3GPP TSG SA WG3 Security — S3#29 **S3-030425**
15 - 18 July 2003
San Francisco, USA

3GPP TSG-SA WG2 meeting #33 **S2-032680**
7–11 July 2003 Revised S2-032674
Sophia Antipolis, France

Title:	**LS on Security issues regarding multiple PDP contexts in GPRS**
Source:	**SA2**
To:	**SA1**
Cc:	**SA3, CN4**
Release:	**Release 6**

Contact Person:
Name: **Gavin Wong, Vodafone UK**
Tel. Number: +44 1635 672912
E-mail Address: gavin.wong@gb.vodafone.co.uk

Attachments: S2-031749, S2-032321, S2-031118

SA2 has been considering the architectural impacts relating to a security issue brought about by the ability for a mobile to connect to more than one access point (concurrently and sequentially). The problem is highlighted in the attached documents from SA3 (S2-031749 & S2-031118) and the scope of the discussion is very broad as highlighted in the attached LS from CN4 (S2-032321). Since this is an important issue, where service to the user may be impacted, it was felt advisable to involve SA1 as early as possible in the discussions.

In summary, it is possible for a mobile terminal to connect to multiple networks, either within GPRS via different PDP contexts to different APNs (i.e. "virtual connections") or via different access networks, e.g. via simultaneous GPRS and WLAN connections (as requested by SA1). SA3 has indicated that multiple PDP contexts are a potential security threat.

Given that terminals are likely to require multiple PDP contexts for the support of different services, e.g. IMS, MBMS, Internet browsing, corporate network access, MMS, WAP, the blocking of simultaneous PDP contexts could have a detrimental effect on services. For instance, a user might want to browse their corporate Intranet while still being able to make IMS based calls. These scenarios and the potential threats are something that 3GPP needs to understand in more detail in order to ensure that a solution can be developed.

Actions

To SA1:

SA2 kindly requests SA1 to consider this security issue highlighted in the attached documents and to consider what is required from a service perspective. Specifically, SA2 asks SA1 to consider the service implications of limiting simultaneous PDP contexts or simultaneous network connections (e.g. CS, WLAN and GPRS).

Next SA2 Meetings

SA2 Meeting #34	18th – 22nd August 2003	Brussels, Belgium
SA2 Meeting #35	27th - 31th October 2003	TBD

3GPP TSG SA WG3 Security — S3#27 **S3-030164**
25 - 28 February 2003
Sophia Antipolis, France

Title: **LS on security issues regarding multiple PDP contexts in GPRS**

Response to:

Source: **SA3**

To: **CN4, SA2**

Cc:

Contact Person:
Name: **Peter Howard**
Tel. Number: **+44 1635 676206**
E-mail Address: **peter.howard@vodafone.com**

Attachment: S3-030087

SA3 have reviewed contribution S3-030087 (attached) which identifies security issues that arise due to the fact that a GPRS terminal may be simultaneously connected to a private network (e.g. a corporate network) and a public network (e.g. the Internet) via multiple PDP contexts. SA3 would like to highlight the fact that similar security issues will also exist if simultaneous connections to private and public networks exist via non-GPRS connections.

It is understood that Network-based solutions have been discussed at the recent CN4#18 meeting and that a solution has been proposed which would require changes to CN4 and SA2 specifications. SA3 noted that other solutions (e.g. Terminal-based solutions) may be possible and that further study is needed before deciding on the best approach.

Actions

SA3 suggest that CN4 and SA2 keep SA3 informed about potential solutions.

Next SA3 Meetings

Meeting	Date	Location
SA3#28	06-09 May 2003	Berlin, Germany
SA3#29	15-18 July 2003	San Francisco, USA

3GPP TSG SA WG3 Security — S3#26 **S3-030087**
25 - 28 February 2003
Sophia Antipolis, France

Source:	Vodafone
Title:	Security issue with multiple PDP Contexts in GPRS
Agenda item:	
Document for:	Discussion and decision

Problem

In GPRS it is possible that a user can have multiple active PDP Contexts to different APNs. This is fine and perfectly acceptable for connections to public networks only e.g. a connection to a WAP gateway and a connection to the Internet, but when there exists a connection to a private network e.g. a corporate intranet, and a connection to a public network at the same time, there is the possibility of the user becoming a router or application layer proxy for data from the Internet on to his/her corporate intranet. This could potentially enable someone on the Internet to attach to the innocent user's computer and from there attach to the corporate Intranet causing such havoc as real time stealing/modification/deletion of confidential information, run a port scan on addresses and then subsequently run DoS attacks on specific services (e.g. intranet web servers) etc.

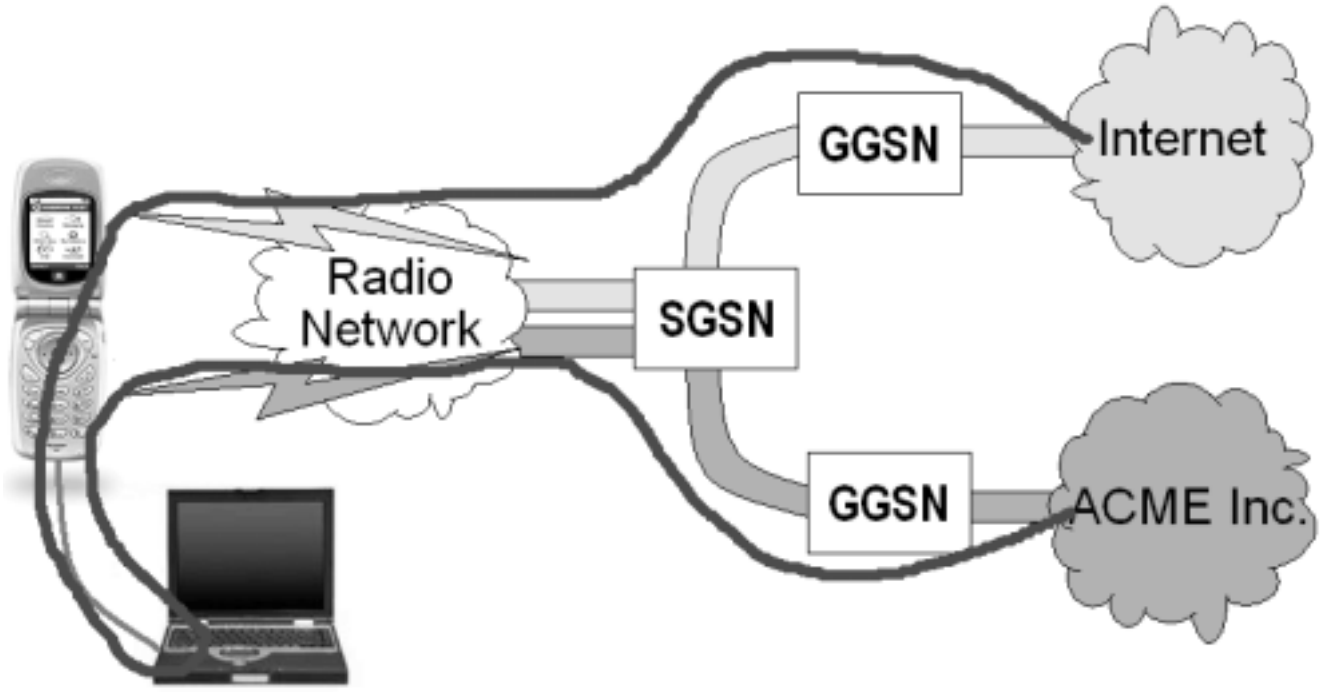

Diagram 1: The red line shows the possible flow of data between a public network (Internet) and a private network (corporate Intranet) if both are connected to by the user at the same time. Note that there is the possibility that only 1 GGSN is involved, rather than 2 as shown. Note also that ACME Inc.'s intranet is connected to the GGSN by a "private wire".

Many companies already have IT policies in place which prohibit, say, connecting one's computer to the company LAN at the same time as dialling into an ISP. But with GPRS, the user may unwittingly connect to both a private and public network for a number of reasons:

- there are no cables for the user to see to remind them to disconnect say, an Ethernet cable before connecting a phone/ISDN cable as they normally would;
- their understanding of GPRS may be such that they think only one connection (PDP Context) can exist at any given time and the previous connection to say, the Internet, will be automatically torn down before connecting to their corporate intranet;
- they forget to disconnect from the Internet first, before establishing a connection to their corporate intranet.

Therefore, individual company/corporate IT policies alone do not cater for the above. An operator may filter out packets where the source address is different from the MS's (which stops the end user becoming a router at the IP layer, unless some NAT is performed) by use of firewall configuration, but this does not stop anything at the application layer, e.g. a hacker from the Internet could still potentially log-in to your computer and from there run some kind of attack on the corporate network.

Corporate GPRS access is sold as a layer 2 – VPN - type service and as such raises expectations that a corporate customer is safely connected to their corporate intranet. Today, most GPRS terminals support only a single primary PDP Context being active at a given time. But as technology moves forward, more and more GPRS terminals will start to support multiple active primary PDP Contexts. This is not necessarily beneficial for corporate customers who may rely on the security of their remote users being able to activate only one PDP Context at a time. This could have an impact on whether some customers upgrade their GPRS terminal i.e. if a new terminal is considered by a customer to be less secure, they will be very reluctant to upgrade.

It is Vodafone's view that we should uphold the high user expectations of the security of the GPRS/VPN service as far as possible as technology in the GPRS terminal evolves.

Proposed Solution

Vodafone propose that the solution be based in the network rather than in the terminal equipment (e.g. firewall software on a computer). There are a number of reasons for this:

- Presence – the network operator can ensure that the functionality is always present when required
- Trustworthiness/integrity – IT administrators can better rely on a mobile network operator to have this functionality present and working, much more than they can rely on a piece of software being installed, *and* properly configured, *and* running correctly on absolutely *any* computer the employees of the company use to attach to the corporate intranet
- Maintenance – changes to policy can be more easily updated in the mobile operators network (update of the configuration for 1 APN) compared to having to update the software in potentially hundreds or even thousands of corporate users computers

Conclusion

Vodafone propose that SA3 endorse the concept of enabling the network to deny the establishment of new PDP Contexts dependant on where there is/are currently other(s) active. Vodafone see the changes as a "Technical Enhancement & Improvement" (TEI) which should be made to Rel-5 and onwards.

3GPP TSG-SA WG2 meeting #33 **Tdoc S2-031749**
Sophia Antipolis, 07th – 11th July 2003

3GPP TSG SA WG3 Security — S3#28 **S3-030303**
6 - 9 May 2003
Berlin, Germany

Title: **Security issues regarding multiple PDP contexts in GPRS**

Source: **SA3**
To: **SA2**
Cc: **CN4**

Reply to: **S2-031589**

Contact Person:
Name: **Peter Howard, Vodafone**
Tel. Number: +44 1635 676206
E-mail Address: peter.howard@vodafone.com

Attachments: None

SA3 has considered the LS from SA2 (S2-031589) which asks SA3 to clarify the nature of the security threats associated with multiple simultaneous PDP contexts in GPRS.

In the LS SA2 made the following comment:

"Specifically, there were questions on whether it was worth blocking multiple simultaneous PDP contexts when similar "problems" could be caused by successive PDP contexts with eg data being downloaded from an intranet, stored in the mobile, and then uploaded to the internet."

In response to this comment, SA3 believes that in general real-time access to a private network (e.g. corporate LAN) from a public network (e.g. the Internet) allows more powerful attacks to be performed compared to the case where real-time access is not possible. Furthermore, SA3 believes that real-time attacks could make use of existing software that is legitimately present on the terminal, whereas some attacks which do not involve real-time access would require the attacker to plant trojan software on the terminal. Attacks which do not involve real-time access are therefore considered to be both more difficult to mount because they require more control over the user's terminal and easier to detect.

For these reasons SA3 consider it worthwhile to block simultaneous PDP contexts even if successive PDP contexts are still allowed. Of course, the mechanism to block simultaneous PDP contexts for particular combinations of APNs needs to be cost effective.

There are also alternative mechanisms to blocking simultaneous PDP contexts to mitigate the threats identified above.

Actions

To SA2 and CN4:

To inform SA3 about potential mechanisms to solve the problem in order for SA3 to evaluate the security aspects

Next SA3 Meetings

SA3 meeting #29	15th – 18th July 2003	San Francisco, CA, USA
SA3 meeting #30	7th - 10th October 2003	TBD

3GPP TSG-SA WG2 meeting #33 **Tdoc S2-032321**
Sophia Antipolis, 07th – 11th July 2003

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