3GPP TSG SA WG3 Security — SA3#37 **S3-050012**
February 21-25, 2005
Sophia Antipolis, France

Source: T-Mobile

Title: Next Steps for MAPsec

Agenda item: MAPsec

Document for: Discussion/Decision

1 Introduction

Several changes need to be introduced into TS 33.200 in order to realize the gateway principle. This paper lists some aspects of the work to be done, open questions, and some proposals.

2 MAPsec Changes

2.1 Protection Profiles

The protection profiles were intended to minimise processing overhead on existing NE when they are upgraded to MAPsec. With the new gateway approach, this special effort is no longer necessary. Typical IPsec gateways today can handle throughput of several hundreds of Megabits per second. For MAPsec, similar encryption and integrity algorithms will be used, so the figures should be comparable. Therefore, it is recommended to apply both confidentiality and integrity protection to all traffic passed through the gateway.

2.2 Protected Protocol Layers

Without the protection profiles, there is no need to analyse the MAP protocol within the gateway. The gateway could just protect the whole MAP payload. There were discussions whether lower layers should be included into the protection. SCCP is required for message routing, therefore it must be kept in the clear. TCAP does not contain sensitive information, so there is no need to protect it. However, it does make sense to protect any protocol on top of TCAP. CAP, as an important protocol for prepaid roaming, could then also benefit from the security provided on the inter-operator interface.

A drawback of this "TCAPsec" idea could be that SA3 is not responsible for TCAP. In that case protection could be applied to CAP and MAP only, which both should be of SA3's concern.

2.3 Protected Message Format

The current definition of TS 33.200 V6.0.0 section 5.5 could be kept, but it would apply to at least CAP and MAP.

2.4 Spoofing Countermeasures

Currently, TS 33.200 does not mandate verification of source address (SCCP Calling Party Address) against MAPsec Sending PLMN-Id and the keys used (at least not explicitly).

The threat scenario is that a fraudulent party agrees to use MAPsec, but still intends to spoof (source) addresses. In that case it would insert a spoofed source address, but sign the message with its own key. According to 33.200 Appendix B, a receiver does not have to match source address to SPI and SA. The receiving entity just uses the SPI to look up the policy table. It then uses the key (looked up using SPI, step 7.) to verify the message and would not detect a spoofed origin address. Address use is only mentioned explicitly in the sending case (but as destination address, in step 1).

No NE behind the gateway will be able to perform this check, as the SA terminates in the gateway. Any traffic that passes the gateway will be considered verified. Therefore, the gateway should perform this check.

2 Summary

SA3 is kindly asked to consider the following proposals, and accept them as working assumptions.

1. MAPsec protection profiles will be dropped for the gateway concept.
2. Any protocol on top of TCAP will be protected when passing through the gateway.
3. Explicit verification of source addresses against spoofing shall be added to the TS.