3GPP TSG SA WG3 Security — S3#29 **S3-030326**
15 - 18 July 2003
San Francisco, USA

3GPP TSG CN WG4 Meeting #19 ***N4-030663***
San Diego, CA, USA, 19th – 23rd May 2003

Title: LS on Security Issues regarding multiple access connections

Response to: LS S3-030303 on **Security issues regarding multiple PDP contexts in GPRS** from SA3.

Source: CN4

To: SA2, SA3

Contact Person:
Name: Dan Warren, Nortel Networks
Tel. Number: +44 1628 431098
E-mail Address: dlwarren@nortelnetworks.com

1. Overall Description:

CN4 thanks SA3 for their most recent LS (S3-030303) on security issues associated with multiple PDP contexts in GPRS. Within this LS, SA2 and CN4 were asked by SA3 to;

> *"inform SA3 about potential mechanisms to solve the problem in order for SA3 to evaluate the security aspects."*

CN4 believes that SA3 are aware that a proposal was made to CN4 #18 for changes to GTP in discussion document N4-030112 and associated CR's. This proposal recommended that the establishment of simultaneous connections to a private network and to the Internet be denied by the 3GPP network in order to protect the integrity of the private network and described a possible mechanism to do this. This was not adopted by CN4 because it was CN4's belief that the requirements for the type of security protection that were being described should be defined by SA3 and because CN4 felt that investigation of other methods of either denying establishment of concurrent contexts or of protecting against cross contamination of malicious content from one connection to the other, should be made. However, this proposal still exists and could be adopted if required.

Following presentation of S3-030303, CN4 has discussed other potential solutions. CN4, whilst agreeing that 'more powerful attacks' may be possible as a result of simultaneous connection to the internet and to a corporate intranet compared to sequential connections, are not aware of situations where that might be the case.

It was also raised in CN4 that this form of attack might occur with any simultaneous connections, be this over GPRS, WLAN, fixed line data access or any other form of access. The analysis of the situation for fixed line data access is out of the scope of 3GPP, but the situation where a connection over fixed line access already exists and a subsequent connection via GPRS or WLAN is established should be considered by 3GPP, since the establishment of this subsequent connection would be over an interface under 3GPP control. Thus any mechanism to prevent subsequent PDP contexts from being established, or alternatively to allow the establishment of the context but to provide suitable protection between the concurrent connections, should also prevent this type of scenario from occurring.

Further, CN4 believes that the security aspects of the R6 work on WLAN should be included within the scope of the work on security for simultaneous connections. Any solution that is recommended should be applicable to similar situations with dual WLAN connections, and WLAN combined with GPRS or fixed line data connections.

This would widen the scope of the problem to be considered to encompass the following combinations.

Established Connection	Subsequent Connection
GPRS	GPRS

GPRS	WLAN
WLAN	GPRS
WLAN	WLAN
Fixed line data connection	GPRS
Fixed line data connection	WLAN

CN4 concluded that for the GPRS/GPRS situation the proposal in N4-030112 or some other core network based proposal could potentially offer a solution, but equally, a UE based solution would work just as well, and would also be effective protection for the other situations described in the table. Further, UE based solutions such as UE private firewalls would protect the UE (and hence the private network) from being exposed to real time attack, would allow the dual connections to exist together (rather than mandating that one of the two connections be refused), would work for any situation where dual connections are required (as opposed to merely those in scope of 3GPP) and are readily available now.

To summarise, whilst the discussion in CN4 recognises that the GPRS/GPRS solution is within the remit of 3GPP to resolve, the next three situations in the table above are also within the scope of 3GPP and possibly the other two situations may also be in scope too, since the establishment of a GPRS or WLAN connection that may pose a threat to the security of the networks that the subscriber is attached to could potentially be denied or made secure via 3GPP standardised means. However, given the variety of access media that this wider problem applies to, the UE is the only place that has knowledge of all the connections that it has established and thus a UE based solution is preferable.

2. Actions:

To SA2 and SA3 group.

ACTION: CN4 asks SA2 and SA3 group to take account of the potential threat that dual WLAN connections or combinations of WLAN and GPRS connections (in addition to the GPRS/GPRS problem) when considering the security and architectural aspects of WLAN interworking for R6.

To SA3 group.

ACTION: CN4 asks SA3 group to take note of the two solutions identified for the dual GPRS connection scenario (either network based or a UE based solution), noting that the UE based solution would require no changes to 3GPP specifications and would be applicable to all six of the scenarios above (indeed, it is applicable to any scenario where dual connections are established) and would in some situations allow both of the connections to remain in place.

3. Date of Next CN4 Meetings:

CN4 #20	25th August – 29th August 2003	Sophia Antipolis, FRANCE
CN4 #21	27th October – 31st October 2003	CHINA