3GPP TSG SA WG3 Security — S3#19 **S3-010343**

3 - 6 July, 2001

Newbury, UK

Joint Meeting on UE Split Security and IMS

Source: Nortel Networks

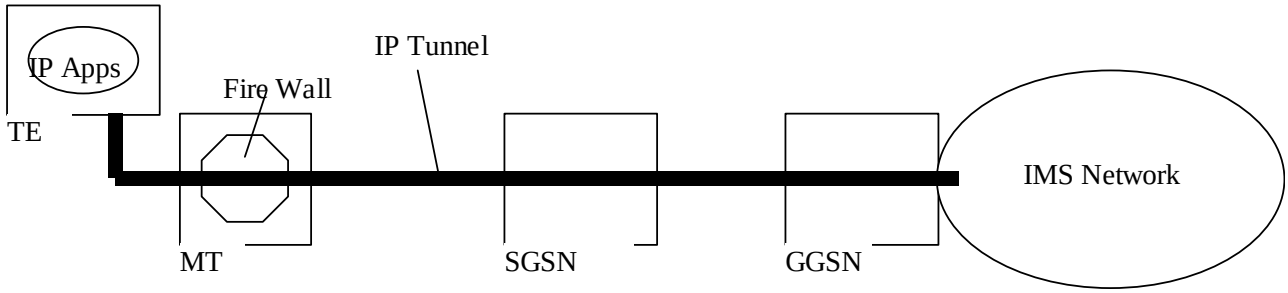
Title: Discussion Document on Location of Firewall Functionality

Introduction

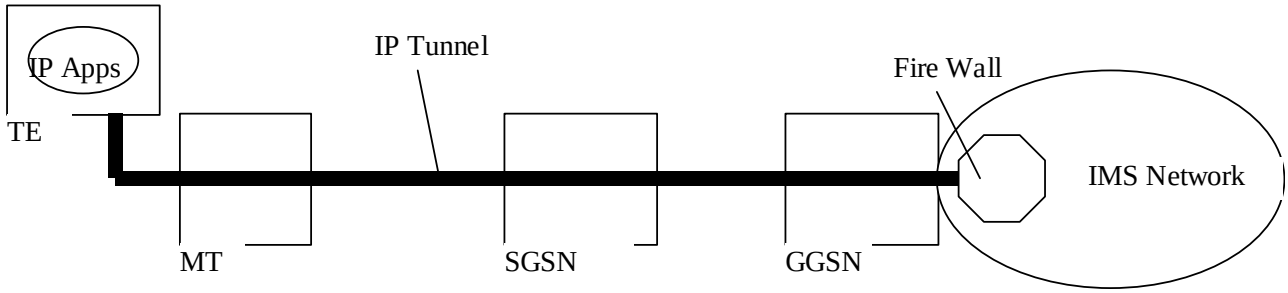
The introduction of the split-UE concept highlights the possibility that IMS clients implemented on a TE may behave in an inappropriate way – either maliciously or because of bad design. In an extreme case a malicious IMS client may attempt to attack the IMS network via a range of well-known techniques (IP port probes, exploitation of maintenance messages, DoS etc.). In order to protect the IMS network against this problem some kind of firewall will need to be introduced. This could take a number of forms – including a back-to-back user agent (B2BUA), an application level gateway (ALG). The intent of this firewall would be to allow "good" normal operations to continue, but to prevent or monitor unusual or "bad" behaviour.

Two locations for the firewall are immediately apparent:
a) In the MT part of the split UE
b) In the network close to the GGSN
These are illustrated below.

a) Firewall in the MT



b) Firewall in the Network



Options for Location of Firewall Functionality

The following sections discuss the two options under a number of headings.

2. Comparison of Options

2.1 Effectiveness

As shown in the figure the firewall can sit either end of a secure IP tunnel. In the proposed configuration no user data can escape-from or enter this tunnel. Therefore the only difference between the two solutions is which end of the tunnel the firewall functionality is applied. If the firewalls contain the same algorithm then exactly the same level of protection of the IMS will result in either case.

If in case a) attacks come from the IMS client on the TE then the firewall will be able to stop data before it travels over the radio interface. However in case b) the data will travel over the radio interface before it is stopped. This is an advantage for case a), but:

- The usage of the radio interface is still subject to the GPRS/PS domain subscription limits and policy
- Any usage made of the radio interface may be chargeable by the network operator – therefore this is not a method to steal service.

The case of an attempt to attack the IMS client from within the IMS network cannot be ruled-out. In this case the advantages of the two approaches are reversed.

2.2 Impact on Applications other than SIP

In release 5 the only standardised application for the IMS is SIP. However in future other applications may be added to the standard. Even in release 5 networks other applications not explicitly discussed in the IMS standard will also be used (eg WAP). A firewall in the network (case b) can be designed to allow correct use of all applications supported in that network. A firewall in the MT (case a) however cannot know about the applications the network supports. Therefore it is hard to see how an MT based solution can provide effective security for applications other than SIP.

2.3 Evolution of the SIP application

Once deployed in UMTS the SIP application will evolve. Case b) allows the firewall to be modified to support an evolving SIP application. However in case a) assumptions made in the design of the firewall in the ME may prove an obstruction to application evolution. For example, how can unknown messages be handled? Which unknown messages are malicious and which are the result of changes to the SIP standard?

2.4 Security

Though modification of MT software is typically much harder than modification of TE software it is not impossible. It can be expected that technology trends will make it easier to modify MT software as time goes on. Therefore it cannot be assumed that any implementation that relies on the MT behaviour is completely secure. A solution based on option a) may need elements of option b) to act as a back-up. In this situation the value added by having a) in addition to b) may be questioned.

2.5 Control of policy

In the case of option a) the policy implemented by the firewall will essentially be set at the time of manufacture of the MT. It will be hard for operators to determine different policies to suit their individual needs. In the case of option b) the policy can be set by the serving network operator.

3. Conclusion

In this discussion paper it would be inappropriate to draw a firm conclusion. However the following points can be noted:

- If the right tunnelling configuration is used then the two options are equal in terms of their effectiveness at protecting the IMS.
- Option a) has the advantage that it can prevent use of radio resources by malicious IMS clients in the UE. However even with option b) the upper limit on the malicious use of resources is set by the PS-domain subscription granted to the user.
- Option b) has advantages in terms of evolution, flexibility and management.

It is proposed that a more detailed comparison of the options is produced. Other factors not mentioned so far which may be studied include:

- Cost
- Impact on users accessing systems other than IMS
- Alignment with other access technologies.