the analysis in [S3-040263] is still valid and propose that the authenticated cipher instruction mechanism should be adopted in preference to the special RAND mechanism.

4 References

[S3-040528] 3GPP Tdoc S3-040528, "Analyse of the countermeasures to the Barkan-Biham-Keller attack", Orange/Nokia.

[S3-030262] 3GPP Tdoc S3-040262, "Analysis of the authenticated GSM cipher command mechanism" Vodafone.

[S3-040263] 3GPP Tdoc S3-040263, "Evaluation of mechanisms to protect against Barkan-Biham-Keller attack" Vodafone.

[1] It may also be possible for the target customer to detect the attack because the correct CLI is not relayed to the called party and because the customer will not be billed for the intercepted call.