**3GPP TSG SA WG3 Security — S3#14** **S3-000467**

**2-4 August, 2000**

**Oslo, Norway**

| | |
|---|---|
| **Source:** | **Vodafone** |
| **Title:** | **Review of the integrity protection procedure** |
| **Document for:** | **Discussion and decision** |
| **Agenda Item:** | **9.2** |

## 1 Introduction

There is some concern that the transmission and processing overhead caused by the integrity protection mechanism is too high. The document attempts to provide information which may be used to clarify which RRC messages should be protected.

## 2 Requirements for integrity protection

Integrity protection has been added to prevent the insertion, modification, deletion and replay of messages exchanged between the mobile equipment and the radio network controller. The reasons for supplementing the existing ciphering mechanism with a dedicated integrity mechanism in 3G are summarised below:

- For various reasons 3G networks must be able to instruct the mobile to use an unciphered connections. Thus, an active man-in-the-middle attacker could potentially compromise user traffic confidentiality by masquerading as a network to establish an unciphered connection towards the user. Since integrity protection can be made mandatory, this attack can be prevented as the user can always verify the instruction from the network to establish an unciphered connection[1].

- The ability to integrity protect ciphering algorithm negotiation messages provides protection against roll-back attacks where an active attacker forces the use of an old ciphering algorithm which may, for instance, allow user traffic confidentiality to be compromised. This feature only becomes of interest when multiple algorithms must be supported in the system. In the first release of the 3GPP standards only one ciphering algorithm is available and this must be supported by all terminals. However, it was considered desirable to design a future-proof system which allowed new algorithms to be deployed effectively, efficiently and securely.

- Although ciphering of signalling traffic provides some integrity protection and the ciphering of user traffic severely limits the usefulness of any successful compromise of signalling message integrity, the application of a dedicated integrity protection mechanism with its own integrity key significantly increases the security margin of the system. This is seen as an important enhancement which will ensure that 3G offers adequate protection against increasingly sophisticated active attackers.

- Although the application of user traffic ciphering is highly recommended not just for confidentiality but also for authentication and integrity purposes, there may be some exceptional cases where it is not applied. In these cases, integrity protection of signalling messages significantly increases the level of resistance against relatively unsophisticated attacks which would have been effective had integrity protection not been provided.

[1] In GSM the instruction from the network to establish an unciphered connection is not integrity protected. However, GSM terminals are provided with a cipher indicator which allows users to check whether or not ciphering is applied and therefore protect themselves against this attack.

# 3 RRC messages which cannot be protected

The following messages are sent only on broadcast channels. Therefore integrity protection can never be applied to these messages. As a result they should not contain any integrity protection related IEs (Information Elements).

PAGING TYPE 1

SYSTEM INFORMATION

The following messages are only sent before the security mode control procedure and never need to be sent after the security mode control procedure. Therefore integrity protection is never applied to these messages. As a result they should not contain any integrity protection related IEs.

RRC CONNECTION REQUEST

RRC CONNECTION SETUP

RRC CONNECTION SETUP COMPLETE

RRC CONNECTION REJECT

HANDOVER TO UTRAN COMPLETE*

* This message cannot be integrity protected in R99. However, in future releases when integrity protection is applied in GERAN, it may be possible to protect this message as part of an ongoing integrity protected signalling connection which exists during handover from GERAN to UTRAN.

# 4 Review of all other RRC messages

The security category of all other messages should be defined to help determine whether integrity protection should be applied if the message is sent after a successful security mode procedure. The results can be used together with the size and frequency of the message to determine whether the message should be protected or not. Messages which are too small and/or too frequent may result in an unacceptable increase in the transmission overhead or an unacceptable processing overhead.

Messages are split into categories and for each category the level of desirability of integrity protection is determined. For messages that can always be integrity protected the status of the integrity protection related IEs should be “mandatory (M)”. For all other messages the status of the integrity protection IEs should be “conditional based on history (CH)” as the IEs are only present if the security mode procedure has been successful.

### *4.1 Security mode*

SECURITY MODE COMMAND - essential (M)

SECURITY MODE COMPLETE – essential (M)

SECURITY MODE FAILURE – essential (CH)

Security mode messages are used to negotiate the ciphering and integrity algorithm and to establish a secure connection. Integrity protection is therefore considered to be essential. SECURITY MODE COMMAND and SECURITY MODE COMPLETE can always be protected (status = M). If a security mode had not be established prior to the security mode procedure then it will not be possible to apply integrity protection to the SECURITY MODE FAILURE message. However, if the security mode procedure is used to change an existing security mode then it will be possible to protect the message and integrity protection (status = CH). A spoofed SECURITY MODE FAILURE could prevent encryption being switched on or upgraded to a stronger mode mid-RRC connection.

### *4.2 Counter check for local authentication*

COUNTER CHECK – essential (M)

COUNTER CHECK RESPONSE – essential (M)

These messages allow the RNC to check that the amount of data sent in both directions during the RRC connection is the same at the UTRAN and at the UE. This is used to prevent an intruder inserting data, especially when ciphering is not applied to radio bearers. COUNTER CHECK and COUNTER CHECK RESPONSE are only of use when integrity protection has been established and the application of integrity protection in that case is considered to be essential. COUNTER CHECK and COUNTER CHECK RESPONSE are therefore always protected (status = M).

### *4.3 Routing of higher layer PDUs*

INITIAL DIRECT TRANSFER – essential (CH)

DOWNLINK DIRECT TRANSFER – essential (CH)

UPLINK DIRECT TRANSFER – essential (CH)

These messages are used to carry higher layer signalling. When these messages are sent after a successful security mode procedure, the application of integrity protection is considered to be essential (status = CH) (at least from the RRC perspective.

### *4.4 System information change*

SYSTEM INFORMATION CHANGE INDICATION – low desirable (CH)

This message is used to indicate new system information or to indicate that the UE should check the broadcast system information for updates. When this message is sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

### *4.5 Transport format combination control*

TRANSPORT FORMAT COMBINATION CONTROL

TRANSPORT FORMAT COMBINATION CONTROL FAILURE[2]

This message is used among other things to control AMR coding in the user plane. When this message is sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH). These messages can in some cases be very small/frequent.

### *4.6 TDD specific messages*

PHYSICAL SHARED CHANNEL ALLOCATION - low desirable (CH)

PUSCH CAPACITY REQUEST - low desirable (CH)

UPLINK PHYSICAL CHANNEL CONTROL - low desirable (CH)

These messages are used among other things for power control estimation and control of timing advance in the TDD mode. . When these messages are sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

### *4.7 Mobility management*

#### 4.7.1 RNTI reallocation

RNTI REALLOCATION - low desirable (CH)

RNTI REALLOCATION COMPLETE - low desirable (CH)

RNTI REALLOCATION FAILURE - low desirable (CH)

When moving to new RNC, a new CRNTI is allocated to the UE. CRNTI is unique per UE per RNC. The CRNTI concatenated with the RNC_id form the URNTI which is a unique UE identifier per network. When the messages are sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

[2] The current specification needs updating since the message name in the list of unprotected messages is incorrect.

### 4.7.2 Cell update

CELL UPDATE - low desirable (CH)

CELL UPDATE CONFIRM - low desirable (CH)

When moving to a new cell, a UE may send a CELL UPDATE to the network. When the messages are sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

### 4.7.3 URA update

URA UPDATE - low desirable (CH)

URA UPDATE CONFIRM - low desirable (CH)

When moving to a new URA, a UE may send a URA UPDATE to the network. When the messages are sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

### 4.7.4 Active set update (soft handover)

ACTIVE SET UPDATE

ACTIVE SET UPDATE COMPLETE

ACTIVE SET UPDATE FAILURE

When a mobile moves to an area where its active set of cells changes, a UE may send an ACTIVE SET URA UPDATE to the network. When the messages are sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

### 4.7.5 Intersystem handover

INTER-SYSTEM HANDOVER COMMAND - high desirable (CH)

INTER-SYSTEM HANDOVER FAILURE - high desirable (CH)

When a mobile moves to an area of GSM coverage, a UE may send an INTER-SYSTEM HANDOVER COMMAND within the UTRAN as part of the intersystem handover procedure. When the messages are sent after a successful security mode procedure the application of integrity protection is considered to be high desirable (status = CH) since it would be undesirable for an active attacker to force a mobile onto GSM in order to exploit the potentially weaker security mechanisms employed in the GSM domain.

### 4.7.6 Radio resource management

DOWNLINK OUTER LOOP CONTROL - low desirable (CH)

This message is used to set the UE outer loop target for power control (block error rate). When the message is sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

### 4.7.7 Measurement control

MEASUREMENT CONTROL - low desirable (CH)

MEASUREMENT CONTROL FAILURE - low desirable (CH)

MEASUREMENT REPORT - low desirable (CH)

These messages are used to report various measurements to the network. When the message is sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

### 4.7.8 Bearer management

RADIO BEARER RECONFIGURATION- medium desirable (CH)

RADIO BEARER RECONFIGURATION COMPLETE - medium desirable (CH)

RADIO BEARER RECONFIGURATION FAILURE - medium desirable (CH)

RADIO BEARER RELEASE - medium desirable (CH)

RADIO BEARER RELEASE COMPLETE - medium desirable (CH)

RADIO BEARER RELEASE FAILURE - medium desirable (CH)

RADIO BEARER SETUP - medium desirable (CH)

RADIO BEARER SETUP COMPLETE - medium desirable (CH)

RADIO BEARER SETUP FAILURE - medium desirable (CH)

TRANSPORT CHANNEL RECONFIGURATION - medium desirable (CH)

TRANSPORT CHANNEL RECONFIGURATION COMPLETE - medium desirable (CH)

TRANSPORT CHANNEL RECONFIGURATION FAILURE - medium desirable (CH)

PHYSICAL CHANNEL RECONFIGURATION - medium desirable (CH)

PHYSICAL CHANNEL RECONFIGURATION COMPLETE - medium desirable (CH)

PHYSICAL CHANNEL RECONFIGURATION FAILURE - medium desirable (CH)

These messages are used for radio bearer management. When the messages are sent after a successful security mode procedure the application of integrity protection is considered to be medium desirable (status = CH).

### *4.8 RRC connection management*

SIGNALLING CONNECTION RELEASE - medium desirable (status = CH)

SIGNALLING CONNECTION RELEASE REQUEST - medium desirable (status = CH)

This message is to release a signalling connection (up to four) which was set up using the radio bearer setup messages. When the messages are sent after a successful security mode procedure the application of integrity protection is considered to be medium desirable (status = CH).

PAGING TYPE 2 - low desirable (status = CH)

This message allows the network to transmit dedicated paging information to the user. When the message is sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

RRC CONNECTION RELEASE COMPLETE – medium desirable (status = CH)

This message is to release an RRC connection. When the messages are sent after a successful security mode procedure the application of integrity protection is considered to be medium desirable (status = CH).

RRC CONNECTION RE-ESTABLISHMENT – **for further study**

RRC CONNECTION RE-ESTABLISHMENT COMPLETE – **for further study**

RRC CONNECTION RE-ESTABLISHMENT REQUEST – **for further study**

RRC STATUS – **for further study**

Further study is required into the usage of messages for re-establishing an RRC connection. These messages may be able to indicate that the previous RRC connection failed due to an integrity check failure, so they might be quite important.

### *4.9 UE capability management*

UE CAPABILITY ENQUIRY - low desirable (status = CH)

UE CAPABILITY INFORMATION - low desirable (status = CH)

UE CAPABILITY INFORMATION CONFIRM - low desirable (status = CH)

These messages allow the network to request the UE capability during mid-RRC session. When the message is sent after a successful security mode procedure the application of integrity protection is considered to be low desirable (status = CH).

## 5

## Annex: Complete list of RRC messages

ACTIVE SET UPDATE

ACTIVE SET UPDATE COMPLETE

ACTIVE SET UPDATE FAILURE

CELL UPDATE

CELL UPDATE CONFIRM

COUNTER CHECK

COUNTER CHECK RESPONSE

DOWNLINK DIRECT TRANSFER

DOWNLINK OUTER LOOP CONTROL

HANDOVER TO UTRAN COMMAND

HANDOVER TO UTRAN COMPLETE

INITIAL DIRECT TRANSFER

INTER-SYSTEM HANDOVER COMMAND

INTER-SYSTEM HANDOVER FAILURE

MEASUREMENT CONTROL

MEASUREMENT CONTROL FAILURE

MEASUREMENT REPORT

PAGING TYPE 1

PAGING TYPE 2

PHYSICAL CHANNEL RECONFIGURATION

PHYSICAL CHANNEL RECONFIGURATION COMPLETE

PHYSICAL CHANNEL RECONFIGURATION FAILURE

PHYSICAL SHARED CHANNEL ALLOCATION

PUSCH CAPACITY REQUEST

RADIO BEARER RECONFIGURATION

RADIO BEARER RECONFIGURATION COMPLETE

RADIO BEARER RECONFIGURATION FAILURE

RADIO BEARER RELEASE

RADIO BEARER RELEASE COMPLETE

RADIO BEARER RELEASE FAILURE

RADIO BEARER SETUP

RADIO BEARER SETUP COMPLETE

RADIO BEARER SETUP FAILURE

RNTI REALLOCATION

RNTI REALLOCATION COMPLETE

RNTI REALLOCATION FAILURE

RRC CONNECTION RE-ESTABLISHMENT

RRC CONNECTION RE-ESTABLISHMENT COMPLETE

RRC CONNECTION RE-ESTABLISHMENT REQUEST

RRC CONNECTION REJECT

- RRC CONNECTION RELEASE
- RRC CONNECTION RELEASE COMPLETE
- RRC CONNECTION REQUEST
- RRC CONNECTION SETUP
- RRC CONNECTION SETUP COMPLETE
- RRC STATUS
- SECURITY MODE COMMAND
- SECURITY MODE COMPLETE
- SECURITY MODE FAILURE
- SIGNALLING CONNECTION RELEASE
- SIGNALLING CONNECTION RELEASE REQUEST
- SYSTEM INFORMATION
  - First Segment
  - First Segment (short)
  - Subsequent Segment
  - Last Segment
  - Complete SIB
  - System Information Blocks
  - Master Information Block
  - System Information Block type 1
  - System Information Block type 2
  - System Information Block type 3
  - System Information Block type 4
  - System Information Block type 5
  - System Information Block type 6
  - System Information Block type 7
  - System Information Block type 8
  - System Information Block type 9
  - System Information Block type 10
  - System Information Block type 11
  - System Information Block type 12
  - System Information Block type 13
  - System Information Block type 13.1
  - System Information Block type 13.2
  - System Information Block type 13.3
  - System Information Block type 13.4
  - System Information Block type 14
  - System Information Block type 15
  - System Information Block type 15.1
  - System Information Block type 15.2
  - System Information Block type 15.3

System Information Block type 16

SYSTEM INFORMATION CHANGE INDICATION

TRANSPORT CHANNEL RECONFIGURATION

TRANSPORT CHANNEL RECONFIGURATION COMPLETE

TRANSPORT CHANNEL RECONFIGURATION FAILURE

TRANSPORT FORMAT COMBINATION CONTROL

TRANSPORT FORMAT COMBINATION CONTROL FAILURE

UE CAPABILITY ENQUIRY

UE CAPABILITY INFORMATION

UE CAPABILITY INFORMATION CONFIRM

UPLINK DIRECT TRANSFER

UPLINK PHYSICAL CHANNEL CONTROL

URA UPDATE

URA UPDATE CONFIRM