3GPP TSG_CN **Tdoc NP-000314**
Plenary Meeting #8, Dusseldorf, Germany
21st – 23rd June 2000.

Source: **BT**

Title: **P-TMSI Signature concept for GPRS Release 99**

Agenda item: **5.1.2**

Document for: **Approval**

---

1 Introduction

P-TMSI Signature parameter provides a system security related function in GPRS. This is an optional security feature under the control of the network. A network may allocate P-TMSI signature to a mobile station. In this case, the mobile station has to send the P-TMSI signature parameter to the network in the relevant GMM message.

For Release 99, when the "Service Request" message is sent to the network it currently carries this P-TMSI signature parameter. It has been proposed that the P-TMSI signature parameter be removed from this message (see Tdoc NP-000266).

The security benefits provided by the inclusion of the P-TMSI signature parameter has been questioned. The security requirement to not use again P-TMSI signature parameter once it has been sent once has also been questioned. There is some additional signalling between the mobile and the network to re-allocate a new value of the P-TMSI signature.

The issue related to the removal of the P-TMSI signature parameter is a primarily a UMTS system security issue and it appears that this has not been considered by TSG S3 who have the overall responsibility for security matters.

2 Proposal

It is proposed that TSG S3 review from a system security viewpoint the impact of the removal of the P-TMSI Signature from the "Service Request" message defined for Release 99 as proposed in tdoc NP-000266 and provide general recommendations on the use of P-TMSI signature concept for Release 99. TSG S3 should take into consideration documents presented at TSG N1 meeting highlighting potential security problems resulting from the removal of the P-TMSI Signature, see attached Tdocs TSG N1-000683 and TSG N1-000790.

It is requested that TSG S3 completes this task at their next meeting (31st July – 3rd August 2000) and liase their conclusions in time for the TSG N1 meeting (14th – 18th August 2000). TSG N1 should prepare CRs to TS 24.008 inline with the S3 recommendations.

Agenda Item: 6.3 Tdoc N1-000683

WI / Topic: GSM/UMTS inerworking

Source: Fujitsu

Title: Necessity of P-TMSI signature in SERVICE REQUEST

Effected Specifications / Releases: 24.008, 23.060 / R99, R00

Document for: Discussion

Date: May 19, 2000

Abstract

This contribution clarifies the necessity of P-TMSI Signature IE in SERVICE REQUEST message.

1. Introduction.

The P-TMSI signature was deleted from SERVICE REQUEST in 23.060 following the discussion in S2. The main reason, which I understood, was explained was as follows;

- SERVICE REQUEST itself does not need to be authenticated since established signalling connection is protected by integrity protection so that malicious user can not take over the signalling connection.
- P-TMSI signature once sent through not secure radio interface shall be re-assigned using P-TMSI reallocation procedure which spend radio resource.
- Therefore, the P-TMSI signature in Service Request should be deleted to avoid unnecessary waste of radio resource.

This contribution shows the case that the SERVICE REQUEST shall be authenticated and proposes to keep the P-TMSI signature IE in SERVICE REQUEST in 24.008.

2. Service Request needs to be authenticated

It is true that malicious user can not take over a service of valid user since the connection is protected by ciphering and integrity protection. Considering the fact the malicious user can not get any actual benefit from his illegal attempt. There are, however, some cases that the valid user is disturbed by the malicious attempt. An example is shown below.

[Case study]

There is a case that a SERVICE REQUEST is sent to a SGSN creating new Iu connection, while there has been an existing Iu connection for the user. Note that such case is not an irregular case, but it happens rather normally as explained below;

> *After a radio link failure, RNC keeps RRC connection for a while waiting for re-establishment. The re-establishment is optional to MS so that an MS may initiate RRC connection establishment procedure instead of re-establishment procedure. In this case, Iu connection is duplicated and such (temporary) duplication shall be accepted by the SGSN. (See Figure 1)*
>
> *The SGSN shall verify the validity of the request creating new Iu, and release the old Iu connection if the new request is turned out to be valid.*

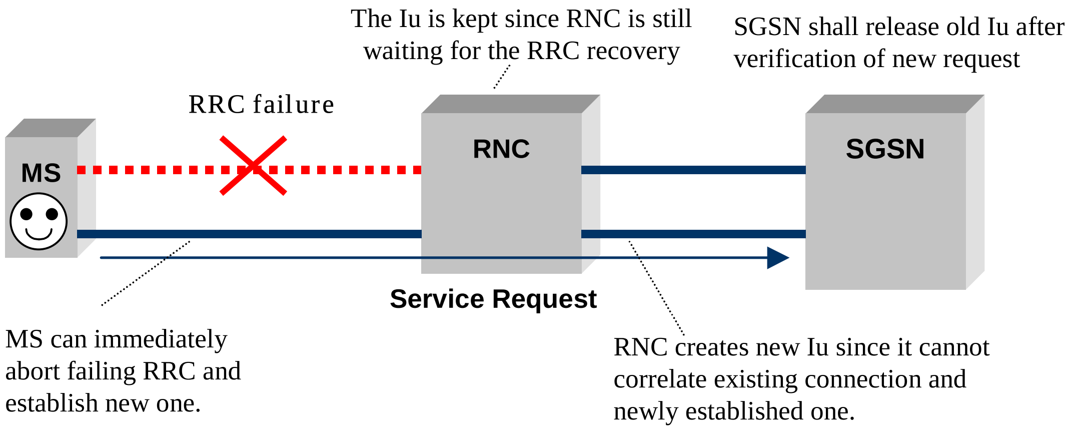
The Iu is kept since RNC is still waiting for the RRC recovery
SGSN shall release old Iu after verification of new request
RRC failure
MS
RNC
SGSN
Service Request
MS can immediately abort failing RRC and establish new one.
RNC creates new Iu since it cannot correlate existing connection and newly established one.

Figure 1 Duplicated Iu establishment from valid user

A SGSN receives SERVICE REQUEST from a malicious user associated with an identification of valid user who has an activated PDP context. The SERVICE REQUEST is sent to the SGSN creating new Iu connection since RNC cannot tell who sends this request. If the SGSN regards the request as valid without authentication, then it will release the Iu connection for the valid user since it is considered that the valid user is under the new Iu connection (and this recognition is not true). In this case, on going communication of an valid user is terminated.

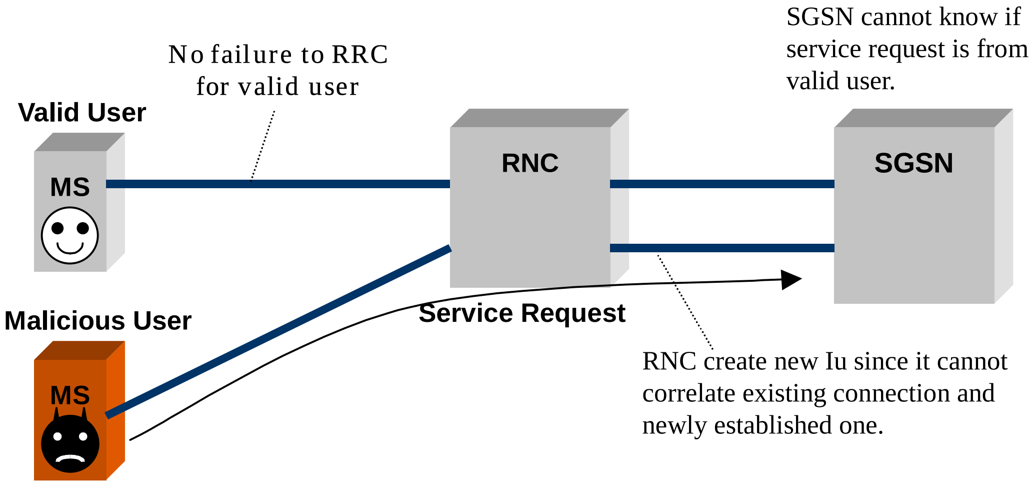
SGSN cannot know if service request is from valid user.
No failure to RRC for valid user
Valid User
MS
RNC
SGSN
Malicious User
MS
Service Request
RNC create new Iu since it cannot correlate existing connection and newly established one.

Figure 2 Duplicated Iu establishment from malicious user

Based on the above discussion, the SERVICE REQUEST shall be validated when received at least in this case. Of course, the SGSN can authenticate an MS without P-TMSI signature using normal security procedure however this discussion is not specific to SERVICE REQUEST but common to other messages (e.g. ATTACH REQUEST).

3. Authentication method

Previous section shows that SERVICE REQUEST needs to be authenticated. This section discusses how it to be done.

Requirements for SERVICE REQUEST are considered as follows;

- Done quickly to prevent the delay of service provisioning
- Not to spend to much network resource (e.g. radio resource, network signalling resource)

There was a concern that SERVICE REQUEST with P-TMSI signature spends radio resource for reallocation of new P-TMSI signature. As discussed in previous section, SERVICE REQUEST needs to be authenticated. For the purpose of it, it has to use either normal authentication (i.e., challenge & response scheme) or P-TMSI signature verification scheme.

Both schemes are evaluated below;

Authentication Speed:

Challenge & response scheme needs 1 round trip air interface signalling. And it may also be necessary to contact to HLR to get new authentication vector. All of these should be done to verify the user.

Contrary to above, P-TMSI signature scheme is finished just receiving the SERVICE REQUEST. This means it provides very quick verification. P-TMSI signature re-allocation is necessary but it is a stand-alone procedure and can be executed in parallel to other procedure so that it will not cause the delay of service provisioning.

SERVICE REQUSET needs very quick handling since it is used, for example, to re-establish radio access bearer for pending user packet to send. Considering this fact, P-TMSI signature scheme is much better than challenge & response scheme.

Network Resource Efficiency:

As discussed above, challenge & response scheme needs 1 round trip signalling at air interface and possibly requires MAP signalling also.

P-TMSI signature requires P-TMSI signature re-allocation that needs 1 round trip air interface signalling.

From this evaluation point, P-TMSI signature scheme is almost equal to or little bit better than challenge & response scheme.

Above evaluation does not cover all the aspect of security procedure, but at least we can say that there can be cases that P-TMSI signature scheme is better than challenge & response scheme.

This study concludes that there are some beneficial cases if SERVICE REQUEST keeps P-TMSI signature.

3. Conclusion

This contribution shows the case that SERVICE REQUEST needs authentication and P-TMSI signature should be able to be used for a one of possible methods of authentication.

It is proposed to keep P-TMSI Signature in SERVICE REQUEST in 24.008, and also proposed to send a liaison statement to S2 advising to recover the information element in 23.060.

Agenda Item: 6.3 Tdoc N1-000790

WI / Topic: GSM/UMTS interworking

Source: Lucent Technologies

Title: P-TMSI signature in SERVICE REQUEST

Effected Specifications / Releases: 24.008, 23.060 / R99, R00

Document for: Discussion

Date: May 2000

Abstract

This contribution clarifies the necessity of P-TMSI Signature IE in SERVICE REQUEST message.

1. Introduction.

The P-TMSI signature was deleted from SERVICE REQUEST in 23.060 following the discussion in S2. This contribution shows the case that the SERVICE REQUEST shall be authenticated and proposes to keep the P-TMSI signature IE in SERVICE REQUEST in 24.008.

2. Service Request needs to be authenticated

It is true that malicious user can not take over a service of valid user since the connection is protected by ciphering and integrity protection. Considering the fact the malicious user can not get any actual benefit from his illegal attempt. There are, however, some cases that the valid user is disturbed by the malicious attempt. An example was shown in Tdoc N1-000683. This contribution considers another case.

[Case study]

Service Request is sent in response to a paging request. The UE is paged using P-TMSI. A malicious user can monitor the paging channel, pick up the P-TMSI from the paging request messages (Figure 1).

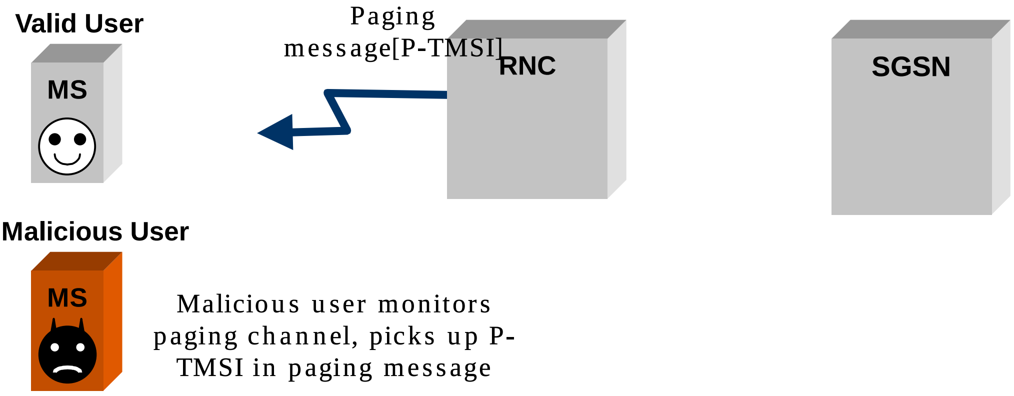
Valid User
MS
Paging message[P-TMSI]
RNC
SGSN
Malicious User
MS
Malicious user monitors paging channel, picks up P-TMSI in paging message

Figure 3 Malicious user picks up P-TMSI in paging messages

It then send a Service Request identifying itself with the P-TMSI it picked up from the paging message (Figure 2). The SGSN will then receive two Service Request messages (assuming that the real user also responded to the paging request) and the SGSN cannot resolve which service request is from the real user without P-TMSI signature.

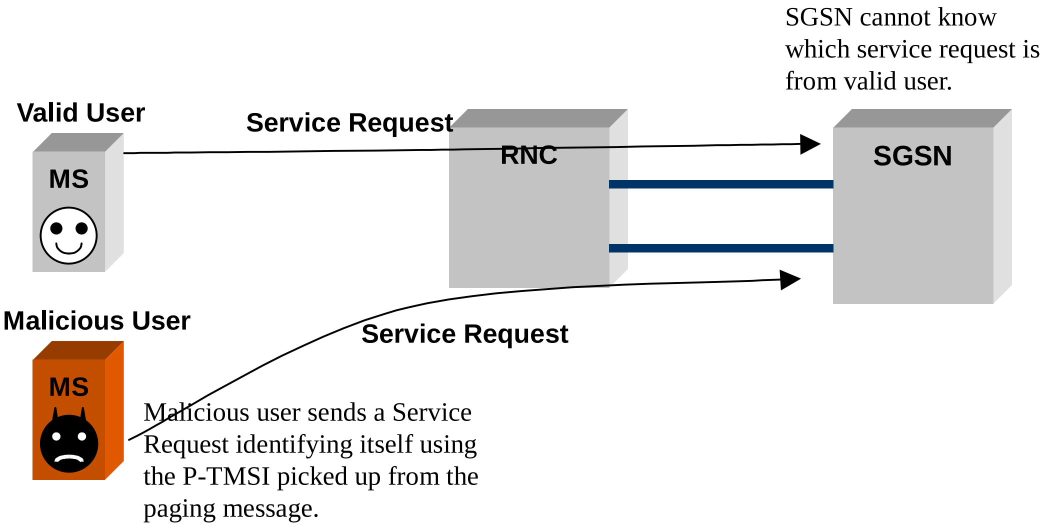
SGSN cannot know which service request is from valid user.
Valid User
Service Request
RNC
SGSN
MS
Malicious User
MS
Service Request
Malicious user sends a Service Request identifying itself using the P-TMSI picked up from the paging message.

Figure 4 Duplicated Serive Request and Iu establishment from malicious user

This can result in losing the call to the real user. Authenticating both Service Request is a possible option, but authenticating a UE over two different Iu links simultaneously will be required. Use of P-TMSI signature in service request will avoid this situation. Note that the two users could in different RNCs.

A malicious user can continue to do this without being tracked and can cause considerable disruption of service to real users.

Note here that integrity check and encryption does not help.

This study concludes that there are some beneficial cases if SERVICE REQUEST keeps P-TMSI signature.

3. Conclusion

This contribution shows the case that SERVICE REQUEST needs authentication and P-TMSI signature should be able to be used for a one of possible methods of authentication.

It is proposed to keep P-TMSI Signature in SERVICE REQUEST in 24.008.

3GPP TSG-CN-WG1, Meeting #12
22-26 May, 2000
Oahu/Hawaii, USA

Tdoc N1-000683

Agenda Item: 6.3

WI / Topic: GSM/UMTS inerworking

Source: Fujitsu

Title: Necessity of P-TMSI signature in SERVICE REQUEST

Effected Specifications / Releases: 24.008, 23.060 / R99, R00

Document for: Discussion

Date: May 19, 2000

Abstract

This contribution clarifies the necessity of P-TMSI Signature IE in SERVICE REQUEST message.

1. Introduction.

The P-TMSI signature was deleted from SERVICE REQUEST in 23.060 following the discussion in S2. The main reason, which I understood, was explained was as follows;

- SERVICE REQUEST itself does not need to be authenticated since established signalling connection is protected by integrity protection so that malicious user can not take over the signalling connection.
- P-TMSI signature once sent through not secure radio interface shall be re-assigned using P-TMSI reallocation procedure which spend radio resource.
- Therefore, the P-TMSI signature in Service Request should be deleted to avoid unnecessary waste of radio resource.

This contribution shows the case that the SERVICE REQUEST shall be authenticated and proposes to keep the P-TMSI signature IE in SERVICE REQUEST in 24.008.

2. Service Request needs to be authenticated

It is true that malicious user can not take over a service of valid user since the connection is protected by ciphering and integrity protection. Considering the fact the malicious user can not get any actual benefit from his illegal attempt. There are, however, some cases that the valid user is disturbed by the malicious attempt. An example is shown below.

[Case study]

There is a case that a SERVICE REQUEST is sent to a SGSN creating new Iu connection, while there has been an existing Iu connection for the user. Note that such case is not an irregular case, but it happens rather normally as explained below;

> *After a radio link failure, RNC keeps RRC connection for a while waiting for re-establishment. The re-establishment is optional to MS so that an MS may initiate RRC connection establishment*

procedure instead of re-establishment procedure. In this case, Iu connection is duplicated and such (temporary) duplication shall be accepted by the SGSN. (See Figure 1)

The SGSN shall verify the validity of the request creating new Iu, and release the old Iu connection if the new request is turned out to be valid.

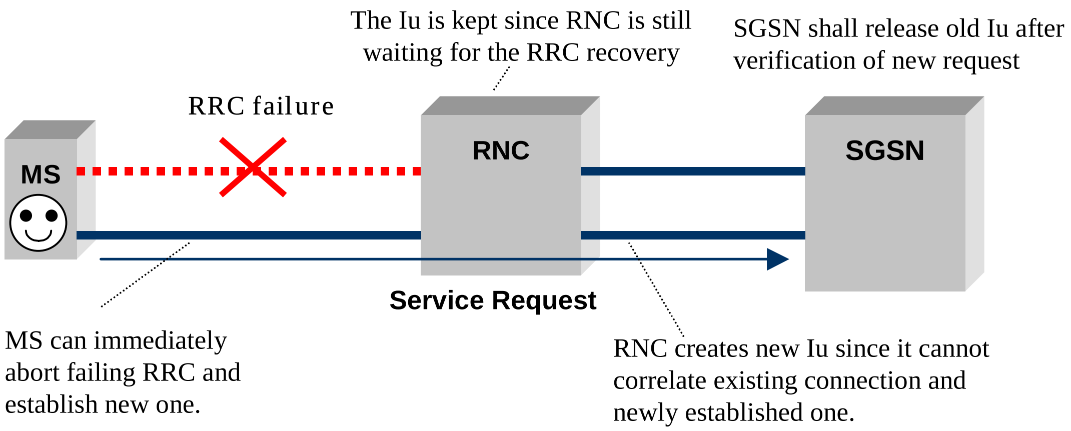
The Iu is kept since RNC is still waiting for the RRC recovery
SGSN shall release old Iu after verification of new request
RRC failure
MS
RNC
SGSN
Service Request
MS can immediately abort failing RRC and establish new one.
RNC creates new Iu since it cannot correlate existing connection and newly established one.

Figure 1 Duplicated Iu establishment from valid user

A SGSN receives SERVICE REQUEST from a malicious user associated with an identification of valid user who has an activated PDP context. The SERVICE REQUEST is sent to the SGSN creating new Iu connection since RNC cannot tell who sends this request. If the SGSN regards the request as valid without authentication, then it will release the Iu connection for the valid user since it is considered that the valid user is under the new Iu connection (and this recognition is not true). In this case, on going communication of an valid user is terminated.

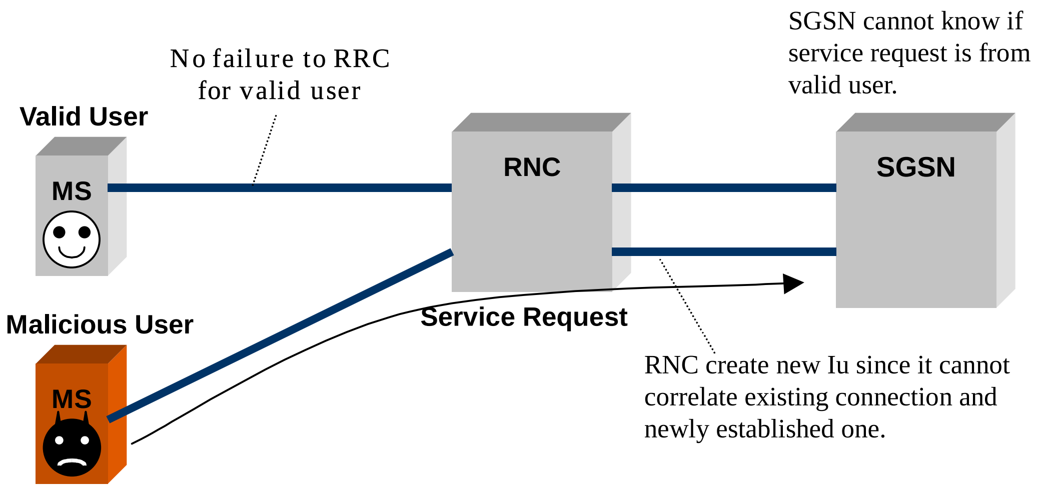
SGSN cannot know if service request is from valid user.
No failure to RRC for valid user
Valid User
MS
RNC
SGSN
Malicious User
MS
Service Request
RNC create new Iu since it cannot correlate existing connection and newly established one.

Figure 2 Duplicated Iu establishment from malicious user

Based on the above discussion, the SERVICE REQUEST shall be validated when received at least in this case. Of course, the SGSN can authenticate an MS without P-TMSI signature using normal security procedure however this discussion is not specific to SERVICE REQUEST but common to other messages (e.g. ATTACH REQUEST).

3. Authentication method

Previous section shows that SERVICE REQUEST needs to be authenticated. This section discusses how it to be done.

Requirements for SERVICE REQUEST are considered as follows;

- Done quickly to prevent the delay of service provisioning
- Not to spend to much network resource (e.g. radio resource, network signalling resource)

There was a concern that SERVICE REQUEST with P-TMSI signature spends radio resource for reallocation of new P-TMSI signature. As discussed in previous section, SERVICE REQUEST needs to be authenticated. For the purpose of it, it has to use either normal authentication (i.e., challenge & response scheme) or P-TMSI signature verification scheme.

Both schemes are evaluated below;

Authentication Speed:

Challenge & response scheme needs 1 round trip air interface signalling. And it may also be necessary to contact to HLR to get new authentication vector. All of these should be done to verify the user.

Contrary to above, P-TMSI signature scheme is finished just receiving the SERVICE REQUEST. This means it provides very quick verification. P-TMSI signature re-allocation is necessary but it is a stand-alone procedure and can be executed in parallel to other procedure so that it will not cause the delay of service provisioning.

SERVICE REQUSET needs very quick handling since it is used, for example, to re-establish radio access bearer for pending user packet to send. Considering this fact, P-TMSI signature scheme is much better than challenge & response scheme.

Network Resource Efficiency:

As discussed above, challenge & response scheme needs 1 round trip signalling at air interface and possibly requires MAP signalling also.

P-TMSI signature requires P-TMSI signature re-allocation that needs 1 round trip air interface signalling.

From this evaluation point, P-TMSI signature scheme is almost equal to or little bit better than challenge & response scheme.

Above evaluation does not cover all the aspect of security procedure, but at least we can say that there can be cases that P-TMSI signature scheme is better than challenge & response scheme.

This study concludes that there are some beneficial cases if SERVICE REQUEST keeps P-TMSI signature.

3. Conclusion

This contribution shows the case that SERVICE REQUEST needs authentication and P-TMSI signature should be able to be used for a one of possible methods of authentication.

It is proposed to keep P-TMSI Signature in SERVICE REQUEST in 24.008, and also proposed to send a liaison statement to S2 advising to recover the information element in 23.060.

3GPP TSG-CN-WG1, Meeting #12
22-26 May, 2000
Oahu/Hawaii, USA

Tdoc N1-000790

Agenda Item: 6.3

WI / Topic: GSM/UMTS interworking

Source: Lucent Technologies

Title: P-TMSI signature in SERVICE REQUEST

Effected Specifications / Releases: 24.008, 23.060 / R99, R00

Document for: Discussion

Date: May 2000

Abstract

This contribution clarifies the necessity of P-TMSI Signature IE in SERVICE REQUEST message.

1. Introduction.

The P-TMSI signature was deleted from SERVICE REQUEST in 23.060 following the discussion in S2. This contribution shows the case that the SERVICE REQUEST shall be authenticated and proposes to keep the P-TMSI signature IE in SERVICE REQUEST in 24.008.

2. Service Request needs to be authenticated

It is true that malicious user can not take over a service of valid user since the connection is protected by ciphering and integrity protection. Considering the fact the malicious user can not get any actual benefit from his illegal attempt. There are, however, some cases that the valid user is disturbed by the malicious attempt. An example was shown in Tdoc N1-000683. This contribution considers another case.

[Case study]

Service Request is sent in response to a paging request. The UE is paged using P-TMSI. A malicious user can monitor the paging channel, pick up the P-TMSI from the paging request messages (Figure 1).

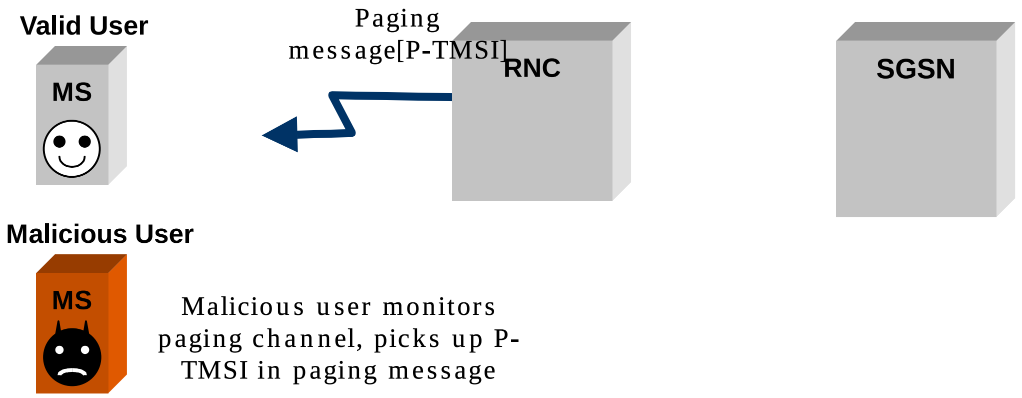
Valid User
MS
Paging message[P-TMSI]
RNC
SGSN
Malicious User
MS
Malicious user monitors paging channel, picks up P-TMSI in paging message

Figure 1 Malicious user picks up P-TMSI in paging messages

It then send a Service Request identifying itself with the P-TMSI it picked up from the paging message (Figure 2). The SGSN will then receive two Service Request messages (assuming that the real user also responded to the paging request) and the SGSN cannot resolve which service request is from the real user without P-TMSI signature.

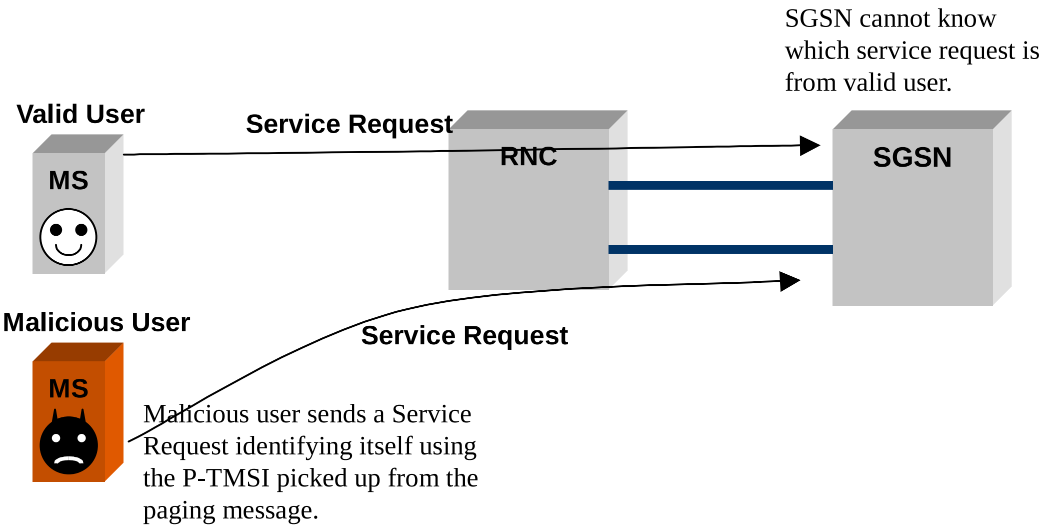
SGSN cannot know which service request is from valid user.
Valid User
Service Request
RNC
SGSN
MS
Malicious User
Service Request
MS
Malicious user sends a Service Request identifying itself using the P-TMSI picked up from the paging message.

Figure 2 Duplicated Serive Request and Iu establishment from malicious user

This can result in losing the call to the real user. Authenticating both Service Request is a possible option, but authenticating a UE over two different Iu links simultaneously will be required. Use of P-TMSI signature in service request will avoid this situation. Note that the two users could in different RNCs.

A malicious user can continue to do this without being tracked and can cause considerable disruption of service to real users.

Note here that integrity check and encryption does not help.

This study concludes that there are some beneficial cases if SERVICE REQUEST keeps P-TMSI signature.

3. Conclusion

This contribution shows the case that SERVICE REQUEST needs authentication and P-TMSI signature should be able to be used for a one of possible methods of authentication.

It is proposed to keep P-TMSI Signature in SERVICE REQUEST in 24.008.