3GPP TSG SA WG3 Security — S3#29 **S3-030477**
15 - 18 July 2003
San Francisco, USA

Title: **Reply to LS on DoS attacks against the 3GPP WLAN Interworking system**
Response to: **S2-032730 (S3-030428)**
Release: **Rel-6**

Source: **SA3**
To: **SA2**
CC : **-**

Contact Person:
Name: Anand Palanigounder
Tel. Number: +1-972-684-4772
E-mail Address: anand@nortelnetworks.com

Attachments: **None**

Overall Description:

SA3 thanks SA2 for their LS on Denial of Service attacks against the 3GPP WLAN Interworking system. SA3 reviewed the conclusions reached in the attached paper titled "Security analysis for tunnel establishment" (S2-032483) and concluded the following:

SA3 agrees with the conclusion reached in the document except that, in case there is no WAG in the VPLMN or traffic routed through it, PDGW will be the one being affected by the Denial of Service attack.

Two ways of facing the attack have been identified by SA3. Both have similar results, although different architectural implications SA2 can take into consideration:

- Firewall policies in the WAG will protect the attack in the boundaries of the GRX. In this case, suitable WAGs are needed, which are able to absorb the attack. This option has the advantage of stopping the attack in the boundaries of the backbone network, but it requires support in the VPLMN (the WAG). This option applies equally to the tunnel-switching and end-to-end tunneling approaches – in either case measures at the WAG are needed in order to block the DoS attack at the boundary of the GRX network.
- If the HPLMN does not want to rely on the fact that traffic from the WLAN AN to the PDGW is always routed through a WAG, or that the WAG performs some of the needed firewall functionality, then the PDGW may need firewall functionality (either in the same node or outside) to enforce the policies. In the same way, PDGWs which are able to absorb the attack will be required. This option has the advantage of not requiring any support in the VPLMN (for roaming cases). However, the attack has to be detected and absorbed in the PDGW of the HPLMN of the user.

SA3 also would like to point out that IP address spoofing is also possible with both end-to-end tunneling and switched tunneling approaches. In order to mitigate the DoS attacks due to address spoofing, once the attack is identified, cooperation in tracking down and terminating the attacks is needed from the operators involved (e.g., HPLMN, VPLMN, WLAN etc.). SA3 further notes that, once the DoS attack is identified, it may be easier to track down the attacker(s) at the WAG than at the PDGW. However, it is not necessarily any easier to identify such attacks on WAG as opposed to the attacks on the PDGW.

Actions:

To SA2:

SA2 is kindly asked to take above conclusions from SA3 in their architectural discussions.

Date of Next SA3 Meetings:

SA3 ad hoc	3 – 4 September 2003	Antwerp, Belgium
SA3#30	6 – 10 October 2003	Povoa de Varzim, Portugal
SA3#31	18 – 21 November 2003	London, UK