3GPP TSG SA WG3 Security — S3#35 **S3-040723**

5 - 8 October 2004

St Paul's Bay, Malta

Title: **Security context separation**

Source: **Nokia**

Document for: **Discussion/Decision**

Agenda Item: **6.6**

Work Item: **GERAN Security**

1 Introduction

Two main solutions to the A5/2 vulnerability problem have been discussed previously: integrity protected A5 version negotiation, and special RANDs. Contribution [S3-040574] from Vodafone notes that even integrity protection could prevent the spreading of the A5/2 vulnerability from the A5 context to the WLAN context.

It is true that the integrity protection solution would indeed prevent the spreading of this particular problem to other contexts by fixing the problem; obviously because the solution is a fix to this known problem. However, the integrity protection solution does not provide the more generic separation of contexts, as provided by the special RAND solution.

Separation of contexts is important in order to prepare for vulnerabilities that might be discovered in the future, rather than only fixing problems that are already known. It is conceivable that a certain context of 2G authentication, such as GPRS GEA, GSM A5, WLAN, or GAA, might become completely compromised in the future, and for example enables an attacker to learn the Kc key for any chosen RAND. The context separation property that is provided by special RANDs would isolate the problem in its original context, so that the vulnerability could not be used to attack other domains. This is because special RANDs make sure that a certain triplet is valid in one context only, and the triplet cannot be used in other contexts at all. This property does not exist for the integrity protected A5 version negotiation, because integrity protected version negotiation is not a generic solution for context separation but rather a fix to the current A5 problem.

2 Examples

The following examples highlight the importance of security context separation:

Example 1:

EAP-SIM provides a mechanism by which several triplets can be combined to provide for 128-bit session keys. The improved key strength relies on the assumption that an attacker cannot brute-force any individual Kc keys, but the attacker will have to brute-force the combined EAP-SIM key. The EAP-SIM protocol does not enable the attacker to attack on individual triplets but the protocol values exchanged in EAP-SIM only allow the attacker to try to brute-force the combined 128-bit keys.

Assume that some other security context (such as GPRS GEA) allows an attacker to learn the ciphertext encrypted with the 64-bit Kc key that corresponds to a RAND that is chosen by the

attacker. Now, the attacker can brute-force each 64-bit Kc key used in EAP-SIM separately, without having to brute-force the full 128-bit EAP-SIM key. This reduces the key strength in EAP-SIM to circa 64 bits. If special RANDs are used, then the attacker will not be able to brute-force the individual EAP-SIM triplets using ciphertext from GPRS GEA, because the special RANDs will only be valid in the WLAN context.

Example 2:

Assume that the MAC used in the integrity protected A5 negotiation is compromised, and an attacker's false basestation that exploits the new vulnerability manages to successfully perform the negotiation with some non-negligible probability. In these cases, the attacker will be able to negotiate the weakest available A5 algorithm and might be able to crack the Kc of any chosen RAND with computationally feasible effort. The attacker will then be able to use all triplets learned from this A5 attack in other contexts, such as WLAN. Special RANDs would prevent this problem -- no matter how badly the A5 context was compromised, it would not be possible to exploit the weakness in other contexts

3 Conclusion

The Special RANDs proposal is the only proposal currently to provide true separation of security contexts. Special RANDs provide assurance that security problems that are not even known currently cannot spread from one context to another. Without special RANDs, the weakest of all security contexts defines the general level of security for the whole 3GPP system, because problems can spread from one context to another.

Separation of contexts is becoming increasingly important as new applications of 3GPP security and new security contexts are taken into use, so the chances of security vulnerabilities in one of the contexts increase. Therefore, we propose that the Special RAND mechanism is introduced also for providing a generic mechanism for security context separation.

4 References

[S3-040574] 3GPP SA3 Tdoc S3-030574: "Comments on Orange/Nokia contribution S3-040528 regarding domain separation", SA3 meeting #34, Acapulco, Mexico, 6-9 July 2004.