3GPP TSG-SA WG3 (Security)

SP-99583, Status report to SA meeting # 6

Sophia Antipolis

15-17 December 1999

Dr. Stefan Pütz

Vice-chairman 3GPP TSG-SA WG3

T-Mobil

Content of presentation

- Summary of documents tabled by S3
- Status of deliverables - followed by approval
- Status of cipher/integrity algorithm design
- Standardisation of authentication algorithm
- Mobile IP security
- GLR security
- Meeting schedule

Document list, 1

- SP-99592, Liaisons to SA plenary
  - MAP security
  - TIA TR-45 AHAG (x 2)
  - Authentication failure message
  - VHE/OSA security

Document list, 2

- SP-99xxx, Report of SA WG3 meeting #7, 26-28 Oct 99, The Hague - *for information*
- SP-99xxx, Report of SA WG3 meeting #8, 16-19 Oct 99, Sophia Antipolis - *for information*
- SP-99xxx, Draft Report of SA WG3 meeting #9, 7-9 Dec 99, Helsinki - *for information*

Document list, 3

- SP-99590, CR to TS 21.133, Security threats and requirements - *for approval*
- SP-99584, CRs to TS 33.102, Security architecture - *for approval*
- SP-99585, CR to TS 33.102, Security architecture - *for approval*
- SP-99586, CRs to TS 33.103, Integration guidelines - *for approval*

Document list, 4

- SP-99587, CRs to TS 33.105, Cryptographic algorithm requirements - *for approval*
- SP-99589, CR to TR 33.902, Formal analysis of security mechanisms - *for approval*
- SP-99588, CR to TS 33.106, LI requirements - *for approval*
- SP-99591, TS 33.107, LI architecture - *for approval*

Liaisons to SA plenary, SP-99592, 1

- MAP security, S3-99553
  - Encryption and integrity on signalling links between and within 3G operators
  - **Essential** security feature for R99
    - All new MAP dialogues to be protected
    - Other messages to be prioritised
  - Joint meeting N2/S3 on 6-7 January 2000
  - BEANO algorithm may be available for use

Liaisons to SA plenary, SP-99592, 2a

- TIA TR-45 AHAG, S3-99463, S3-99551
  - 3GPP authentication mechanism proposed as a candidate for TIA TR-45 ESA
  - TR-45 plenary in December decided to adopt 3GPP mechanism with three month review period
  - Specific technical requirements from TR-45 to be studied
  - Joint meeting with AHAG in Stockholm in April 2000
  - Lobbying in TIA should be continued, especially in TR-45.2

Liaisons to SA plenary, SP-99592, 2b

- TIA TR-45 AHAG
  - Proposal for S3 to remain design authority but changes are approved in both groups - *for SA endorsement*

T-Mobil

Liaisons to SA plenary, SP-99592, 3

- Authentication failure message, S3-99537
  - Failure indication from MSC/SGSN to HLR
  - Indication of active attacks against networks
  - See CR33.102-040

Liaisons to SA plenary, SP-99592, 4

- VHE/OSA security, S3-99554
  - HE does not manage services obtained directly from VASP - authorisation in this case is transparent for OSA
  - UA to application authorisation via secure access to User Profile Data verifies that UA has rights to specific applications. If UA selects application via VHE then he can be assumed to have rights to access that application.
  - The secure user identity used for network access authentication may be transferred to the application layer since VHE is a mechanism to provide applications to users authenticated in the UMTS network

Status of 3GPP security deliverables, 1

TS33.120	Security principles and objectives	Approved at SA#3	Stable
TS21.133	Security threats and requirements	Approved at SA#3.	CR at SA#6 to clarify security requirements relating to integrity protection of user traffic.
TS33.102	Security architecture	Approved at SA#3. 11 CRs approved at SA#4. 10 CRs approved at SA#5.	CRs at SA#6.

Status of 3GPP security deliverables, 2

TS33.103	Integration guidelines	Approved at SA#5.	CRs at SA#6. Further CRs required to align with architecture.
TS33.105	Cryptographic algorithm requirements	Approved at SA#4. 3 CRs approved at SA#5.	CRs at SA#6. Further CRs required to align with architecture.
TR33.901	Criteria for cryptographic algorithm design process	Approved at SA#4.	Stable.

Status of 3GPP security deliverables, 3

TS33.106	Lawful interception requirements	Approved at TSG-SA #4.	CRs at SA#6.
TS33.107	Lawful interception architecture and functions	Approval at SA#6 planned.	Presented for approval at SA#6.
TR33.900	Guide to 3G security	Approval at SA#6 planned.	Postponed until SA#7.
TR33.902	Formal analysis of security mechanisms	Approved at SA#5.	CR at SA#6 to add missing analysis.

Other security deliverables

- TS 23.048, USIM toolkit security
  - Transfer of GSM 03.48 v8.1.0 into 3G R99
  - Enhancements for R00
- TS 22.022, ME personalisation (now under S3 control)
  - Transfer of GSM 02.22 into 3G R99
  - Do we need this feature in R00?

TS 21.133, Security requirements and threats

- CR for approval, SP-99590:
  - CR001, Data integrity of user traffic, S3-99450

TS 33.102, Security architecture, 1

- CRs for approval, SP-99584:
  - CR022, Refinement of enhanced user identity confidentiality, S3-99459
  - CR025, Length of KSI, S3-99389
  - CR026, Mobile IP security, S3-99541
  - CR027, Clarification of re-authentication during PS connections, S3-99552
  - CR030, Handling of the ME UEA and UIA capability information, S3-99409

TS 33.102, Security architecture, 2

- CRs for approval, SP-99584:
  - CR031, see later
  - CR032, Removal of duplicate network-wide encryption section, S3-99543
  - CR033, Distribution of authentication data within one serving network domain, S3-99545
  - CR034, Interoperation and intersystem handover between UTRAN and GSM BSS, S3-99544
  - CR035, Authentication and key agreement, S3-99538

TS 33.102, Security architecture, 3

- CRs for approval, SP-99584:
  - CR036, Sequence number management, S3-99539
  - CR037, Authentication and key agreement, S3-99548
  - CR038, Clarification on system architecture, S3-99528
  - CR039, Update definitions and abbreviations, S3-99529
  - CR040, An authentication failure report mechanism from SN to HE, S3-99536
  - CR041, UIA and UEA identifications, S3-99520

TS 33.102, Security architecture, 4

- CR for approval, SP-99585:
  - CR031, Removal of alternative authentication mechanism described in Annex D, S3-99542

TS 33.103, Integration guidelines

- CRs for approval, SP-99586:
  - CR001, Refinement of enhanced user identity confidentiality, S3-99456
  - CR002, Corrections to Figure 1, S3-99390
  - CR004, Change length of KSI (and other miscellaneous corrections), S3-99415

TS 33.105, Cryptographic algorithm requirements

- CRs for approval, SP-99587
  - CR004, Time varying parameter for synchronisation of ciphering, S3-99384
  - CR005, Direction bit in f9, S3-99455

TR 33.902, Formal analysis of security mechanisms

- CR for approval, SP-99589:
  - CR001, Formal analysis of 3G authentication protocol, S3-99505

TS 33.106, LI requirements

- CR for approval, SP-99588:
  - CR001, Lawful interception requirements, S3-99522

TS 33.106, LI architecture

- TS 33.206 v1.0.0 for approval, SP-99591/S3-99508
  - Architecture and Functions for 3G lawful interception
  - This specification complements 33.106, Lawful interception requirements. There has not been raised any controversial issues raised during its genesis
  - The specification is presented for immediate approval, because lawful interception will be a mandatory regulatory requirement from the beginning.
  - There are no changes to other specifications resulting from the approval of 33.107.

Review by S3 of all security relevant specifications

- S3 propose to assist in the review of all the relevant specifications for all the security work topics on completion of tasks by TSGs
- Ensure that S3 security features are properly implemented in the R99 specifications
- Identify where corrective CRs are required

(see also S2 security co-ordination presentation)

Status of cipher/integrity algorithm design, 1

- Evaluators selected jointly with SAGE at S3#7
  - Bart Preneel, Katholieke Universiteit Leuven(B), Lars Knudsen, University of Bergen (N) and others
  - Jacques Stern, Ecole Normale Supérieure(F)
  - Fred Piper, Royal Holloway (UK)
- Evaluation period: 15 Nov - 13 Dec
- SAGE reviewing results this week
- Publication of KASUMI at SA#7

Status of cipher/integrity algorithm design, 2

- Biryukov/Shamir A5/1 analysis
  - Requires known plaintext
  - Enhanced time-memory trade-off (making best use of computing resource)
  - Theoretically interesting but not proven to be practical
  - Such developments are to be expected as attackers have access to increased computing power - A5/1 is getting old
  - Proposal to develop a mode of operation of KASUMI for GSM

Standardisation of authentication algorithm

- S3 to provide authentication algorithm for 3GPP that could be used by operators who do not wish to provide one of their own
- To be published as a 3GPP specification
- May be defined around a kernel function which would allow operators to choose different kernels
- S3 currently writing requirements specification
- Will seek approval of specification and process at next meeting

Mobile IP security

- IP security renamed mobile IP security in R99 specifications
- Mobile IP security is provided independently to the 3G security architecture in R99
- Further study for R00
  - Profiling of IETF application security solutions for mobile environment
  - Mapping of 3G access security features to “all-IP” network

GLR security

- S3 is studying security issues associated with GLR concept
- Offers opportunities for easier handling of authentication vectors
- May aid key management for MAP security and provides more options for its introduction

Meeting schedule

- *25 Oct 99, The Hague, Joint session with SAGE*
- *26-28 Oct 99, The Hague, S3#7 (with SMG10)*
- *16-19 Nov 99, Sophia Antipolis, S3#8 (with SMG10)*
- *7-9 Dec 99, Helsinki. S3#9*
- 19-21 Jan 2000, Antwerp, S3#10
- 22-24 Feb 2000, Mainz, S3#11
- 11-14 Apr 2000, Stockholm, S3#12
- 23-25 May 2000, Tokyo, S3#13