3GPP TSG SA WG3 Security — S3#29 **S3-030428**
15 - 18 July 2003
San Francisco, USA

3GPP TSG SA2#32 **S2-032730~~44220~~**
Sophia Antipolis, France, 7th – 11th July 2003

Title:	**LS on ~~PDG IP~~ Denial of Service attacks against the 3GPP WLAN Interworking system**
Source:	**SA2**
To:	**SA3**
Release :	**6**
Contact:	**Mark Watson (mwatson@nortelnetworks.com)**
Number :	**+441628434456**
Attachements :	**S2-032483 "**Security analysis for tunnel establishment"

1 Overall Description

SA2 is currently defining the architecture for interworking between WLAN systems and 3GPP networks. In particular mechanisms for UEs to obtain IP connectivity to the External IP networks currently accessed over the Gi interface.

SA2's architecture for this includes a Packet Data Gateway (PDG) which acts as a gateway between the External IP Networks and an inter-PLMN backbone (which could be GRX). SA2 has also defined a WLAN Access Gateway (WAG) which acts as a gateway between the WLAN Access Network itself and the same inter-PLMN backbone.

Various solutions are under discussion regarding the level of security required at the WAG, for example the extent to which users can send packets towards the WAG which will then be routed onto the inter-PLMN backbone towards the PDG.

SA2 has received the attached contribution which considers the level of protection afforded to the PDG against Denial of Service attacks under several of these solutions.

The security properties of these solutions are a major consideration for SA2 in making an architecture choice and therefore SA2 would appreciate any comments that SA3 has on the validity of the attached analysis, or indeed on other security issues that they believe SA2 should take into account.
~~'PDG Address Discovery' is the process by which the UE obtains the IP address of the PDG. It is required for the **end-to-end tunnelling**.~~

~~In more detail about the DNS proposal:~~

~~After UE is authenticated by WLAN and gets a local IP address and DNS server address from WLAN. The UE then will use a FQDN (stored in terminal or generated itself) to query the DNS server in the WLAN to get the IP address of the PDG.~~

2 Action

SA2 kindly asks SA3 to comment on the validity of the attached paper and any other security issues that they believe should be considered in SA2's ongoing architecture work.

3 Next meeting

SA2 #34	18 - 22 Aug 2003	Brussels
SA2#35	27 – 31 October 2003	tbd

3GPP TSG-SA2#33 ***Tdoc S2-032483***
Sophia Antipolis, France, 7-11 July, 2003

Agenda Item: **11.2 WLAN**

Source: **Nortel Networks**

Title: **Security analysis for Tunnel Establishment**

Document for: **Decision**

1. Introduction

A number of discussions on the tunnelling options, both at the meeting and on the email lists, have focussed on the security implications for the inter-PLMN backbone.

This contribution analyses some of the security issues to be considered.

We note that the inter-PLMN backbone to be used for WLAN roaming may or may not be the same inter-PLMN backbone used for GPRS (the 'GRX'). In this paper we assume that is it the same network.

2. GRX addressing

The GRX network is essentially a private network shared between GRPS operators and disconnected from the Public Internet. However, the addresses of elements on the GRX are still public addresses. The following is from GSM-A document IR.34 (https://infocentre.gsm.org/tmp_docs/ir34330.htm)

> "2. **IP Addressing**
>
> Public addressing should be applied in all GPRS backbone networks. Using public addressing means that each operator has a unique address space that is officially reserved from Internet addressing authority. However, public addressing does not mean that these addresses should be visible to Internet. GPRS intra- and inter-PLMN backbone networks shall remain invisible and inaccessible to public Internet.
>
> It is imperative to use unique public addressing in *all* visible network elements of the intra and Inter-PLMN networks. With current Network Address Translation (NAT) implementations it is impossible to use NAT because NAT can not change IP addressed, such as SGSN address in PDP context activation request, that are carried inside GTP tunnel.
>
> IP version 4 address space is a limited resource. IPv6 will eventually resolve addressing limitations but the introduction of GPRS services cannot be tied to the schedule of IPv6. Regardless of IPv4 address space limitations, the usage of public addresses is a feasible solution. Schedule and terms of IPv6 deployment in the Inter-PLMN backbone will be subject to bilateral agreements and/or Inter-PLMN backbone operators to PLMN operator agreements."

For a host to be visible from the Public Internet means that any other device on the Internet can send packets to and receive packets from that host. Therefore, the above requirement does not prohibit *specific* authorised *devices* from sending packets to and from the GRX – for example authorised 3GPP UE's.

3. GRX Security threats

A comprehensive analysis of GRX Network Domain Security is available in GSM-A Association Document "GPRS/3G Roaming Inter-PLMN Backbone: Network Domain Security Considerations" (https://infocentre.gsm.org/cgi-bin/securenonprddownload.cgi/gp%20network.zip?56758&zip).

This largely addresses the mechanisms needed to ensure that the GRX network is isolated from other networks using the same physical infrastructure, but also notes:

"What is of concern to the IREG PacketWP is the level of security each of these solutions provide. It has been agreed within the PacketWP (ref PWP#1 and GRX TF #1 meetings, Düsseldorf) that the main security requirement is the prevention of DoS or DDoS attacks on each Operators platforms/systems. The priority of this is based on the potential loss of revenue caused by such attacks. D/Dos attacks can occur if a hacker is able to maliciously insert IP packets into the GRX network domain from another IP network domain.

It was also agreed within the PacketWP that although protection against eavesdropping on GTP content (especially signalling information containing IP addresses of the SGSNs and GGSNs) is important it not a critical requirement since many thousands of people will know these IP addresses anyway."

As a result, this paper concentrates on Denial of Service attacks which could be launched from a 3GPP WLAN UE.

4. Assumptions

In this analysis we assume the following:

- Only users which have been authorised to use the 3GPP system will be able to have their traffic routed to the VPLMN, or be able to receive traffic from the VPLMN

  i.e. we assume some kind of routing policy enforcement in the WLAN and/or on the VPLMN border which protects the VPLMN from users which are not authorised for WLAN access at all

- The WLAN is not secure against IP address spoofing. i.e. depending on the solution to routing policy enforcement describe above, one authorised 3GPP UE may be able to masquerade as another in the source address of IP packets (although security on the WLAN radio link will make it quite difficult to *discover* the IP address of another authorised UE on the same WLAN)

- Firewall policies at the edge of the GRX network (i.e. the WAG) will *at least* block any traffic which is not either Tunnel Establishment traffic or Tunnelled Data itself, based on destination port filtering

- Firewall policies at the edge of the GRX network (i.e. the WAG) will *at least* block traffic which is not addressed to or from a PDG of a roaming partner of the VPLMN

5. Tunnelling and security options

Various levels of security have been proposed within the "tunnel-switching" and "end-to-end" approaches. We examine these different levels, from the seemingly 'least secure' the seemingly 'most secure'. The objective is to determine whether these initial impressions are in fact correct.

5.1 End-to-end tunnelling with static security

In this case the only security functions at the edge of the GRX network are those described in Section 4.

3GPP UEs which are authorised for WLAN access will be able to freely send Tunnel Establishment and Tunnel Data packets on to the GRX towards the PDGs of any network which has a roaming agreement with the VPLMN.

This security should protect the GRX against all attacks except Denial of Service attacks, since the only traffic from the UE which will pass onto GRX is Tunnel Establishment or Tunnel Data packets addressed to PDGs.

We note that both Tunnel Establishment and Tunnel Data mechanisms will include security features which allow the PDG to reject unauthorised Tunnel Establishment requests, or to drop unauthorised Tunnel Data packets. However both such operators consume resources at the PDG and on the link to the PDG, so floods of such requests could result in a Denial of Service to authorised users.

This situation is no different from that applying to any VPN gateway connected to the Internet – for example VPN gateways of corporate networks. In fact, the Firewall policies applied at the WAG are similar to those that would be applied at the exterior firewall of the DMZ (De-Militarised Zone) on which such gateways (and other servers) would usually reside. In effect the GRX is made into a DMZ.

We can therefore expect VPN gateway products (which might then become PDGs) to be robust against such attacks, as far as is possible.

A further measure would be to apply statically configured Diffserv policies at each WAG to limit the rate of Tunnel Establishment and Tunnel Data traffic to something just above the 'busy hour' rate. We can assume that the data rate required to effectively deny service at a PDG is significantly greater than this, since a single PDG could be expected to normally handle traffic from several WAGs.

[For example: suppose a given PDG receives traffic on average from n different WAGs. Suppose the busy hour traffic through each WAG is X erlangs and we apply Diffserv shaping to limit the traffic through each WAG to 2X erlangs. A DoS attack through a single WAG could then result in a maximum of (n+1)X erlangs towards the PDG. Since the PDG must be engineered to handle nX erlangs in any case, then the additional capacity required at the PDG to survive such an attack is minimal, especially as n increases. We apply this scheme separately to Tunnel Establishment and Tunnel Data packets.]

This greatly mitigates the effect of any DoS attack from a single WLAN. In the event of such an attack, Tunnel packets will be dropped at the WAG, meaning that the PDG, GRX, and Tunnel packets routed through different WAGs are not affected.

So, the Denial of Service would be limited to users of the WLAN from which it was launched. Further, the effect would be to deny (or reduce) service to all users on that WLAN. This means it would not be possible to target an attack at a single 3GPP operator, which greatly reduces the motivation for such attacks.

In fact, the attack would be less effective than a simple attack against the WAG or even the WLAN itself, which could be launched by flooding the WAG or WLAN with packets. Such attacks cannot be mitigated by the 3GPP network in any way.

The above measure does not protect against Distributed Denial of Service attacks, in which many UEs on different WLANs are used to launch an attack against a single PDG. However, these are significantly more complex to launch, requiring the compromise of many separate UEs (standard UE software can be designed so that it will not re-attempt failed Tunnel Establishment requests to quickly, even if instructed by higher layers. So, a DDoS attack requires modified software on all participating UEs.)

5.2 End-to-end tunnelling with dynamic security

In this case, the security policies on the WAG are dynamically updated according to the UE's authorisation status. A special kind of 'controllable firewall' would be needed, along with standardisation of the control protocol. This could be based on the UE's basic WLAN authorisation status, or additionally on its tunnel authorisation status.

5.2.1 Dynamic update based on WLAN Authorisation

In this case, default firewall policies at the WAG block traffic from all WLAN UE's on to the GRX.

When a UE is authorised for connection to the WLAN, then these policies are modified to allow:

- Tunnel establishment and Tunnel data packets from this UE to the PDGs of its Home Network, and
- Tunnel establishment and Tunnel data packets from this UE to the PDGs of the Visited Network

Compared to the security described in 5.1, this offers no additional protection to the PDGs of the Home or Visited networks or to the WAG and WLAN. However, it does prevent a DoS attack from the UE against a completely different network.

This has some value, since both Home and Visited networks are in possession of information which can link a particular UE IP address back to the actual user, so it is possible for either of them to trace a DoS attack and take action against the originator.

However, there does not seem to be any other obvious mitigation of DoS or DDoS attacks compared to the schemes described in 5.1.

5.2.2 Dynamic update based on Tunnel authorisation

In this case, the scheme of 5.2.1 is applied to Tunnel establishment packets only. Tunnel data packets are by default blocked.

When the user is authorised for tunnelling to a particular PDG, then the policy at the WAG is modified to allow Tunnel Data packets to that specific PDG only.

This mechanism limits the attacks mentioned above to:

- Attacks from any WLAN authorised UE using Tunnel Establishment packets
- Attacks from a Tunnelling authorised UE using Tunnel Data packets

In the first case, this scheme has some advantage since the Diffserv controls applied to Tunnel Establishment packets can be more closely engineered than those applied to Tunnel Data (which will be expected to be fairly high volume even in normal cases). But this does not seem to be a very significant advantage.

5.3 PDG address hiding using NAT

It has been suggested that the WAG could consist of a dynamically configured NAT function, which will hide the real PDG address, providing an externally visible address for the PDG only when the user is authorised for Tunnel Establishment to that PDG.

This requires a separate exchange between UE and WAG to request tunnelling authorisation and NAT configuration from the WAG. Before successful completion of this exchange, no tunnel establishment or tunnel data packets are allowed, and so DoS attacks against the PDG are not possible.

However, a DoS attack could still be launched using this separate protocol. On receipt of a request from the UE, the WAG must contact the HPLMN to obtain an authorisation decision. This will likely take place using the AAA infrastructure. It is possible, therefore, to attack the AAA infrastructure in the HPLMN by launching repeated requests.

As with the scheme of 5.1, the AAA traffic from each WAG can be limited, for example to twice the busy hour traffic flow, so that the effects of the attack are limited to a single WAG and in fact become no worse than a simple DoS attack against that WAG or the WLAN.

However, this scheme again does not appear to offer any additional security compared to that described in 5.1.

5.4 Tunnel switching

In this approach, tunnel establishment requests are terminated on the WAG and a subsequent tunnel established from WAG to PDG only if the UE is authorised.

The same attacks as those described in 5.2.2 are possible with this scheme. Again, it would be expected that the WAG would limit the rate of tunnel authorisation requests and tunnel data packets to something slightly greater than the busy hour norm, and again this limits the effect of such attacks to the WAG itself.

So, even this scheme does not appear to offer any advantage over 5.2.2, and so no significant advantage over 5.1

6 Conclusion

One of the most important principles in network security is never to encourage a sense of security where non exists.

From the above analysis, none of the more complex policing schemes which have been suggested offer significant advantage over simple static firewall policies and traffic limiting at the WAGs as described in 5.1. In this scheme, the effect of DoS attacks is limited to the WAG. DoS attacks against the WAG cannot be prevented in any of the schemes.

None of the schemes offer additional protection against Distributed Denial of Service attacks, but these are extremely difficult to launch in any case.

We believe that in order for additional functionality, complexity and cost to be justified, it must offer a significant advantage to network operators.

As a result, we do not see that the suggested additional functions at the WAG are justified on security grounds. At least they are not justified in terms of mitigation of Denial of Service attacks, which is seen as the principle threat against operators systems by GSM-A IREG.