06 - 10 October 2003

Povoa de Varzim, Portugal

Title:	**Analysis of proposed network based access control solution for multiple PDP contexts**
Source:	**Nokia**
Agenda item:	**7.10**
Document for:	**Discussion and decision**

1 Introduction

SA3 has received the SA2 reply LS [S2-033240] on *Security issues regarding multiple PDP contexts in GPRS* where SA2 asks SA3 *'to discuss/document the security problem regarding multiple active connections and to inform SA2 of the most appropriate mechanism to address the security issues'*.

According to the LS, SA2 has been discussing potential mechanism to resolve the security issues. Contributions [S2-032978] on *Discussion on Security Issue with Multiple Active Connections* and the respective CR [S2-032979] on *Security Issue with Multiple PDP Contexts* were presented in SA2#34 according to the draft minutes of the meeting.

This discussion paper analyses the network based access control solution presented in these SA2#34 contributions.

2 Threat Model

Security analysis in [S2-032978] begins with a threat model, but the document does not seem to provide one.

The suggested "security hole" is that an MS can have several open primary PDP contexts, and it would seem that packets could flow from one to another, possibly circumventing firewalls or other security checks. However, since the network is packet-switched, the packets will pass through the MS only if a path has been established trough it, and the path has been advertised to the rest of the network as a better alternative to other routes. For this to be possible, the following conditions must be fulfilled:

- The MS acts as a router, *i.e.* it supports a routing protocol
- The GGSN daemon runs a routing protocol over the PDP context
- The GGSN accepts and forwards the route advertised by the MS
- The corporate network accepts the route advertised by the MS
- The route does not conflict with the Autonomous System boundaries of Border Gateway Protocol (BGP)

For the packets to pass through the MS, all of the above must be fulfilled (logical AND), but in real life *none* of them seem to be possible. Therefore routing through the MS is not a realistic threat. Only packets that are explicitly addressed to the MS will reach it.

The only case where packets can flow from one PDP context to another is software entity that deliberately bridges the two interfaces. If we assume that the subscribers are not evil (they could copy the material by other means if they were), the only possibility is that the MS has a "Trojan horse" program, installed by someone else and unnoticed by the lawful authorized to do so.

So the threat model is a Trojan horse.

3 Suggested Solution

The CR [S2-032979] suggests using a token to indicate which Access Points can be used at the same time:

Table X. Valid Combinations of APN Restriction

Value	Type of APN	Typical endpoint	Valid Combination with Values:
0	Public-1	WAP or MMS	0, 1, 2
1	Public-2	Internet or PSPDN	0, 1
2	Private-1	Corporate (who use e.g. MMS)	0
3	Private-2	Corporate (who do not use e.g. MMS)	None

In case of conflict the operator decides what to do. The CR doesn't specify or suggest actions, but it is obvious from the text that the conflict would be resolved by dropping one or more PDP contexts.

But a Trojan horse does not depend on simultaneous PDP contexts. It can

- use the existing PDP context to send the material to a public IP address through the corporate intranet (it is well known that edge routers have no scalable way of blocking all malicious addresses in real time);
- store the material it wants to deliver to malicious hands, and send it later; or
- format its material to a multimedia message, and send it to any phone number (case "Private-1" above).

Thus the suggested method does not offer defence against the threat model.

4 Alternative solution for the network based solution

Assuming that some combinations of simultaneous PDP contexts are to be prevented, it is possible to do so even with existing equipment. For example, an employer distributes SIM cards to its employees. The subscriptions lists the corporate APN as the only allowed APN. The users can access the Internet through the employer's intranet, which can filter the content if necessary. If the cellular operator offers a dedicated MMS AP, its APN can also be listed as allowed (case "Private-1" above).

Users who want to use the Internet directly (bypassing the corporate intranet) can use private subscriptions. Those SIMs cannot give access to the corporate AP, thus preventing simultaneous PDP contexts from that side.

5 Conclusion

According to the analysis the following conclusions can be made

- the suggested solution does not offer protection against the threat, and
- similar restrictions can be implemented with existing equipment anyway.

terminal based solution, e.g. personal firewall implementation in the terminal, should be preferred solution for the problem.

6 References

[S2-033240] SA2 reply LS to SA3, Security issues regarding multiple PDP contexts in GPRS

[S2-032978] Discussion on Security Issue with Multiple Active Connections, SA2#34, Vodafone UK

[S2-032979] CR to 23.060, Security Issue with Multiple PDP Contexts, SA2#34, Vodafone UK