3GPP TSG SA WG3 Security — S3#31 **S3-030702**
18 - 21 November 2003
Munich, Germany

Title: **Security Analysis on the SA2 resolution architecture**

Source: **Huawei Technologies Co., Ltd.**

Agenda item: **WLAN interworking**

Document for: **Discussion**

1. Overall Description:

This doc addresses the security related questions with the solution in the SA2 LS S2-038313:

- the solution relies on the assumption that it is possible to separate the tunnel establishment and tunnel data handling into separate nodes, noting that these nodes are both in 3G networks, and not linked over the public internet.
- Additionally, no decision has been made on whether the W-APN Resolution Gateway would be located in the VPLMN or HPLMN and therefore these nodes may not necessarily be in the same PLMN.
- The security advantages offered by protecting the PDG before user authentication/authorisation in the way described above
- Whether the W-APN Resolution Gateway would become a single point of failure.

2. Analysis:

2.1 It is possible to separate the tunnel establishment and tunnel data handling into separate nodes.

(1) This can be realized with tunnel broker techniques for various tunneling mechanisms. (Is this out scope of SA3?)

For example: IPv6 Tunnel Broker, refer: RFC3053, IPv6 Tunnel Broker. A. Durand, P. Fasano, I. Guardini, D. Lento. January 2001.

(2) In the security sense, the architecture in the LS is in line with the current SA3 GAA/GBA: PDG is a kind of NAF, 3GPP AAA server together with the R-GW act as BSF for authentication,

The R-GW:

- does not need to be trusted by the home operator to handle authentication vectors, 3GPP AAA server is the entity for it.
-needs only to be trusted by the home operator to handle derived key material, if these material need to handle in it.
-needs to be trusted by the home operator to broke the tunnelling for PDGs, the trust level is same to PDGs.

It is also possible for the R-GW to be in the VPLMN, if there is trust relation between the home and visited network. The VPLMN R-GW can serve for VPLMN PDG, and for HPLMN PDG.

2.3 Advantages of security with the R-GW architecture: Ensure the UE is authenticated and authorized before UE can directly contact PDG.

The UE data do not allowed to be routed to any of the PDG before it was authenticated and authorized to access that PDG, so the PDGs will keep from the attack from unauthenticated or unauthorized UEs, the range of exposing is then limited.

Separate the transport signaling and the control signaling (authentication, resolution & authorization, tunnel establishment) improves the security condition of PDGs：

（1） PDGs are accessible only to those who was authorized to access it, it do not need to be designed or updated to take care of various attack and face to unauthorized users.

（2） The R-GW is limited and can be enhanced to deal with various attack, is easy to manage, operate or update incase of security accident. Better and easier than the PDGs in the network have to be enhanced and updated to prevent a new virus or attacks

（3） Even the R-GW is attacked and fail, the PDGs and the services already running at the PDGs will not be affected.

2.4 Whether the W-APN Resolution Gateway would become a single point of failure?

The R-GW is only involved in the tunnel establishment, combining authentication, authorization and resolution functionalities, is not involved in further interaction between the UE and PDG after the tunnel is established, it will not be a single point of failure. Even it is attacked or failure, the PDGs and their ongoing services will not be affected. However, as R-GW is exposed to all the WLAN access authorized UEs, it need more security enhancement (e.g. Dos attack absorbing capability) than the PDGs.

3. Proposals:

Considering the analysis in this doc, include valid points into the Reply LS to SA2.

3GPP TSG-SA3 Meeting #31 ***Tdoc ⌘S3-03xxxx***
Munich, Germany, 18-21 November 2003

Title: Reply LS on "Tunnel Establishment and Security Association"
Response to: LS (S2-033813) on Tunnel Establishment and Security Association from SA2
Release: Release 6
Work Item: 3GPP-WLAN interworking
Source: SA3
To: SA2
Cc:

Contact Person:
Name: **Robert Jaksa, Huawei Technologies Co., Ltd.**
Tel. Number: +1 972 509 5599
E-mail Address: rjaksa@futurewei.com

Attachments: None

---

1. Overall Description:

SA3 has been considering the security implications of SA2's LS in S2-033813 and have been discussing the security issue as requested in the LS. The conclusions are:

1. From the security view, it is possible to separate the tunnel establishment and tunnel data handling into separate nodes, if the two nodes are equally trusted by home operator. It shall be possible to support R-GW functions in the operator's home network, and need not preclude the support of R-GW function in the visited network, or possibly even in a third network. In security sense, this architecture is quite in line with the current SA3 work on GAA/GBA (Generic Authentication Architecture/ Generic Bootstrapping Architecture)
2. To the security advantages offered by protecting the PDG before user authentication/authorisation in the way described in the LS, SA3 concludes it improves the security environment of PDGs by separating the transport signaling and the control signaling (authentication, resolution & authorization, tunnel establishment) :

– PDGs are accessible only to those who was authorized to access it, it do not need to be designed or updated to take care of various attack and face to unauthorized users.
– The R-GW is limited and can be enhanced to deal with various attack, is easy to manage, operate or update incase of security accident. Better and easier than the PDGs in the network have to be enhanced and updated to prevent a new virus or attacks
– Even the R-GW is attacked and fail, the PDGs and the services already running at the PDGs will not be affected.

3. The R-GW is only involved in the tunnel establishment, combining authentication, authorization and resolution functionalities, is not involved in further interaction between the UE and PDG after the tunnel is established, it will not be a single point of failure. However, as R-GW is exposed to all the WLAN access authorized UEs, it need more security enhancement (e.g. Dos attack absorbing capability) than the PDGs.

2. Actions:

To SA2 group.

ACTION: **SA3 kindly asks SA2 to take notice of the SA3 conclusion.**

3. Date of Next TSG-SA3 Meetings:

TSG-SA3 Meeting #32 16-20 February 2004, Australia