3GPP TSG SA WG3 Security — S3#26 **S3-020649**
19- 22 November 2002
Oxford, UK

Source: Lucent Technologies

Title: Group release security mechanism

Document for: Discussion and Approval

Agenda item:

Introduction

At the Munich meeting it was decided to have an email to discuss the need for a security solution for the group release mechanism currently being proposed in RAN2. This contribution attempts to summarise the various postions in the hope that SA3 can make a final decision that can be sent to RAN2.

Broadly speaking the discussion covered the following areas.

Threat impacts

Jamming

Common channel protection

Other solutions

Discussion

Threat impacts

Brad Owen (Lucent Technologies)

Since any attack using the connection release mechanism would be through the Node B - the attack could only effect a small fraction (tens) of the UEs served by an RNC. The efficiency benefits provided by the group release mechanism are aimed at the RNC level (a single RNC sends out the group release message to multiple Node B's).

A group release will only be picked up by "idle" mobiles and the "temporary" release followed by a subsequent re-connection to a real network causes almost no disruption in most cases (save the case where the UE happens to have outgoing data immediately after the "attack"). Again when are the consequences of an attack determined to be severe enough to warrant protection?

It is also really very complicated to get to a state where the group release mechanism can be used for a denial of service attack. Either a rogue needs to substitute itself with the current cell - that would require to use the same cell id and other RF parameters. Or the attacker mimics a NodeB upon which the UE camps. Are these really practical scenarios?

Krister Borman (Ericsson)

There are a number of possible attacks at different interfaces that could be mounted should the Group Release message be left unprotected. As already pointed out by Brad an RNC can serve in order of 100 Node-Bs indicating that if an attacker can achieve for him a succesful attack it can be very costly for an operator (lost revenues).

It seems that the worst case scenario to consider is if the attacker can launch a 'false RNC' attack. It is difficult to estimate how probable such an attack really is however according to TS33.120 the following text can be found:

Conclusion:

SA3 still needs to determine whether the unlikely attack scenario presented for group release versus the commercial benefit of the group release mechanism warrants protection of this mechanism.

Jamming

Brad Owen (Lucent Technologies)
…easiest way to do a DoS attack is to send jamming signals eg by blanket blocking of radio frequencies rather than going through the elaborate process of tuning in to a specific frequencies.

You don't need to transmit continuously - you only need to send a few seconds burst to throw the UEs in Cell-DCH out of sync and disconnect all ongoing voice calls for example. This is a lot more disruptive than moving a few "idle" users to RRC idle.

Also it is a lot easier to build and use a jamming transmitter and drive around the country sending bursts of RF power and these won't be easy to detect either. To build a sophisticated piece of equipment that will effectively "capture" the UEs is more difficult.

On the question of how quick the recovery is between jamming and group release - a point to note is that with jamming all calls - including voice calls will be lost and that is really bad. For group release only mobiles that are in "idle" state will need to re-initialise the connection.   Depending on the period of jamming and the resulting state the UE finds in, the recovery for both cases is to do a fresh cell re-selection and to re-establish the radio connection.   So recovery period will be similar for both attacks.

Stefan Schröder (Tmobile)
To my mind, we cannot argue that security is not needed for group release because an attacker could also set up a jamming transmitter. It is significantly easier to detect a constantly transmitting (high-power!) DoS attacker than to spot a more sophisticated one sending a very short RELEASE message every few minutes. Furthermore, I suppose a 3G network will quickly (instantly) recover from a brute jamming attack when the transmitter is stopped. Recovering from more sophisticated protocol attacks requires higher layer activities.

If I was wrong in my assumption that the UMTS system will more easily recover from a short jamming signal than from a forged group release command then I agree that we don't need any security mechanism for group release.

Marc Blommaert (Siemens)

The adding group release functionality introduces an additional DoS-possibility. This however requires to my opinion more complex equipment and handling at the attackers side than using a jammer.

Conclusion

It seems that jamming does provide an easier and more effective denial of service attack than the group release mechanism. Whether the availability of the jamming attack makes protection of the group release unnecessary is still to be determined by SA3.

Common Channel protection

Brad Owen (Lucent Technologies)
This "security hole" is an attribute of a requirement to have messages sent on the common channel (CCCH) unprotected. This allows fraudulent UTRANs to temporarily disrupt service for a UE.

Marc Blommaert (Siemens)
TS 25.331 describes the following:
"Then UTRAN transmits an RRC CONNECTION RELEASE message the downlink DCCH
should be used, if available. If the downlink DCCH
is not available in UTRAN and the UE is in CELL_FACH state, the downlink
CCCH may be used."

This means that in most cases the RRC connection release will be protected !
It is hard to estimate how many UE's shall be released using CCCH, after RNC
reset (many of the connected UE's will have adapted their connection state
before the RNC is up again due to expired timers).

What threat should be solved by protecting a single release on CCCH ?
The mobile is addressed by RNTI when releasing a connection on CCCH. It will
not be easy by an attacker to obtain the RNTI linkage to IMSI so the single
release may not be used to deliverate release a particular mobiles RRC
connection. This again means that using a jammer will again be more
effective as DoS.

Stefan Schröder (Tmobile)
…the missing protection is related to the common channel, which was explicitly excluded from current protection in TS 33.102. We have no protection at all for the CCCH. If this channel is used to transmit potentially damaging messages, this might be a hole we should generally fix. We could consider introducing a protection for the common channel as proposed for the group release - but it might be too late to be really effective because we have to be backward compatible. It is one thing to accept an existing hole but a completely different story to make it even bigger by allowing more efficient misuse (group release).

The fact that most RELEASEs will be protected does not prevent misuse of the unprotected mechanism. To me the question is: If the target UE receives the RELEASE command unprotected, will it check if it should have received it protected and consequently discard it? I don't think so.

Krister Boman(Ericsson)
Furthermore SA3 should investigate if it is required and feasible to protect those CCCH messages that are currently not offered any security. Ericsson suggests that such an investigation should be kept as a seperate issue from the protection of Group Release Messages.

Conclusion

The lack of protection for the common channel is acknowledged but should probably considered as a separate issue to the need to protect the group release mechanism.

Other solutions

Marc Blommaert (Siemens)

After an RNC reset certain UE's will detect immediatly (I.e. timers expiring soon) and recover from the RNC reset while others will only do it after a while (depending on their state - see TS 25.331). The main reason for the group release feature is the 'possibility' that the RNC has lost information (after an RNC reset) which it needs (in certain states only) to release the hanging RRC connection for UE's immediatly.
Would a solution that only affects the RNC-implementation not be adequate ? If only the data needed to properly release the hanging connection be stored on recovery-resistant media, then it would avoid UE-impacts (from Rel-5 on). Such a solution could release 95% of the hanging connections. From Brads mail, i would derive that the amount of problematic UE's is not so big (so not leading to big permanent storage requirements).

Conclusion

There seems to be the possibility of other inherently secure solutions for group release but this should be for the RAN groups to decide.

Summary

It is recommended that SA3 study arguments put forward for and against the need for protection for the group release mechanism.

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.