3GPP TSG SA WG3 Security **S3-030243**

xx, 2003

Berlin, Germany

Agenda Item: 7.3 NDS/IP

Source: Ericsson

Title: NDS/IP and SIGTRAN security

Document for: Discussion

1. Scope

This paper aims to discuss the SIGTRAN protocols security and its potential impacts on 3G security and TS 33.210.

2. Introduction

The IETF SIGTRAN WG addresses the transport of packet-based PSTN signalling over IP Networks. For example, signalling traffic such as Q.931 or SS7 ISUP messages may need to be transported between a Signaling Gateway and a Media Gateway or SS7 SCCP messages may need to be transported between two Signalling Gateways. Figure 1 shows the SIGTRAN protocol suite with the M3UA User Adaptation Layer. The SIGTRAN WG deals with the generic transport protocol (SCTP) and the User Adaptation Layer (M3UA in this case).

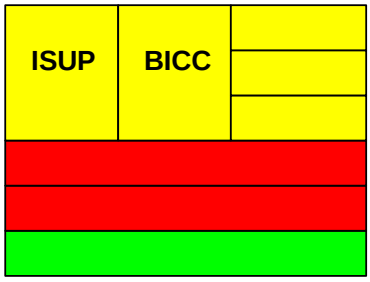

Figure 1 SIGTRAN Protocol Suite with M3UA

Security for SIGTRAN protocols is addressed in the Internet Draft “Security Considerations for SIGTRAN Protocols” [1]. The support for IPsec is mandatory in all nodes running SIGTRAN protocols. The support for TLS is optional.

All SIGTRAN nodes MUST support IPsec ESP in transport mode with non-null encryption and authentication algorithms. Thus, authentication, integrity protection and confidentiality protection MUST be supported. In addition, the replay protection mechanism of IPsec MUST be supported. The nodes MUST support IKE for peer authentication using pre-shared secrets, for negotiation of Security Associations and for Key Management. Both Main Mode and Aggressive Mode MUST be supported. [1]

3. Discussion

Using IPsec to protect SIGTRAN traffic provides security on the network layer. This makes it possible to protect against attacks on all the layers above the network layer. Every SIGTRAN protocol can be protected, as the protection mechanism resides on the network layer.

As IPsec resides on the network layer, it can be used transparently.

M3UA was chosen as the mandatory UA layer protocol to support interworking with legacy SS#7 networks and nodes for the foreseeable future. Due to this choice and the fact that addressing in the SS#7 protocols is not globally unique, every node on the path from the originating node to the destination node may need to decide (for instance, when using Global Title Translation in the case of SCCP) where to forward the packet next. For SIGTRAN, this means that a node needs to send the packet with the destination address of the next node on the path, and so on. Due to this fact, the IPsec protection must be done hop-by-hop. If end-to-end security for SIGTRAN protocols is desired, security mechanisms have to be implemented on the application layer.

The hop-by-hop security leads to some latency in the transport, as each intermediate node on the path from the originating node to the destination node needs to decrypt the inbound packet, do the routing processing and create a new IP packet for the next hop and encrypt that packet.

The use of hop-by-hop security implies trust in each intermediate node on the path, as the information is decrypted in the intermediate nodes and thus disclosed there.

When using IPsec to protect SIGTRAN protocol traffic, the upper layer protocols are not aware of the IPsec being used. Thus, on the higher layers, it cannot be confirmed that the traffic is really secured.

Figure 2 describes a use case where the Signaling End Point A (SEP A) sends a protected message to SEP B. The Signaling Gateways (SG A, SG 1, SG 2, SG B) on the transmission path from SEP A to SEP B need to decrypt the information to do Global Title (GT) Translation, and encrypt the information again when forwarding the packet to the next node on the path.

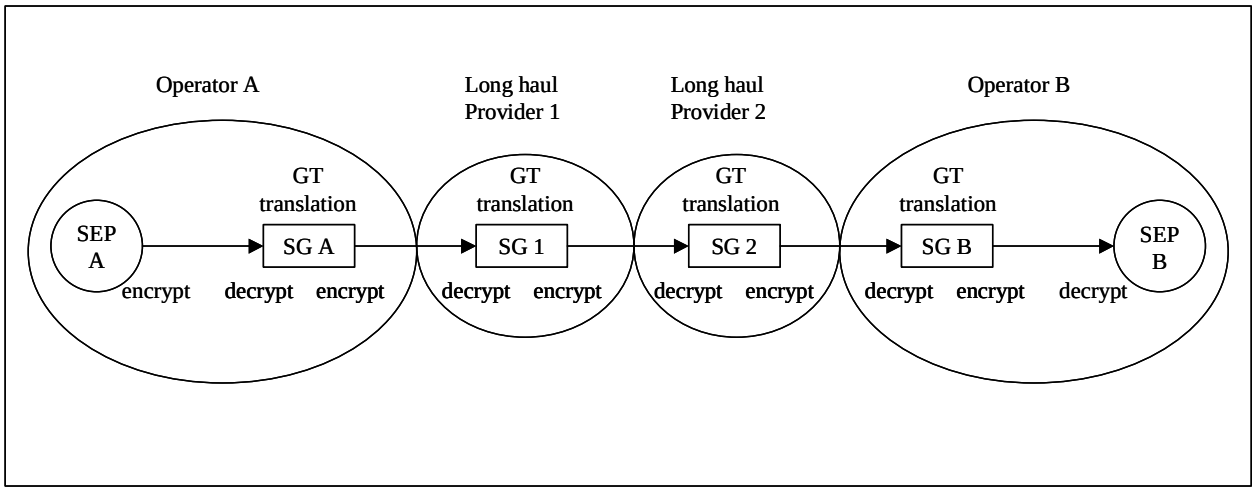

Figure 2 Use case: protected signaling message from SEP A to SEP B

4. Conclusions and Recommendations

SIGTRAN security might have an impact on the trust model of TS 33.210 and might require definitions of new Z-interfaces. SA3 is encouraged to study this issue further and evaluate the impacts on TS 33.210.

5. References

[1] J. Loughney, M. Tuexen, J. Pastor-Balbas , Security Considerations for SIGTRAN Protocols, Internet Draft draft-ietf-sigtran-security-02.txt (Work in Progress), IETF, January 2003