3GPP TSG SA WG3 Security — S3#31 **S3-030788 (a)**
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, but may need extra efforts .

(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.

If this is in scope of SA3, then we need to verify whether current tunnel protocols can support the tunnel broker, how much efforts will be needed to make current tunnel protocol to support tunnel broker.

(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, so share all the advantages of GBA.

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.

2.2 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, and 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 design to serve all or several PDGs and can be easier to be enhanced to deal with various attack, easy to manage, operate or update incase of security accident.

Better and easier than all 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） Enables the control of service applicator source: keep the network configuration confidential in reasonable extent: the UE can only know what it is authorized to know;

~~if~~If the UE is not subscribed several services he can not know where the services are provided. ~~if~~If it is open to public DNS, then, even the UE did not authorized to know some information, it can, so it can easily get the whole configure information; Moreover, it is also possible, any kind of internet user also can know it from public internet, just through several public DNS queries.

2.3 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.

Further more, this is similar with BSF in GBA, and then BSF is also a single point of failure?

3 Threat of the tunnel establishment attacks

To PDG, the attacks using tunnel establishment messages ~~is~~may be much danger than those using tunnel~~e~~ data: PDG can quickly detect a data is forgery, because it have the keys share with UE, and do not need to check all the data, but some header security parameters, then it cost very limited time and resource to do it, even the data volume can be very large.

If a tunnel establishment reach PDG before the UE is authenticated and authorized, the PDG have to interact with AAA for authentication and authorization,~~When process with a tunnel establishment it have to interact with AAA for authentication and authorization~~, then AAA may need to contact with HSS for new vectors, the AAA need to derive keys, interact with the UE for authentication, the PDG have to ~~save~~ store the requests and wait the process results, attacking requests then consume lot of its time and resource.

Of cause, PDGs can be make more strong to d~~u~~eal with this kind of attacks, but if authentication can be decomposed from it, as in GBA, it will be easy to~~for~~ detect and deal with such kind of attacks, better for security management.

4 Confidentiality of network configuration of PDGs

.The configuration of PDGs, seems always be simply understood as only address of one or several PDG, this is not true, it is the whole information of the arrangement that the services are deployed to PDGs and the address of the PDGs, it is

taken as confidential business information by some operators, should not expose to public DNS which can be easily queried by any user from any device, mobile or fixed line, even from Internet.

We agree that ~~its~~it's difficult to keep one PDG address confidential for very long, and it can not help to mitigate the Dos attack to a PDG. But this is not a good reason for operators to open the configuration of PDGs to open DNS. If we can prevent it from expose to significant larger extent, we should do that. We can not absolutely keep it confidential; ~~but we~~but we should not then open the information for every one to access.

5. Security advantages of R-GW without tunnel broker function

Other one of three options discussed in SA2 for the SA2 3GPP-WLAN architecture is: decomposition of authentication authorization from PDG, set a RGW without tunnel establishment function: the UE perform authentication authorization& APN resolution with R-GW which will interact with 3gpp ~~AAA to~~AAA to process the request, and then setup tunnel with PDG.

Even If the tunnel broker can not be realized or too expensive to be realize, to separate the service authentication, authorization&APN resolution to RGW; PDG deal with the tunnel establishment also have the security advantage:

1.since the UE is authenticated and authored by the RGW+AAA, the PDG can detect the validity of the tunnel establishment request quickly with the TID as specified in GBA (not need to interact with AAA, then AAA interact with HSS for vectors, AAA derive keys), although it can not forbid all the tunnel establishment from access the PDG, but with GBA style authentication, the verification in PDG is far more quick than perform authentication then it also mitigates the Dos attack effects to PDG.

2. ~~same~~Same with second advantage of above mechanism: ease the security management of the whole architecture.~~.~~

3. ~~same~~Same with third advantage of above mechanism: enables the control of service applicator source: keep the network configuration confidential in reasonable extent

6. Summary security compare of possible architecture model

UE DNS client model was also discussed in SA2: a model in which users obtain a PDG address through DNS and establish a tunnel with this PDG using standard IP VPN procedures. It may be also acceptable to SA3 from only security perspective, if the control of confidentiality of network in reasonable extent is not a security issue.

Base on the security analysis, here we list the main security compare with the 3 proposed model discussed in SA2.

Architecture model	**attacks by tunnel establishment messages**	**Confidential of network configuration of PDGs**	**Feasibility from security related perspectives**	**Acceptable only from security perspectives?**
R-GW combine tunnel establishment	**Prevented**	**Access is limited to reasonable rang**	**Need verify the availability of tunnel broker enabled tunnel protocols**	**Yes, best**
R-GW without tunnel establishment	**Mitigated**	**Same with above**	**Reuse current VPN tunnel protocols**	**Yes , better**
Users obtain a PDG address through DNS and establish a tunnel	**Vulnerable**	**Open to all DNS query**	**Reuse current VPN tunnel protocols**	**May be also acceptable, with enhanced PDGs and ignoring the**

with this PDG using standard IP VPN procedures				**confidential of network configurations info**

7. Proposals:

Considering the analysis in this doc, we propose that:

(1) SA3 should acknowledge the security advantage with the 2 R-GW based architectures,

Separating the RGW and PDG has obvious security advantages:

1. mitigates the attacks threat to PDGs and facilitates the security management by decomposing the authentication from PDGs
2. in line with the SA3 GBA, have the advantages of separating service authentication with service data tunnel traffics interaction.
3. enables the control of service applicator source: keep the network configuration confidential in reasonable extent

By combining of tunnel establishment in RGW, the first advantage can be enhanced to prevent UE contact the PDGs before it is authorized , but this need develop broker support for the current tunnel protocols, it's advantage need to be evaluated with the additional cost introduced by supporting of tunnel establishment broker functionality.

(2) Guidance about the tunnel broker protocol is necessary if in scope of SA3;

(3) SA3 encourage separating at least service authentication authorization from PDG to achieve the security advantage of R-GW base architecture, and keep the architecture in line with GBA

~~**Separating the RGW and PDG has obvious security advantages:**~~

~~**1.mitigates the DoS attacks threat to PDG**~~

~~**2.in line with the SA3 GBA, have the advantages of separating service authentication and authorization with service data tunnel traffics interaction.**~~

~~**3.enables the control of service applicator source: keep the network configuration confidential in reasonable extent**~~

~~**By combining of tunnel establishment in RGW, the first advantage is stronger, but seems need develop broker support for the current tunnel protocols, this advantage need to be evaluated with the additional cost introduced.**~~

3GPP TSG SA WG3 Security — S3#31 **S3-030788 (b)**
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, but may need extra efforts.

(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.

If this is in scope of SA3, then we need to verify whether current tunnel protocols can support the tunnel broker, how much efforts will be needed to make current tunnel protocol to support tunnel broker.

(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, so share all the advantages of GBA.

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.

2.2 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, and 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 design to serve all or several PDGs and can be easier to be enhanced to deal with various attack, easy to manage, operate or update incase of security accident.

Better and easier than all 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） Enables the control of service applicator source: keep the network configuration confidential in reasonable extent: the UE can only know what it is authorized to know;

If the UE is not subscribed several services he can not know where the services are provided. If it is open to public DNS, then, even the UE did not authorized to know some information, it can, so it can easily get the whole configure information; Moreover, it is also possible, any kind of internet user also can know it from public internet, just through several public DNS queries.

2.3 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.

Further more, this is similar with BSF in GBA, and then BSF is also a single point of failure?

3 Threat of the tunnel establishment attacks

To PDG, the attacks using tunnel establishment messages may be much danger than those using tunnel data:
PDG can quickly detect a data is forgery, because it have the keys share with UE, and do not need to check all the data, but some header security parameters, then it cost very limited time and resource to do it, even the data volume can be very large.

If a tunnel establishment reach PDG before the UE is authenticated and authorized, the PDG have to interact with AAA for authentication and authorization,, then AAA may need to contact with HSS for new vectors, the AAA need to derive keys, interact with the UE for authentication, the PDG have to store the requests and wait the process results, attacking requests then consume lot of its time and resource.

Of cause, PDGs can be enhanced more strong to deal with this kind of attacks, but if authentication can be decomposed from it, as in GBA, it will be easy to detect and deal with such kind of attacks, better for security management.

4 Confidentiality of network configuration of PDGs

.The configuration of PDGs, seems always be simply understood as only address of one or several PDG, this is not true, it is the whole information of the arrangement that the services are deployed to PDGs and the address of the PDGs, it is taken as confidential business information by some operators, should not expose to public DNS which can be easily queried by any user from any device, mobile or fixed line, even from Internet.

We agree that it's difficult to keep one PDG address confidential for very long, and it can not help to mitigate the Dos attack to a PDG. But this is not a good reason for operators to open the configuration of PDGs to open DNS. If we can prevent it from expose to significant larger extent, we should do that. We can not absolutely keep it confidential; but we should not then open the information for every one to access.

5. Security advantages of R-GW without tunnel broker function

Other one of three options discussed in SA2 for the SA2 3GPP-WLAN architecture is: decomposition of authentication authorization from PDG, set a RGW without tunnel establishment function: the UE perform authentication authorization& APN resolution with R-GW which will interact with 3gpp AAA to process the request, and then setup tunnel with PDG.

Even If the tunnel broker can not be realized or too expensive to be realize, to separate the service authentication, authorization&APN resolution to RGW; PDG deal with the tunnel establishment also have the security advantage:

1.since the UE is authenticated and authored by the RGW+AAA, the PDG can detect the validity of the tunnel establishment request quickly with the TID as specified in GBA (not need to interact with AAA, then AAA interact with HSS for vectors, AAA derive keys), although it can not forbid all the tunnel establishment from access the PDG, but with GBA style authentication, the verification in PDG is far more quick than perform authentication then it also mitigates the Dos attack effects to PDG.

2. Same with second advantage of above mechanism: ease the security management of the whole architecture.

3. Same with third advantage of above mechanism: enables the control of service applicator source: keep the network configuration confidential in reasonable extent

6. Summary security compare of possible architecture model

UE DNS client model was also discussed in SA2: a model in which users obtain a PDG address through DNS and establish a tunnel with this PDG using standard IP VPN procedures. It may be also acceptable to SA3 from only security perspective, if the control of confidentiality of network in reasonable extent is not a security issue.

Base on the security analysis, here we list the main security compare with the 3 proposed model discussed in SA2.

Architecture model	attacks by tunnel establishment messages	Confidential of network configuration of PDGs	Feasibility from security related perspectives	Acceptable only from security perspectives?
R-GW combine tunnel establishment	**Prevented**	**Access is limited to reasonable rang**	**Need verify the availability of tunnel broker enabled tunnel protocols**	**Yes, best**
R-GW without tunnel establishment	**Mitigated**	**Same with above**	**Reuse current VPN tunnel protocols**	**Yes , better**
Users obtain a PDG address through DNS and establish a tunnel with this PDG using standard IP	**Vulnerable**	**Open to all DNS query**	**Reuse current VPN tunnel protocols**	**May be also acceptable, with enhanced PDGs and ignoring the confidential of network**

VPN procedures				**configurations info**

7. Proposals:

Considering the analysis in this doc, we propose that:

(1) SA3 should acknowledge the security advantage with the 2 R-GW based architectures,

Separating the RGW and PDG has obvious security advantages:

1. mitigates the attacks threat to PDGs and facilitates the security management by decomposing the authentication from PDGs
2. in line with the SA3 GBA, have the advantages of separating service authentication with service data tunnel traffics interaction.
3. enables the control of service applicator source: keep the network configuration confidential in reasonable extent

By combining of tunnel establishment in RGW, the first advantage can be enhanced to prevent UE contact the PDGs before it is authorized, but this need develop broker support for the current tunnel protocols, it's advantage need to be evaluated with the additional cost introduced by supporting of tunnel establishment broker functionality.

(2) Guidance about the tunnel broker protocol is necessary if in scope of SA3;

(3) SA3 encourage separating at least service authentication authorization from PDG to achieve the security advantage of R-GW base architecture, and keep the architecture in line with GBA