3GPP TSG SA WG3 Security — S3#18 S3-010204

21-24 May, 2001

Phoenix, USA

Source: Nokia

Title: Proposed changes to 33.xxx about protecting user plane traffic

Document for: Discussion and decision

Agenda Item: ?

This contribution proposes clarifications to the text concerning user plane traffic protection. It is edited with change markers against 33.xxx v. 0.5.0.

---

4 Overview over UMTS network domain security for IP based protocols

4.1 Introduction

The scope of this section is to outline the basic principles for the network domain security architecture. A central concept introduced in this specification is the notion of a network security domain. The security domains are networks that are managed by a single administrative authority. Within a security domain the same level of security and usage of security services will be typical. Typically, a network operated by a single operator will constitute one security domain although an operator may at will subsection its network into separate sub-networks and hence separate security domains.

4.2 Protection at the network layer

For native IP-based protocols, security shall be provided at the network layer. The security protocols to be used at the network layer are the IETF defined IPsec security protocols as specified in RFC-2401 [10]. All network domain entities supporting native IP-based control plane protocols shall support IPsec.

4.3 Security for native IP based protocols

The UMTS network domain control plane is sectioned into security domains and typically these coincide with operator borders. The border between the security domains is protected by Security Gateways (SEGs). The SEGs are responsible for enforcing the security policy of a security domain towards other SEGs in the destination security domain. The network operator may have more than one SEG in its network in order to avoid a single point of failure or for performance reasons. A SEG may be defined for interaction towards all reachable security domain destinations or it may be defined for only a subset of the reachable destinations.

The UMTS network domain security may also ~~does not~~ extend to the user plane. ~~and consequently the security domains and the associated security gateways towards other domains do not encompass the user plane Gi-interface towards other, possibly external to UMTS, IP networks.~~

A chained-tunnel/hub-and-spoke approach is used which facilitates hop-by-hop based security protection.

All secure communication between security domains shall take place through Security Gateways (SEGs). Although IPsec allows for manual entry of SAs, key management for IPsec between security domains shall always be automated in order to support IPsec anti-replay protection.

---------- next modification ----------

6 Security protection for GTP

This section details how NDS/IP shall be used when GTP is to be security protected.

6.1 The need for security protection

The GPRS Tunnelling Protocol (GTP) is defined in 3G TS 29.060 [4]. The GTP protocol includes both the GTP control plane signalling (GTP-C) and user plane data transfer (GTP-U) procedures. GTP is defined for Gn interface, i.e. the interface between GSNs within a PLMN, and for the Gp interface between GSNs in different PLMNs.

GTP-C is used for traffic that that is sensitive in various ways including traffic that is:

- critical with respect to both the internal integrity and consistency of the network
- essential in order to provide the user with the required services
- crucial in order to protect the user data in the access network and that might compromise the security of the user data should it be revealed

Amongst the data that clearly can be considered sensitive are the mobility management messages, the authentication data and MM context data. Therefore, it is necessary to apply security protection to GTP signalling messages (GTP-C).

The security domain operators may apply NDS procedures to protect also GTP-U.~~Network domain security is not intended to cover protection of user plane data and hence GTP-U is not normally protected by NDS/IP mechanisms~~ .

6.2 Policy discrimination of GTP-C and GTP-U

SGNs must be able to discriminate between GTP-C and GTP-U messages.~~, which shall receive protection, and other messages, including GTP-U, that shall not be protected~~. Since GTP-C and GTP-U are~~is~~ assigned ~~a~~ unique UDP port-number~~s~~ in (TS29.060, [4]) IPsec can easily distinguish them~~GTP-C datagrams~~ from other datagrams that may not need IPsec protection.

As discussed in section 5.2.2 the Security Policy Database (SPD) is consulted for all traffic (both incoming and outgoing) and it processes the datagrams in the following ways:

- discard the datagram
- bypass the datagram (do not apply IPsec)
- apply IPsec

Under this regime other messages~~GTP-U~~ will simply bypass IPsec while GTP-C (and possibly GTP-U) will be further processed by IPsec in order to provide the required level of protection. The SPD has a pointer to an entry in the Security Association Database (SAD) which details the actual protection to be applied to the datagram.

NOTE: Selective protection ~~of GTP-C~~ relies on the ability to uniquely distinguish GTP-C datagrams from GTP-U datagrams. For R99 and onwards this is achieved by having unique port number assignments to GTP-C and GTP-U. For previous version of GTP this is not the case and provision of selective protection for GTP-C for pre-R99 versions of GTP is not possible.