3GPP TSG SA WG3 Security — S3#25 **S3-020537**
8 - 11 October 2002
Munich, Germany

Source: Lucent Technologies

Title: Group release security mechanism

Document for: Discussion and Approval

Agenda item: 6.7

Introduction

In the proposal for group release as presented to SA3 in [1] an extra security requirement was suggested. It was postulated that it would be necessary to add protection to existing release 99 messages in the case of adding a group reset function to prevent a single message releasing multiple UEs erroneously.

SA3 identified in [2] to RAN2 that they did not consider not authenticating this group release function, as RAN2 already highlighted that it was insecure. It should be noted that this is also the current situation with the messages to be affected by this proposed mechanism.

This contribution intends to highlight the existing security aspects of supporting connection release, to assist SA3 on their assessment of the perceived increased security risk.

Discussion

Firstly it should be clarified that the group release proposal is intended to send UEs in cell_FACH and cell_PCH states to idle, whereas any UEs in cell_DCH states would detect the RNC reset and act autonomously to reselect a suitable cell. This proposed group release functionality, is in response to an RNC being reset, whereupon some UEs (i.e. those in radio connection states cell_FACH & cell_PCH) may remain unreachable for some time (due to the loss of their temporary UTRAN ids). It is anticipated that the total number of these unreachable UEs under any one RNC would be relatively low. To this extent with this general group release mechanism this smaller number of UEs would then move to idle mode on successful reception of the message. Then they would reselect a suitable cell, and so subsequently re-establish a new temporary UTRAN identity.

It should be clarified that currently, the existing RRC connection release message sent on the CCCH, and paging type 1 messages are not protected (see Annex A and TS33.102 section 6.5.1). It is these messages that the group release indicator and any associated 'authentication release key' would be added to.

That is to say currently a rogue transmitter can send the release message to a UE causing it to release from the network and return to idle mode. This is the current situation without the addition of this group indicator, and will remain even after the addition of the group release mechanism as proposed in [3].

It is acknowledged however, that in order for UEs to correctly receive this message, the identity included in the message must match the receiving UE's identity. Clearly to match the identity of a single UE (U-RNTI) would require a match with a larger number of bits (32 bits) when compared to the smaller group identity. However, it should be noted that this group identity could extend from 1-31 bits (with the current definition of the URNTI mask being 1-31 bits in length [3]). This reduced identity would mean a match is probably more likely for more mobiles, within a single message. Although clearly using one message to release several UEs has some implicit increase as a security risk, particularly when compared to sending multiple messages to achieve the release of multiple UEs, in real terms the ability to perform such an action in a real network could be considered to be similar.

Also, currently if denial of service is the intended result of a rogue transmitter, there are several existing mechanisms that could be considered more effective, such as the transmission of bogus system information for example.

The inclusion of such an additional security mechanism would impact significantly more messages, in order to support the indication of the proposed indicia during the existing mobility procedures. As the indication using this scheme may utilise a varying number of bits to identify a group of UEs, it has a similar (up to within 1 bit) address length to the existing signalling mechanism for one UE, which is currently unprotected.

Summary

It is recommended that SA3 study the need for this additional authentication mechanism, in particular with reference to the existing mechanisms affected by the proposal in [3].

The result of this study should be communicated to RAN2 so that they may fully understand the need for additional impact of any extra security requirements, associated with this possible denial of service, and implement all necessary signalling support for this proposal.

References

[1] R2-020797	LS on Group release security solution, RAN2
[2] R2-021552	(S3-020287, to TSG-RAN WG2) Response to LS (R2-020797) on Group release security solution, TSG-SA WG3
[3] R2-020734	Actions at RNC reset, Ericsson
[4] TS 25.331	RRC protocol Specification
[5] R2-022580	Recovery of UEs upon RNC reset, Lucent Technologies

Annex A – TS25.331[4] RRC Connection Release Message

10.2.37 RRC CONNECTION RELEASE

This message is sent by UTRAN to release the RRC connection. The message also releases the signalling connection and all radio bearers between the UE and UTRAN.

RLC-SAP: UM

Logical channel: CCCH or DCCH

Direction: UTRAN→UE

Information Element/Group name	Need	Multi	Type and reference	Semantics description
Message Type	MP		Message Type	
UE information elements				
U-RNTI	CV-*CCCH*		U-RNTI 10.3.3.47	
RRC transaction identifier	MP		RRC transaction identifier 10.3.3.36	
Integrity check info	CV-*DCCH*		Integrity check info 10.3.3.16	Integrity check info is included if integrity protection is applied
N308	CH-*Cell_DCH*		Integer(1..8)	
Release cause	MP		Release cause 10.3.3.32	
Other information elements				
Rplmn information	OP		Rplmn information 10.3.8.15	

Condition	Explanation
CCCH	This IE is mandatory present when CCCH is used and not needed otherwise.
DCCH	This IE is mandatory present when DCCH is used and not needed otherwise.
Cell_DCH	This IE is mandatory present when UE is in CELL_DCH state and not needed otherwise.

10.3.3.23 Paging record

Information Element/Group name	Need	Multi	Type and reference	Semantics description
CHOICE *Used paging identity*	MP			
>CN identity				
>>Paging cause	MP		Paging cause	

Information Element/Group name	Need	Multi	Type and reference	Semantics description
			10.3.3.22	
>>CN domain identity	MP		CN domain identity 10.3.1.1	
>>CHOICE *UE Identity*	MP			Three spare values are needed.
>>>IMSI (GSM-MAP)			IMSI (GSM-MAP) 10.3.1.5	
>>>TMSI (GSM-MAP)			TMSI (GSM-MAP) 10.3.1.17	
>>>P-TMSI (GSM-MAP)			P-TMSI (GSM-MAP) 10.3.1.13	
>>>IMSI (DS-41)			TIA/EIA/IS-2000-4	
>>>TMSI (DS-41)			TIA/EIA/IS-2000-4	
>UTRAN identity				
>>U-RNTI	MP		U-RNTI 10.3.3.47	
>>CN originated page to connected mode UE	OP			
>>>Paging cause	MP		Paging cause 10.3.3.22	
>>>CN domain identity	MP		CN domain identity 10.3.1.1	
>>>Paging record type identifier	MP		Paging record type identifier 10.3.1.10	

Condition	Explanation
CHOICE *Used paging identity*	**Condition under which the given *used paging identity* is chosen**
CN identity	For CN originating pages (for idle mode UEs)
UTRAN identity	For UTRAN originating pages (for connected mode UEs)

Annex B - Extracts from RAN2 documents

R2-020734 [3] Actions at RNC reset –

Introducing possibilities to release a group of UEs is a challenge from a security point of view. If the release message was sent without ciphering, integrity protection or authentication, a non-friendly intruder could efficiently release all radio connections in a cell.

An advantage would therefore if there was a more secure way of releasing a group of UEs. Ciphering and integrity protection is normally established per-UE basis with individual keys. Using “group keys” together with ciphering or integrity protection might be possible, but there are much simpler ways to use a group key but still keeping a sufficient security level.

R2-022580 [5] Recovery of UEs upon RNC reset –

This is addition to the open issues identified by [*3*] & [*4*] with regard to the security. We do not think authentication on group release at reset is necessary.

UEs affected by RNC reset will have to release RRC connection anyway. UE air interface security will be regained after UE’s next connection to the network. Therefore, we propose not to perform authentication on group release, and hence adopt NEC’s proposal (if denial of service is a real concern, integrity protection may need to be considered for RRC CONNECTION RELEASE on CCCH at first place in general);

[*3*] R2-021866 (SAGE 02 06, copy TSG-RAN WG2) LS on the Use of Kasumi-based functions for Group release security solution SAGE

[*4*] R2-021552 (S3-020287, to TSG-RAN WG2) Response to LS (R2-020797) on Group release security solution TSG-SA WG3