3GPP TSG SA WG3 Security — S3#23 **S3-020234**

Victoria, Canada

14 – 17 May, 2002

Source: **Siemens**

Title: **Justification for proposed changes to text on SIP integrity in TS 33.203 v510**

Document for: **Discussion**

Agenda Item: **6.1**

Abstract

It is the intention of this document to provide a justification for the text proposed in the CR relating to SIP integrity which was simultaneously submitted by Siemens to SA#23. The main points addressed are:
- Editorial issues;
- Implementation of decision for IPsec (with integrity and no confidentiality);
- Separate security associations (SAs) for TCP and UDP;
- Mitigation of reflection attacks through unidirectional SPIs;
- Integrity keys, algorithms and key expansion;
- Other SA parameters and selectors;
- Rules for IPsec handling at UE and P-CSCF;
- Adaptation to changes in draft-IETF-sip-sec-agree and other changes to security mode set-up;
- SA handling and failure cases.

Two issues addressed in this contribution should be mentioned in particular:

- *a Denial of Service attack during registration and its mitigation are described;*
- *the proposed text may, in certain places, impose undue restrictions on the use of IP addresses and ports for reasons of simplicity rather than security. These issues, and possible alternatives to the proposed text, have been noted in Editor's notes which should be brought to the attention of CN1.*

---

1. Editorial stuff

A general editorial clean-up was done and clarification was provided where felt needed.

2. Implementation of decision for IPsec (with integrity and no confidentiality)

All the material in Annexes B and D has been moved to section 7, and the generic text in section 7 has been replaced with text specific to IPsec. All references to confidentiality have been removed.

3. Separate security associations (SAs) for TCP and UDP

UDP is the preferred transport protocol over the air in the IMS, but the use of TCP is mandated by SIP when the message exceeds a certain size. Consequently, both transport protocols need to be supported, and the corresponding SAs need to be set up during registration. In order not to put any undue restrictions on the IPsec implementation it seems

advisable to establish separate SAs for UDP and TCP. Please also note that there has been a discussion on this issue on the SA3-list involving Stefan Schroeder, Greg Rose and Guenther Horn.

4. Mitigation of reflection attacks through unidirectional SPIs

In a reflection attack, an attacker may try to reflect an IP packet sent from the UE to the P-CSCF or vice versa back to the sender in the hope that it passes the integrity check. When IKE is used to negotiate SAs for IPsec then this attack is countered by the use of unidirectional integrity keys generated by IKE. In the IMS, the integrity key used by IPsec is established using AKA which generates only one 128 bit integrity key. In order to avoid potentially costly key derivation procedures it is proposed to use the same integrity key in both directions (which is compatible with RFC2406(ESP)) and to counter the reflection attacks by using unidirectional SPIs (security paramter indices). This makes packets on the uplink and on the downlink always different.

5. Integrity keys, algorithms and key expansion

It is proposed that HMAC-MD5-96 [rfc2403] and HMAC-SHA-1-96 [rfc2404] shall be supported by both, the UE and the P-CSCF. This should not be too much overhead as this is required for compliant ESP-implementations anyhow , cf. rfc2406. (But the author would also find the specification of only one authentication algorithm for IMS Rel5 acceptable.) If only one of the two authentication algorithms is compromised then it suffices for the IMS to remain secure that the algorithm is no longer supported by any P-CSCF. The security mode set-up procedure (cf. section 7.2) will then ensure that the other authentication algorithm is selected.

HMAC-SHA-1-96 requires 160 bit keys, so the integrity key generated by the AKA needs to be expanded from 128 bits to 160 bits A simple expansion function is proposed which appends the first 32 bits of the AKA integrity key to itself to obtain the 160 nit key. It is further proposed to have this decision double-checked by ETSI SAGE by sending them an appropriate LS.

6. Other SA parameters and selectors

It is clarified that the SA lifetime is controlled by the application (it shall be equal to the registration period), and that therefore the SA lifetime in the IPsec SAD can be set to the maximum value which cannot be reached during the lifetime of the system. (already in the current text, change merely editorial).

The parameter “mode” has been added. This change also is editorial as transport mode is the mode already specified in the current version of the spec.

In IPsec, SAs are bound to selectors, i.e. source and destination IP addresses, source and destination ports, and transport protocol. It is clarified in the text which selectors to choose when setting up an SA.

The proposal for the binding of selectors assumes that a single IP address of the UE is used during a registration period. This may be too restrictive, and is not necessary from a security point of view. But additional IP addresses of the UE would have to be negotiated in the security mode set-up procedure, and, possibly, more than one SA per direction and per transport protocol would have to be established during the registration. It is not required either from a security point of view that the UE sends and receives protected messages on the same port. It just seems to make things easier. These issues are addressed in three “Editor’s notes” in the new text for sectoin 7.1 which should be brought to the attention of CN1.

7. Rules for IPsec handling at UE and P-CSCF

The current text in the spec lacks a comprehensive set of rules in one place on how to set up security associations, and how to use IPsec for SIP integrity. Therefore, such rules were introduced in section 7.1. The importance of rules 2 and 3 is discussed in the following:

- rule 3 states that the triple (UE_IP_address, UE_protected_port, transport protocol), which can be communicated from the transport stack to the application layer through a socket, is used by the SIP application to identify the SA which was in use at the network layer. This means in particular, that this triple has to point to a unique user (IMPI). Furthermore, the P-CSCF shall check that, for one IMPI, no more than three SAs per direction and per transport protocol are stored at any one time. (More than three SAs are not required according to the discussion on SA handling in the new text for sectoin 7.4 provided by H3G.)

- rule 2 clarifies that the UE's IP address which is bound to an SA must be checked against the IP address in the protected part of the REGISTER message (in the contact header or in the security mode set-up, cf. also Editor's note), cf. also Nokia's contribution S3-020108. Rule 2 is required to mitigate a Denial of Service attack which is described in the next section of this document.

8. Denial of Service attack at registration and its mitigation

In the registration procedure, a user's IP address is bound to a security association. Assume that Alice tries to register, that Bob has not yet registers, and that an attacker Eve can read and modify packets on the way between a UE and the P-CSCF. So, Eve can change Alice's IP address to that of Bob in the IP packet header containing the REGISTER message. Note that the IP address in the IP packet header is not protected by IPsec ESP. If Eve does this consistently for both the unprotected REGISTER message sent first, and the protected REGISTER message sent the second time, and if the P-CSCF does not check the IP address in the packet header against a copy of that IP address in the protected part of the REGISTER message then the effect will be that Alice will not be able to communicate (because its true IP address is not bound to the established SA). Therefore, rule 2 is needed (see section 7 of this document and section 7.1 of TS 33.203).

In addition, Bob may have problems to register later for the following reason: Eve has already managed to get Alice registered under Bob's IP address, and if Bob wanted to use the same protected port for a particular transport protocol, then the P-CSCF would reject Bob's registration because according to rule 3, the triple (UE_IP_address, UE_protected_port, transport protocol) has to point to a unique user.

But even with rule 2, a limited form of DoS attack remains:
Eve may register herself, authenticating herself as Eve in the IMS, under Bob's IP address if Eve can send and receive IP packets under Bob's IP address. Bob may then have the same trouble registering later as described in the previous paragraph. But when rule 2 is applied the scope of the attack is severly limited due to the following factors:
1. Eve has to reveal her true IMS address, i.e. the IMPI; to the P-CSCF.
2. According to rule 3, Eve can use up no more than three port numbers when registering with her IMPI..
3. In a note following rule 6 in the new text for section 7.1, it is recommended that the UE randomly selects the number of the protected port from a sufficiently large set of numbers not yet allocated at the UE. Then Bob would be unlikely to select a protected port number already used up by Eve.
These factors together seem to make the chances of success of the DoS relatively low, and the risk of being caught non-negligible.
In addition, security features in the access network may help: in the UMTS PS domain, the GGSN matches the IP addresses of incoming packets with the PDP contexts, hence an attacker would have to break PS domain access link security, or successfully attack GTP-U.

9. Adaptation to changes in draft-IETF-sip-sec-agree and other changes to security mode set-up

This concerns section 7.2 on security mode set-up, and here mainly the content of the protected REGISTER message SM7. References to confidentiality were removed.

10. SA handling and failure cases

The text on failure cases has been cleaned up and repetitions and generic text were removed. The current section 7.3.3 contains a detailed treatment of procedures for changing SAs. This is now covered in section 7.4 by text provided in a CR by H3G. Hence, the text in section 7.3.3 is deleted.