3GPP TSG-SA WG2 meeting #31 Tdoc S2-031589

Seoul, Korea, 7th – 11th April 2003 **rev of S2-031529**

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

Response to: **S2-031118 = S3-030164**

Source: **SA2**

To: **SA 3**

Cc: **CN 4**

Release: **Rel-6**

Contact Person:
Name: **Chris Pudney**
E-mail Address: **chris.pudney@vodafone.co.uk**

Attachment: S2-031369

SA 2 received the LS from SA 3 on this topic and discussed the attached S2-031369. No conclusion was reached on the proposals within this SA 2 tdoc because the discussion focused on the exact nature of the security threats.

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.

Actions

SA3 are requested to clarify the nature of the security threats.

Next SA2 Meetings

Meeting	Date	Location
SA2#32	12-16 May 2003	San Diego, USA
SA2#33	7-11 July 2003	Sophia Antipolis, France

Title:	**Discussion on Security Issues with Multiple Primary PDP Contexts**
Source:	Vodafone UK
Agenda item:	9
Document for:	Discussion and Proposal

1 Problem

In GPRS it is possible that a user can have multiple active PDP Contexts to different APNs (Multiple Primary PDP Contexts). If there exists simultaneous connections to a private network (e.g. a corporate intranet) and to a public network (e.g. internet connection), there is the possibility of the UE becoming a router or application layer proxy for data from the Internet on to the private network.

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.

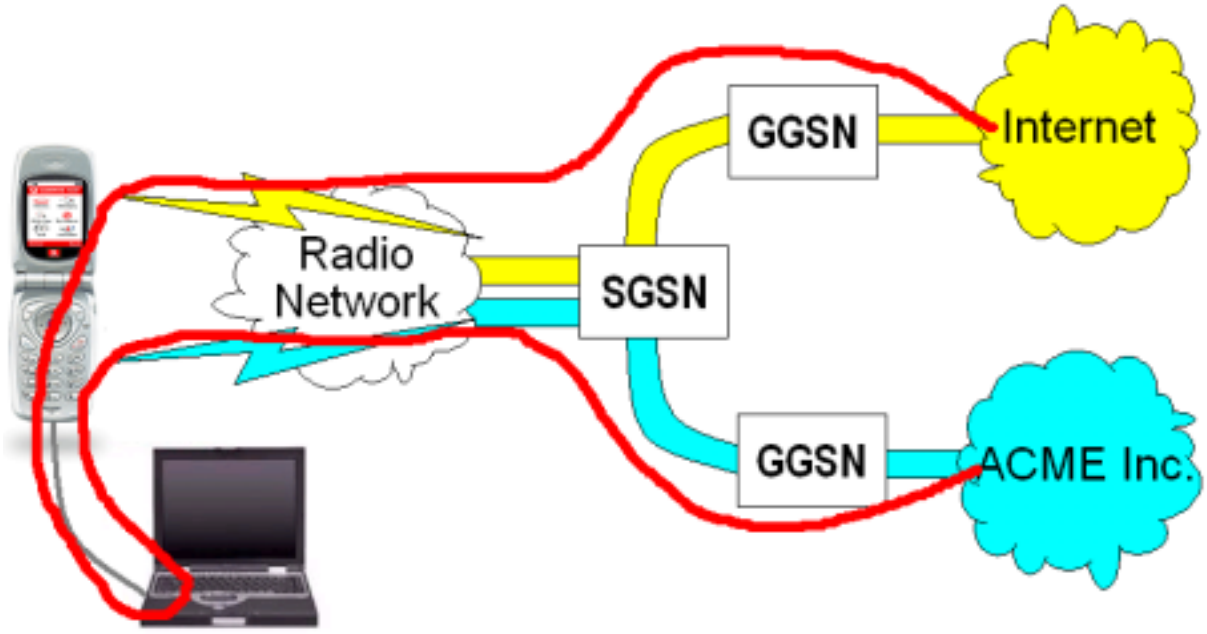

Figure 1: The red line shows the possible flow of data between a public network (Internet) and a private network (corporate Intranet) if both are connected to by the user at the same time.

Note 1: There is the possibility that only 1 GGSN is involved, rather than 2 as shown.
Note 2: ACME Inc.'s intranet is connected to the GGSN by a "private wire".

Many companies already have IT policies in place which for example prohibit 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 concurrently 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.

2 Options

Any solution needs to cater for approved combinations of PDP contexts of different types of APN. For example, there should be the possibility to allow PDP contexts to be established to APNs which deal with the sending and delivery of Multimedia Messages (MMs); otherwise some users who use the Multimedia Messaging Service will not be able to receive any MMs while they are connected to the internet. Conversely, for corporate customers who take their security *very* seriously (e.g. government organisations, the military etc.) the solution also needs the possibility to prohibit *any* other connections existing at all while connected to the corporate network.

An example of the way each APN may be classified is shown in Table 1.

Table 1. Table Showing Possible Types of APN

Type	Public or Private APN	Typical endpoint	Allowed to exist with (types)
0	Public	WAP	0, 1, 2
1	Public	Internet or PSPDN	0, 1
2	Private	Corporate (who use MMS)	0
3	Private	Corporate (who do not use MMS)	None

There is the question, though, of how the network should deal with setting up a connection to a corporate network while there already exists a connection to a public network(s) (or vice versa)? There is a number of options which can be taken:

1. Put the existing PDP Contexts on hold;
2. Tear down the already existing PDP Contexts, and then establish the PDP Context being requested;
3. Deny the PDP Context being requested from being set up.

The first option is not viable as there is not much the SGSN can actually do with any packets coming in from the PDP Contexts which are put on hold; the user's application

sessions/downloads/etc. could time-out. Also holding of a PDP context is only really feasible over short periods of time.

The second option is also not really viable as it is not particularly user friendly; without warning, sessions/downloads from the public network(s) will terminate.

This leaves only the third and last option, which seems to be the most viable as long as an appropriate failure cause is received. This would then allow the user to perform the appropriate actions necessary to activate the PDP context (if it is still required). Further details of this option are provided below.

2.1 Terminal Based Solution

2.1.1 UE Based

In this case, the control of approved context combinations lie in the UE. The UE must detect the PDP Context Activation Request and check whether there is an already active PDP context. The UE must also be aware of the subscribed APNs and their associated restrictions. This mechanism is required to be performed per user and as there may be many users subscribed to a particular APN, management of this would require a large amount of resources. Therefore this solution is undesirable.

2.1.2 TE / Software Based

In this case, the control of approved context combinations lie in the TE (even for combined TE and ME) and may be performed by software. Vodafone accepts that this is outside the scope of 3GPP, but wish to further note that controls using this method would require large scale management from an IT perspective. This is because a new connection management installation would be necessary by users whenever a subscribed APN changes configuration (for allowed context combinations). Also there is an issue with software corruption requesting undesirable behaviour. Therefore this is an undesirable solution.

2.2 Network Based Solution

Vodafone proposes that a new field is added to the GPRS information stored in the GGSN for each APN. This field shall enable the GGSN to prohibit active PDP Contexts to specific APNs existing at the same time. Depending on APN configuration, PDP contexts may not necessarily terminate at the same GGSN for all APNs that a user is subscribed to. This can be seen in figure 1 and therefore the SGSN is likely to be the common point in a network and may be able to store information about already active PDP contexts. Therefore the general procedure can be described as follows:

1st (Primary) PDP Context Activation:

1. SGSN sends Create PDP context request message to GGSN.
2. GGSN sends back a Create PDP context response which contains the Type of the APN requested.
3. SGSN remembers the Type for the now active PDP Context.

Subsequent (Primary) PDP Context Activation:

1. SGSN sends Create PDP context request message to GGSN which contains the type of the most restrictive APN which currently has an active PDP Context (e.g. type 0, 1, or 2).

2. GGSN performs the following check before sending back anything:

If the type of APN for this PDP context request does not conflict with the type of the most restrictive APN for already active PDP context(s), then the connection shall be allowed. Otherwise, the context connection shall be prohibited.

If the connection is allowed, the GGSN shall accept the Create PDP context request which contains the Type of the APN of this request, otherwise it shall reject the Create PDP context request with an appropriate error cause.

3. If the SGSN receives a rejection then it shall prohibit the user from setting up the new PDP Context and shall send an appropriate error to the MS. Otherwise, the remainder of the PDP Context Activation procedure may proceed and the SGSN shall store the Type of the new PDP Context. The SGSN then calculates the highest “restrictiveness” of the types of APN that already have active contexts. This value shall then be stored also.

Upon Deactivation of a PDP Context:
The SGSN must recalculate the highest restrictiveness of the Types of the currently existing PDP Contexts and store this value.

2.2.1 Known Issues

For Inter-SGSN Routing Area Updates, it is possible to move to a SGSN that does not support the feature for barring contexts and therefore the user may set up non-approved PDP context combinations.

3 Conclusion

It is proposed that the associated CR on 23.060 using the network based solution, detailed in section 2.2, is discussed and approved.

It is also recognised that this security issue afflicts over access technologies, most notably WLAN that is being standardised in 3GPP.