3GPP TSG SA WG3 #21bis aSIP ad hoc **Tdoc S3z020008**
Antwerp, Belgium
31st January – 1st February 2002

Source: **Vodafone**

Title: **Reflection attacks in IMS**

Document for: **Decision**

Agenda Item: **6.1**

Introduction

One of the candidate mechanisms for integrity protecting SIP messages involves the use of an extended HTTP digest authentication mechanism. In this contribution, it is considered whether the current proposals adequately protect against reflection attacks. This issue was briefly discussed at SA3#21.

Discussion

In S3-010664 it was shown how the replay protection scheme in 33.203 v1.0.0 is flawed and may lead to loss of calls due to the lack of synchronization of counters at the UE and P-CSCF respectively. The author suggested that the problem could be solved by using different counters on each side, one for each direction. In this contribution we assume that the solution suggested in S3-010664 is adopted. The new scheme would therefore work as follows:

1. There are two counters at the UE, nc_UE_ul for uplink/sending messages and nc_UE_dl for downlink/receiving messages. In addition there are two counters at the P-CSCF: nc_P_ul for uplink/receiving messages and nc_P_dl for downlink/sending messages. These counters may be preset to 0.
2. When a entity sends a message it increases its sending counter by one and includes the (new) counter value nc in the integrity-protected part of the message.
3. When an entity receives a message and can verify its integrity it sets the receiving counter to the nc-value in the received message provided the received nc-value is higher than the receiving counter value. Otherwise, the received message is rejected.

While this solution seems to address the problem identified in S3-010664, it does not seem to offer full protection against all types of replay. In particular, it seems that a particular type of replay attack, known as reflection, is possible.

In normal operation the nc value will increment by one for each successive message in a particular direction. However, in SIP the number of uplink messages may be different to the number of downlink messages even if no messages are lost during transmission. Therefore, the uplink and downlink counters at a particular entity may be different at a particular instance even if they are both initialized to the same value. If the counters are different then a reflection attack is possible as described in the example below:

1. Assume that the uplink counter is 7 and the downlink counter is 5.
2. The UE sends a new message to the P-CSCF. The UE increments its uplink counter and includes an nc value of 8 in the message.
3. The P-CSCF receives the message. The integrity check passes and the nc value of 8 is accepted because it is greater than the P-CSCF's uplink counter value of 7. The P-CSCF then sets its uplink counter to 8.
4. Meanwhile an attacker intercepts the message sent to the P-CSCF. The attacker sends this message to the UE, i.e. the intercepted message is reflected in the opposite direction.

The UE receives the message sent by the attacker. The integrity check passes and the nc value of 8 is accepted because it is greater than the UE's downlink counter value of 5. The UE then sets its downlink counter to 8.

If the uplink or downlink counters are the same then an attacker could force them to drift apart to mount this attack by blocking the transmission of messages in a particular direction. Alternatively the attacker could simply call the target since the resulting message flow involves more uplink messages than downlink messages (see Figure 7.4.2.1-1 in 24.228 v180).

Although this example demonstrates that the integrity protection mechanism does not prevent messages from being reflected, it does not mean that an attacker could exploit this to attack the IMS system. In fact, it seems that all SIP messages are directional and therefore cannot be replayed in a meaningful way in the opposite direction. However, it is recommended that the integrity protection mechanism should offer protection against reflection attacks which does not depend on the details of SIP. This is because the mechanism should be effective even if the SIP is changed. Furthermore, it should be possible to re-use the mechanism for protecting other protocols.

To protect against replay attacks it is proposed to include a direction bit in the integrity check calculation. The rules for setting the direction bit should be included as part of the security mode procedure. For example, the first integrity protected message with a new IK could set the bit to one for that message and all subsequent messages sent in the same direction. The receiver of that message then uses bit zero for sending messages in the opposite direction. Note that the direction bit does not necessarily have to be transmitted with the message – this is for further study.

Conclusion

All SIP messages are directional and therefore cannot be replayed in a meaningful way in the opposite direction. However, it is proposed that the security of the integrity protection mechanism should not depend on the details of SIP. Therefore it is proposed to add a direction bit to the integrity check to provide robust and future-proof protection against reflection attacks.