SP-010312

3GPP TSG-SA WG3 (Security)

Status Report to SA#12

18-21 June 2001

Stockholm, Sweden

Professor Michael Walker

Chairman 3GPP TSG-SA WG3

Content of Presentation

- Report from TSG-SA WG3 and review of progress (AI 7.3.1)
- Questions for advice from TSG-SA WG3 (AI 7.3.2)
- Approval of contributions from TSG-SA WG3 (AI 7.3.3)

Report and Review of Progress in SA3 (AI 7.3.1)

- Contents for agenda item 7.3.1
  - General overview of progress
  - Elections
  - Meetings since SA#11
  - Review of progress on major work items
  - Liaisons copied to SA
  - Meetings scheduled after SA#12

General Overview of Progress

- Focus has been on correcting R99, completing MAP security for Release 4, and progressing IP network layer security and IP multimedia subsystem security for Release 5
- SA3 has also reviewed the work programme and has produced a one new work item description and four revised work item descriptions
- In addition, SA3 has addressed feedback from other groups

Elections

- Valtteri Niemi (Nokia) was elected as vice chairman
  - Valtteri Niemi replaces Stefan Pütz (T-Mobil) who resigned
- Bernie McKibben (Motorola) has resigned as chairman of the lawful interception subgroup
  - Elections will be held at the next SA3 LI meeting

Meetings since SA#11

(TD SP-010348)

- SA WG3 meeting #17bis, Madrid, 23-27 April 2001
  - NDS ad hoc (2 days)
  - IMS security ad hoc (1 day)
  - SA3/SA2 IMS security joint meeting (1 day)
  - SA3/GERAN joint meeting (1 day)
- T3 ad hoc meeting #37 (joint with SA3), Munich, 3 May 2001
- SA WG3 meeting #18, Phoenix, 21-24 May 2001
  - Including joint meeting with TIA TR-45 AHAG

A5/3 development and A5 key length

- An ETSI SAGE work plan on A5/3 was endorsed at SA3#18 subject to some further consideration on the development of a GEA3 algorithm
- Development of A5/3 continues to be delayed as ETSI and GSMA have not reached agreement on the distribution and ownership of the algorithm
- GSM operators are reminded that they are now expected to support full length 64 bit cipher keys

MAP security for Release 4

- SA#11 granted SA3 an extension to allow MAP security (TS 33.200) to be submitted for approval as part of Release 4 at SA#12
- TS33.200 v1.0.1 was distributed to SA for information by email on Friday 8th June
- TS33.200 v2.0.0 is presented to SA#12 for approval

MAP security for Release 5

- The remaining work for Release 5 is to specify automatic key management
- Completion is expected at SA#15 in March 2002

- ***The approval of the revised WID will be handled under agenda item 7.3.3***

IP network layer security for Release 5

- Some progress was made on IP network layer security
  - Use of IPsec to secure signalling within and between networks
  - E.g. GTP, IMS signalling
- New timescales:
  - TS 33.210 will be presented to SA#14 for information in December 2001 and presented for approval at SA#15 in March 2002
- ***The approval of the revised WID will be handled under agenda item 7.3.3***

IP Multimedia Subsystem Security

- Some progress was made on specifying access security mechanisms for the IP multimedia subsystem
- In particular, it was agreed to locate the user authentication check in the the S-CSCF
- New timescales:
  - TS 33.203 will be presented to SA#14 for information in December 2001 (originally planned at SA#11) and presented for approval at SA#15 in March 2002
- ***The approval of the revised WID will be handled under agenda item 7.3.3***

GERAN Security

- An LS was sent to GERAN informing them that SA3 did not accept that a MAC of 24, 16 or 8 bits could be used because it would be so vulnerable as to not warrant the effort expended in computing or verifying it
- RLC/MAC control messages in GERAN should not be integrity protected unless a full 32 bit MAC-I can be provided – anything less represents a totally false sense of security
- A CR was agreed to include a reference in TS 33.102 to the security specifications in the GERAN stage 2 specification TS 43.041

Liaisons copied to SA

- SP-010349: Security and UE functionality split
  - Sent in response to LSs from SA1 and T3 on the possibilities for splitting UE functionality
  - SA3 reminds the other groups
    - Authentication of USIM cannot imply authentication of any other UE component
    - User traffic and signalling information is only protected over the radio access link and not within the UE
    - The only device that provides a secure environment within the UE is the USIM
  - SA3 invite SA1, T2 and T3 to a joint meeting on this subject on 3rd July in Newbury, UK

Meetings Scheduled after SA#12

- SA1/SA3/T3/T3 UE functionality split joint meeting, 3 July 2001, Newbury UK
- SA3#19, 4-6 July 2001, Newbury, UK
- SA3#20, 15 or 16-18 October 2001, Sydney, Australia
- SA3#21, 3-5 December 2001, Sophia Antipolis, France (TBC)
- SA3#22, 26-28 February 2002, Bristol, UK
- SA3#23, 14-16 May 2002, Canada / NW USA
- SA3#24, 9-11 July 2002, Helsinki, Finland (TBC)
- SA3#25, 15-17 October 2002, Munich, Germany (TBC)

Questions for Advice from S3 (AI 7.3.2)

- SA3 specifications for IMS security will depend on IETF documents
- Late changes or future modification by the IETF could cause problems with 3GPP implementations
- Advice is sought from SA on how dependency on the IETF should be handled in general within 3GPP

Approval of Contributions from S3 (AI 7.3.3)

- Contents for agenda item 7.3.3
  - TIA TR-45 / 3GPP joint AKA control
  - TS 33.200, MAP security
  - CRs to SA3 specifications
  - New work item description
  - Revised work item descriptions

TIA TR-45 / 3GPP joint AKA control

- SP-010349: TR-45 / 3GPP Joint AKA Control
  - Ownership of specifications remains with 3GPP but TR-45 AHAG can submit requests for CRs via SA3
  - Clauses in 33.102, 33103 and 33.105 have been identified for joint control
  - Two classes of CRs from TR-45 AHAG to 3GPP SA3 (normal and priority)
  - Liaison officers have been appointed
  - Joint meetings twice a year (last one was at SA#18 in Phoenix in May)

TS 33.200 v2.0.0, MAP security

- SP-010322, TS 33.200 v2.0.0, MAP security
  - An extra ad hoc meeting was scheduled to progress this work
  - Some editor's notes remain but none have prevented CN4 from completing the corresponding stage 3 changes to TS 29.002
  - The changes to TS 29.002 were submitted for approval at CN#12
- SP-010347, Summary of editor's notes in TS 33.200 v2.0.0

CRs on Security Architecture (1/2)

- 5 corrective CRs to 33.102 (R99 / Release 4)
  - SP-010313: CR144/145: Periodic local authentication
    - Earlier CR not fully implemented in R99 version and further changes required to align with stage 3 changes agreed at RAN#11
  - SP-010314: CR146/147: COUNT-C description
    - To align with RAN stage 3 specification so that for all transparent mode RLC bearers the same COUNT is used for uplink and downlink (it remains that different values are used for RLC AM and RLC UM)
  - SP-010316: CR149/150: START calculation and wrap around
    - Produced in response to LS from RAN2. Once START reaches its maximum it is kept there and not allowed to wrap. Corresponding CRs to stage 3 specifications were tabled at RAN#12
  - …

CRs on Security Architecture (2/2)

- 5 corrective CRs to 33.102 (R99 / Release 4)
  - …
  - SP-010317: CR 151/152: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted
    - Produced in response to LS from RAN2. ME uses default THRESHOLD value because corresponding USIM file not available. CRs to stage 3 specifications were tabled at RAN#12
  - SP-010319: CR 153/154: THRESHOLD check at RRC connection establishment
    - Produced in response to LS from RAN2. The THRESHOLD check is now done at RRC connection release. Corresponding CRs to stage 3 specifications were tabled at RAN#12

CRs on Security Architecture

- 1 category B CR to 33.102 (Release 5)
  - SP-010315: CR148: Include reference to TS 43.041 GERAN stage 2 specification
    - GERAN security specifications are contained in TS 43.041 rather than TS 33.102

CRs on Integration Guidelines

- SP-010320, 1 corrective CR to 33.103 (R99 / Release 4)
  - CR014/015: The multiplicity of data integrity symbols
    - Some of the symbols in the tables are corrected

CRs on Algorithm Requirements

- SP-010321, 1 corrective CR to 33.105 (R99 / Release 4)
  - CR019/020, Deletion of the maximum size of an RRC message

CR on Lawful Interception

- SP-010374, CR to 33.107 (Rel-5)
  - CR 004r1: Update for Rel-5

New Work Item Description

- SP-010324, New WI: Security aspects of requirement for network configuration independence

Revised Work Item Descriptions

- New timescales:
  - SP-010323, Revised WI: Access security for IP-based services
  - SP-010325, Revised WI: Network domain security; MAP application layer security (NDS/MAPsec) (formerly known as MAP application layer protection)
  - SP-010326, Revised WI: Network domain security; IP network layer security (NDS/IP) (formerly known as network domain security)
- Adds new linked work item: OAM&P– User Equipment Management:
  - SP-010327, Revised WI: MExE security analysis activity