SP-000664

3GPP TSG-SA WG3 (Security)

Status Report to SA#10

11-14 December, 2000

Bangkok, Thailand

Michael Walker

Chairman 3GPP TSG-SA WG3

Content of Presentation

- Report and review of progress in SA WG3
- Approval of contributions from SA WG3

Report and Review of Progress in SA3

- General overview of progress
- Confidentiality/integrity algorithms
- Authentication algorithm
- Work programme
- Outlook for future meetings
- Meetings scheduled after SA#10
- Recommendation on MAP security

General Overview of Progress

- SP-000621, Report of SA WG3 ad hoc meeting and draft report of meeting #16 - ***for information***
  - Report of SA WG3 ad hoc meeting, 8-9 November 2000, Munich, Germany
  - Draft report of SA WG3 meeting #16, 28-30 November 2000, Sophia Antipolis, France
- Focus has been on completing R99, progressing network domain security for R4/R5, progressing IM subsystem security for R5 and addressing feedback from other groups
- SA3 has also reviewed the work programme and has produced one revised work item description

Publication of KASUMI: Confidentiality & Integrity Algorithms

- SA#7 approved report on the work performed by SAGE task force
  - Published as 3G TR 33.908
- And approved algorithms for distribution to 3GPP partners
  - Publication of algorithm specifications and report on evaluation results was delayed for procedural reasons
- Algorithm specification published on ETSI web site on 4 September 2000 (3G TS 35.20x series)
  - http://www.etsi.org/dvbandca/
- SP-000629, 33.909 v1.0.0: Report on the evaluation of the 3GPP confidentiality and integrity algorithms - ***for approval***

Authentication Algorithm

- SA#7 approved the development of standard authentication algorithm and SAGE work plan tabled at SA#7
  - Funding approved by 3GPP in June 2000
  - SAGE work now complete on schedule
- SP-000630, SAGE authentication algorithm deliverables - ***for approval***

Network Domain Security

- MAP security specifications in TS 33.200 were scheduled to be presented for information at SA#10 and for approval at SA#11
- At S3#16 a simplified architecture for securing native IP-based protocols using IPsec was adopted
- Although the specifications for MAP security are stable it was not possible to create a new version of TS 33.200 for approval by S3 and submission to SA
- A new draft of 33.200 will be distributed to the SA mailing list for information in the New Year
- If acceptable to SA, it is still planned to present TS 33.200 to SA#11 for approval
- SP-000631, Information on WI “Network domain security” - ***for information***

IP Multimedia Subsystem Security

- Competing proposals have been considered in SA3
  - discussion around where to terminate authentication
- Email discussion to agree proposal for S3#17
- TS scheduled to be presented to SA#11 for information
  - other groups can then start to use TS as basis for their specifications
- TS scheduled to be presented to SA#12 for approval

Work Programme

- Structured programme of security work items is being reviewed and maintained
  - 15 WIDs approved at SA#8
  - 2 revised WIDs approved at SA#9
  - 6 new WIDs approved at SA#9
  - SP-000629, Revised WI: FIGS/IST work item description - ***for approval***
  - See also latest project plan and security IGC report from S2

Outlook for Future Meetings

- With the stability of R99, SA3 will now continue with the work for R4 and R5.
- Main work items for R4
  - Network domain security - MAP security
  - GERAN security
- Main work items for R5
  - Network domain security
  - IM subsystem security

Meetings Scheduled after SA#10

- S3#17, 27 February - 1 March 2001, Sophia Antipolis, France
- S3#18, 21 or 22 - 24 May 2001, Phoenix, USA (location TBC)
- S3#19, 3 or 4 - 6 July 2001, London, UK (location TBC)
- S3#20, 15 or 16 - 18 October 2001, Madrid, Spain (location TBC)

Risks in Introduction of MAP security

- Introduction of MAP security by a limited number of operators would give only limited protection even to those operators who choose to implement MAP security in their networks
- S3 suggest to set a cut-off date for the introduction of MAP security
- S3 feel that GSM association are the appropriate body to set such a cut-off date
- SA are requested to send a corresponding LS to the GSM association
- SP-000622, LS from SA3: Security risks in introduction phase of MAP security

Approval of Contributions from S3

- CRs to SA3 specifications
- New SA3 specifications and reports
- Revised work item descriptions

CRs on Lawful Interception

- SP-000623, CRs 002 and 003 to 03.33: Addition of parameters to the X3-Interface (S3-000762)
  - Note that CR003 to R99 is classified as Cat ‘C’ but corresponds to LI requirements already agreed for R99
- SP-000624, CRs 004 and 005 to 03.33: Deletion of mono-mode and addition of optimal routing (S3-000764)
- SP-000625, CR 001 to 33.107: Addition of parameters to the X3-Interface (S3-000763)

CRs on Security Architecture

- SP-000626, 6 CRs to 33.102
  - CR 129 Corrections on ciphering and integrity protection (S3-000666)
  - CR 130 Re-transmission of authentication request using the same quintet (S3-000725)
  - CR 131 Corrections to Counter Check procedure (S3-000726)
  - CR 132 Intersystem handover for CS Services – from GSM BSS to UTRAN (S3-000727)
  - CR 133 Correction on use of GSM MS classmark in UMTS (S3-000729)
  - CR 134 START value handling for MS with a GSM SIM inserted (S3-000739)
- SP-000627, CR 015 to 33.105: Layer 2 related corrections (S3-000667)

New SA3 Reports and Specifications

- SP-000629, 33.909 v1.0.0: Report on the evaluation of the 3GPP confidentiality and integrity algorithms (S3-000660)
  - SA#10 are asked to forward TR 33.909 to PCG for approval for publication by the Partner SDOs
- SP-000630, SAGE authentication algorithm deliverables (S3-000730)
  - SA#10 are asked to forward authentication algorithm deliverables to PCG for approval for publication by the Partner SDOs

Revised Work Item Description

- SP-000629, Revised WI: FIGS/IST work item description (S3-000745)