3GPP TSG-SA WG3 (Security)

Status Report to SA#13

24-27 September 2001

Beijing, China

Michael Walker

Chairman 3GPP TSG-SA WG3

Report and Review of Progress in SA3 (AI 7.3.1)

- General overview of progress
- Meetings since SA#12
- Lawful interception sub-group election
- Review of progress on major work items
- Meetings scheduled after SA#13

General Overview of Progress

- Correcting MAP security for Rel- 4
- Progressing IP network layer security for Rel-5
- Progressing IP multimedia subsystem security for Rel-5
- Considering security implications for IMS access of UE split
- Addressing feedback from other groups

Meetings Since SA#12

- SA WG3 meeting #19, Newbury, UK, 3-6 July ‘01 (***SP-010491 – for info***)
    - Included joint SA1/SA3/T2/T3 meeting on security implications of UE functionality split
    - and a meeting on IMS with CN1 representatives
- SA WG3 meeting #19bis, Sophia Antipolis, France, 13-14 Sept ‘01
    - MAP security ad hoc (1 day)
    - IMS security ad hoc (1 day)

Lawful Interception Sub-Group Election

- Rolf Schnitzler (D2 Vodafone) was elected as chairman for one year
  - Rolf Schnitzler replaces Bernie McKibben (Motorola) who resigned

MAP Security (Rel-4)

- The MAP security specification (TS 33.200) was approved at SA#12
- SA#12 asked SA3 to remove the remaining editor’s notes as soon as possible
- CRs are presented to SA#13 which resolve issues described in the editor’s notes
- Problem with standard for (counter) mode of operation of algorthim
  - ISO/IEC 10116 will not be complete until 2003
  - NIST 800-xy possible - but not all agree

MAP Security (Rel-5)

- The work for Rel-5 is to specify automatic security association establishment (keys, etc)
- Progress has been made on an IETF MAPsec Domain of Interpretation for the Internet Key Exchange protocol which will be used between the Key Administration Centres in different PLMNs
- Approval is expected at SA#15

IP Network Layer Security (Rel-5)

- Profiling IPsec to secure signalling within and between networks
- TS 33.210 will be presented to SA#14 for information and presented for approval at SA#15

IP Multimedia Subsystem Security (Rel-5) Meeting with Representatives from CN1

- It was confirmed that the following security features would be provided for IMS
  - authentication, support for signalling encryption, signalling integrity, configuration hiding, security mode set-up and security implications for session transfer (a fraud issue for the GSMA)
- Current assumption is that authentication will be provided only at registration and re-registration
- The need for network initiated authentication is still being studied - in order to handle authentication of different public identities

IP Multimedia Subsystem Security (Rel-5) Meeting with Representatives from CN1, 2

- It was noted that the security architecture
  - assumes that a user has one private identity (with which all keys are associated) but may have several public identities
  - re-registration is handled by the same S-CSCF that performed the original registration
- A joint meeting with CN1 will be organised towards the end of the year.

IP Multimedia Subsystem Security (Rel-5) Progress

- Information flows for authentication are under development
- Proposals for security mode establishment at SIP-level being considered
- Two approaches for integrity protecting the UE to P-CSCF link proposed (IPsec or SIP-level protection)
  - ad-hoc held to try to resolve issue - no agreement
  - continue with both approaches but monitor progress in IETF to check availability of SIP-level solution for Rel5

IP Multimedia Subsystem Security (Rel-5) Progress, 2

- Scope of the hiding needs further elaboration
  - Currently domain names and numbers of S-CSCfs
  - Callers IP address, public identity?
- TS 33.203 will be presented to SA#14 for information and to SA#15 for approval

IP Multimedia Subsystem Security (Rel-5) working with IETF

- SA3 delegates participated in the London IETF meeting
- SA3 specifications for IMS/SIP security will use solutions acceptable to the IETF so that they apply to generic SIP- S3 to work together with IETF SIP security group
- SA3 reviewed security aspects of the “3GPP requirements on SIP” ID developed in CN1 - comments to IETF on 21st September

UE functionality split

- SA1, T2 and T3 invited to SA3#19 in Newbury, UK for a meeting on security implications of UE functionality split
- Regarding IMS issues and UE functionality, SA3 has introduced concept of the ISIM
    - recognises that IMS identities and keys are distinct from those used for UMTS - but AKA mechanism is re-used
    - A corresponding LS was sent to SA1, T2, T3
- UE functionality split will be considered at future SA3 meetings

GERAN Security

- Two LSs were sent to GERAN
  - confirming that RLC/MAC messages cannot be integrity protected because 32-bits for the MAC are not always available (but shall be ciphered) (S3-010373)
  - confirming that UMTS authentication and key agreement mechanism (as specified in TS 33.102) shall be used for Iu-mode GERAN (S3-010374)

Meetings Scheduled after SA#13

- SA3#20, 16-19 Oct 2001, Sydney
- SA3#21, 27-30 Nov 2001, Sophia Antipolis **– *new date***
- SA3#22, 26 Feb – 1 Mar 2002, Bristol
- SA3#23, 14-17 May 2002, Vancouver / Seattle, (TBC)
- SA3#24, 9-12 July 2002, Helsinki, (TBC)
- SA3#25, 15-18 Oct 2002, Munich, (TBC)

Approval of Contributions from SA3 (AI 7.3.3)

- CRs to 33.102, Security Architecture
- CRs to 33.103, Security Integration Guidelines
- CRs to 33.107, Lawful Interception Architecture
- CRs to 33.200, MAP security

CRs on 33.102, Security Architecture (Rel-4)

- SP-010492, CR155R1: Removes the list of access type codes from the authentication failure report
  - The specification of access type codes is left to the stage 3 specification in 29.002 so that it is easier to update the authentication failure report when new access codes are added

CRs to 33.103, Integration Guidelines (R99, Rel-4)

- SP-010493, CR016/CR017: Correction of USIM parameter descriptions for authentication
  - Aligns 33.103 with 33.102 by removing certain parameters that need to be stored on the USIM and clarifying the definition of others

CRs to 33.107, Lawful Interception Architecture (R99, Rel-4)

- SP-010494, CR005: Missing location-related information in Packet Data Event records (R99)
  - Include service area identity
- SP-010495, CR007R1/CR008R1: Reporting of Secondary PDP context (R99, Rel-4)
  - clarifies that secondary PDR context is to be reported

CRs to 33.200, MAP Security (Rel-4) (1)

- SP-010496, CR001: Alignment with stage 3 to clarify that if one or more MAP component in a given dialogue needs protection then all components within that dialogue must be sent in a MAPsec container
    - Stage 3 very clear on this - 33.200 needs to be aligned
- SP-010497, CR002: Clarification of scope to remove misleading and ambiguous text - namely reference to ‘MAP version 3’
- SP-010498, CR003: Clarification on the policy for security association renewal - explanation of how one deals with renewed and old SAs
- SP-010499, CR004: Adds message flows to the annex B to describe what happens when two MAP network elements in different PLMNs engage in secure communications

CRs to 33.200, MAP Security (Rel-4) (2)

- SP-010500, CR005: Corrects policy requirements to ensure that MAPsec can be made secure against active attacks
  - Deals with cases where different operators use different protection modes
- SP-010501, CR006: Removes fallback indicator from MAP security association database (for alignment with CR005). Also describes how a MAP security association is identified
- SP-010502, CR007: Specifies length of integrity algorithm key (128 bits) and message authentication code (32 bits)
  - Previously assumed clear from context
- SP-010503, CR008: Corrects the order of encryption and authentication in part of the TS (the ordering is correctly specified as encrypt-then-authenticate elsewhere in the TS)