Title

Ad Hoc Authentication Group Meeting Summary
June 20-21, 2000 in Ottawa, Ontario, Canada

Source

Frank Quick (QUALCOMM), AHAG Vice-Chair

Recommendation

Approve and forward to the TIA. All contribution numbers pertain to AHAG, unless otherwise specified.

Summary:

- AHAG received and discussed contributions related to the "rogue shell" threat.
- AHAG sent a liaison to 3GPP stating that AHAG is working on guidelines for interaction with 3GPP, and suggesting that the matter be discussed during the September joint meeting.
- AHAG sent a liaison to TR-45.3 describing a problem found in Common Cryptographic Algorithms, Revision D, and asking whether TR-45.3 would like an update to be issued.
- AHAG sent a liaison to TR-45.5 suggesting that the Subcommittee establish a procedure for selecting an ESP algorithm for CDMA.
- AHAG sent a liaison to all Subcommittees stating that the AKA security association timer will not be supported by 3GPP, and recommending that revocation of the security association is an alternative mechanism that meets the intent of TR-45 home control requirements.

1. Call to Order and Opening Remarks. TR45.AHAG met June 20-21, 2000 in Ottawa, Ontario, Canada. Frank Quick (AHAG Vice-Chair) called the meeting to order at 9:00 AM EDT.

2. Meeting Attendance was:

1. Frank Quick (Qualcomm)	2. Dan Brown (Motorola)	3. Mike Karimian (Panasonic)
4. Bob Rance (Lucent)	5. Bob Slocum (Ericsson)	6. Dan Robertson (Denso)
7. Jason Brown (SBC TRI)	8. Michael Marcovici (Lucent)	

3. Meeting Agenda (2000.06.20.01, approved as submitted)

1. Call to Order and Opening Remarks
2. Attendance Registration
3. Introduce Contributions and Associate with Agenda
4. Agenda Review and Approval
5. Review Meeting Summary
6. Correspondence
7. Liaison Reports
    a. Committee TR-45
    b. Subcommittee TR-45.1
    c. Subcommittee TR-45.2
    d. Subcommittee TR-45.3
    e. Subcommittee TR-45.4
    f. Subcommittee TR-45.5
    g. Subcommittee TR-45.6
    h. Subcommittee TR-45.7
    i. 3GPP Security Group
8. Old Business
    a. Enhanced Subscriber Authentication
    b. Enhanced Subscriber Privacy
    c. Export Issues
    d. UIM
    e. Transport Security using IP
9. New Business
    a. To be determined.
10. Presentations
11. Schedule of Meetings
12. Assignments
13. Open Discussion
14. Adjournment

4. TR45.AHAG/2000.05.09-10 AHAG Contributions (T=TIA,E=EAR[1] Sensitive).

.##	Title	Sens.	Source	Agenda	Status
.01	Agenda	-	Chair	4.0	
.02	Meeting Summary; Seattle, Washington (May, 2000)	-	Chair	5.0	
.03	Proposed Security Enhancement to AKA	-	Qualcomm	8.a	
.04	Break and Fix Cycles	-	Qualcomm	8.b	
.05	The State of the ESP Process	-	Qualcomm	8.b	
.06	Relative Performance of Encryption Algorithms	-	Qualcomm	8.b	
.07	DCCH Message Encryption Correction for CCA Rev. D	**E**	Lucent	9.a	
.08	C Code for SHA-based functions for AKA	**E**	Lucent	8.a	
.09	SHA-based functions for AKA	**E**	Lucent	8.a	
.10	Enhanced local authentication for a 3GPP mobile	**E**	Lucent	8.a	
.11	A Practical Analysis of the SHA-based functions for AKA	-	Qualcomm	8.a	
.12	TR-45 Contribution 00.05.31.34 (ESA Correspondence)	-	TR-45 secy.	8.a	
.13	Draft Liaison to 3GPP on Interaction Guidelines	-	Chair	8.a	
.14	Draft Liaison on Home System control	-	Chair	8.a	
.15	Draft Liaison on ESP for CDMA-2000	-	Chair	8.b	
.16	Draft Liaison on Changes to CCA Rev D	-	Chair	9.a	

[1]As specified in the Export Administration Regulations (EAR), Title 15 CFR parts 730 through 774 inclusive.

5. The Meeting Summary.

The May 9-10, 2000 (Seattle, Washington) meeting summary (2000.06.20.02) was approved as modified.

Page	Line	Description
Global		Correct spelling of Marcovici
6	38	Change “9” to “5”.
6	21	Delete “it”.
7	13	Change “unpalatable…” to “inconsistent with 3GPP specifications.”

Bob Slocum (Ericsson) asked whether there would be a meeting summary for the conference call held May 19, 2000. Frank Quick, vice chair, agreed to ask Chris Carroll whether a summary would be available.

6. Correspondence

No correspondence was received.

7. Liaison Reports

7.a TR-45 (Committee)

Frank Quick, AHAG vice chair, provided a verbal report.

- TR-45 approved the AHAG/TR-45.2 recommendations on AKA with one modification. The recommendations as submitted to TR-45 were attached to the Seattle meeting summary (2000.06.20.02). The modification made by TR-45 was to add "as a priority" regarding the investigation of solutions to the "rogue shell" threat. It was agreed to add AHAG agenda item 8.f, 3GPP issues, to address these recommendations.

- Peter Nurse, TR-45 vice chair, noted that there may be copyright issues in using the AKA specifications from 3GPP.

7.b TR-45.1 (Analog)

There was no report.

7.c TR-45.2 (Intersystem)

Bob Slocum (Ericsson) provided an unofficial report. Mr. Slocum noted that the copyright issue raised in TR-45 was also mentioned in TR-45.2, but in his opinion this issue will not slow down the development of AKA standards in TIA. He also noted that the Authentication Focus Group plans to review the 3GPP specifications on AKA.

7.d TR-45.3 (TDMA)
Mike Karimian (Panasonic) provided a verbal report.

- Working groups 2 and 6 were meeting concurrent with the AHAG meeting, at TIA headquarters in Arlington, VA. The goal is to complete the 136-C ballot by the end of July.

- Work is in progress to include satellite positioning in the TDMA standards.

- Support for ESA is not included in 136-C. SCEMA is supported. It was noted that 136-B references Common Cryptographic Algorithms Revision D.

7.e TR-45.4 (Radio to Switching Technologies)

Dan Brown (Motorola) provided a verbal report.

- Two meetings were held since the last AHAG meeting. The subcommittee completed editorial review of PN-4545 (IOS version 1.0), and this revision has been sent for

publication.

- PN-4604, the A_{bis} interface standard, has been released for ANSI ballot.

- PN-4683, an IOS update including tandem-free operation, will go forward as an ANSI ballot, but will be split in the next revision to provide separate documentation of CDMA and TDMA services.

- IOS version 4.1 is under discussion. The goal is to complete this revision in July, but the schedule appears to be very tight.

7.f TR-45.5 (CDMA)

There was no report. The following points were discussed:

- The subcommittee has undertaken some discussion of AKA.

- The selection of an encryption algorithm for IS-2000 appears not to be on the subcommittee's agenda. (It was agreed later in the AHAG meeting to send a liaison to TR-45.5 on this subject.)

- The subcommittee is considering security standards for high-speed data services. It was felt that these standards should be brought to the AHAG for review.

7.g TR-45.6 (CDPD)

- There was no report.

7.h TR-45.7 (OAM&P)

There was no report. It was noted that this subcommittee is down to four voting members, of which only three typically attend meetings.

7.j 3GPP Security Group (S3)

Michael Marcovici (Lucent) provided a verbal report.

- Mr. Marcovici has been appointed the official liaison to AHAG.

- S3 met a few weeks before the AHAG meeting, in Yokohama, Japan. Several liaisons to AHAG have been approved, but apparently not yet transmitted. Mr. Marcovici plans to bring the correspondence to the next AHAG meeting.

- The subject of home control by revoking/renewing the authentication vector has been forwarded to CN4 for comment. The deadline for response is the September meeting.

- The AHAG correspondence on the use of SHA-1 for AKA functions f0-f5 was submitted to S3, where it was forwarded to SAGE for study. Frank Quick, AHAG vice-chair, was designated the contact for SAGE if any questions arise.

- The 3GPP specification sections subject to "joint control" have been tentatively identified. This information was circulated to S3 via email, and will likely be discussed during the next S3 meeting, planned for August 1-4 in Oslo, Norway.

- Mr. Marcovici reported that the security association duration timer was removed from specification 33-102. He believed that a liaison to AHAG had been approved stating this, but was unable to locate the temporary document containing the liaison. This issue is discussed further in agenda item 8.a.

- The subject of an authentication success report was discussed by CN4, but no response has been sent to S3. The deadline is the September meeting. CN4 may need more clarification. The general feeling appears to be that this should apply only to 3GPP2 mobiles and not to 3GPP mobiles.

- Authentication failure reporting remains a mandatory feature. A CR was submitted to make it optional, but this CR was rejected.

- A joint S3/AHAG meeting has been approved for September, provided that suitable facilities are available. The meeting may be at TIA headquarters or may be at a hotel in the Washington area.

- It was noted that AHAG should be prepared to discuss guidelines for interaction with 3GPP during the joint meeting with TR-45.2 in August. AHAG members were requested to consider this issue and be prepared to discuss it at the next meeting. It was agreed to send a liaison to 3GPP SA3 stating that we are working on such guidelines, and suggesting that we discuss the topic at the joint AHAG/SA3 meeting in September. The liaison is contribution #13, approved as submitted.

8. Old Business

8.a Enhanced Subscriber Authentication

- Frank Quick (Qualcomm) introduced contribution #3, Proposed Security Enhancement to AKA. This contribution describes a method for mitigating the "rogue shell" threat by keeping IK inside the UIM and creating a new key IK' from IK, where IK' is passed to the shell for its current uses in 3GPP systems. To prevent the rogue shell problem, the UIM would perform new local authentication procedures using IK.

- Michael Marcovici (Lucent) introduced contribution #10, Enhanced Local Authentication for a 3GPP Mobile. This contribution describes another method for mitigating the rogue shell threat. In this approach, the present anonymity key AK is

extended to 128 bits, and the upper 80 bits are used as a secret key for local authentication procedures. It is claimed that these bits are calculated already, but discarded, hence this approach does not involve extra computation in the UIM and HLR/AC. The upper 80 bits of AK must be added to the AV in network messages.

It was noted that billing practices in GSM lessen the impact of these threats on service providers, hence there is less interest in prevention.

It was suggested that a joint contribution be developed summarizing both the method of contribution #3 and contribution #10.

Jason Brown (SBC TRI) noted that neither method prevents all types of rogue shell attacks. For example, a shell could be programmed to modify a user's call forwarding while the legitimate UIM is in place. Prevention of such attacks would require switch procedures authenticating the user him/herself.

- Michael Marcovici (Lucent) introduced contributions #8 and #9, which provide an update of the procedures for using SHA-1 as functions f0-f5 in AKA. Contribution #9 provides a pseudocode description of the procedures, and contribution #9 provides C code. Notably, the whitening function was added to the AKA functions that depend on the MAC property of SHA.

- Frank Quick (Qualcomm) introduced contribution #11, which discusses the practicality of certain attacks that have been alleged against Sober. It is claimed that time/space tradeoff attacks are not practical, and that similar tradeoffs would also make Shazam appear to be much weaker than 128 bits.

- There was continued discussion of the security association timer issue brought up in the 3GPP liaison report. It was agreed to draft a liaison to the Subcommittees on this issue.

  The draft liaison is contribution #14, introduced by Frank Quick, Vice Chair. The liaison recommends that the revocation of a security vector meets those TR-45 requirements for home control that were formerly addressed through control of the timer. The liaison was amended to add "We note that, to be effective, this mechanism requires that the visited system delete the security association in a timely manner." The liaison was approved as amended.

- Contribution TR45/00.05.31.34 was reintroduced as contribution #12. This document is a liaison from TR-45.3 on the AKA issues discussed with 3GPP in Stockholm. It was noted that the only issue with TR-45.3's statement is that any efficient solution to the rogue shell threat appears to require changes to the UIM that would also affect AKA procedures.

8.b Enhanced Subscriber Privacy

- Frank Quick (Qualcomm) introduced contributions #4, #5 and #6.

  Contribution #4 states that the fixing of problems found in an algorithm does not necessarily make it weak. It also states that most of the algorithms in use by TIA have been modified in some way in response to critiques.

  Contribution #5 suggests that there is no clear choice among the proprietary algorithms proposed for ESP, and suggests that the ESP candidates be expanded to include the AES algorithms.

  Contribution #6 is an update of contribution 2000.05.09.04, adding an extrapolation of the performance data to large data sizes.

- In connection with these contributions, it was discussed whether AHAG can select an ESP algorithm for use in the CDMA air interface. There was general agreement that AHAG will be unable to make such a selection because of the lack of consensus on the preferred algorithm. It was agreed to send a liaison to TR-45.5 informing them of this, and suggesting that they establish a procedure for selecting an algorithm.

  The draft liaison is contribution #15, introduced by Frank Quick, Vice Chair. The liaison was amended to change “position” to “recommendation”. Statements were added that the AES selection should be made by the end of this year, and that NIST is responsible for the AES process. The last sentence (lines 12-13) were struck. The Vice Chair agreed to determine whether the CDMA standard will be an Interim Standard or a full ANSI standard, and to look for the date of the earlier liaison to the Subcommittees informing them of the availabile ESP candidates. The liaison was approved as amended.

8.c Export Issues

- There was no news in this area. The Vice Chair agreed to check with TIA on the ability to post AHAG documents to a web site.

8.d UIM

- There were no contributions for this Agenda item.

8.e Transport Security using IP

- There were no contributions for this Agenda item.

9. New Business

Contribution #07, from Lucent Technologies, points out an error in Common Cryptographic Algorithms, Revision D and proposes text changes to remedy the problem. The problem is that the text and code incorrectly call for the use of the DTC key schedule for encryption of the DCCH. The reason for having two key schedules was to allow

encryption of control channel information before the traffic channel key schedule has been created. The error can cause calls to fail since the DTC key schedule may not have been initialized at the time DCCH encryption occurs. This problem affects TIA/EIA-136 revision B and later. It was agreed to send a liaison to TR45.3, describing the problem and asking for guidance on whether to create a revision D.1 of the CCA to address the problem. This liaison was submitted as contribution #16, which was approved with modifications.

This item will be carried forward as old business for the next AHAG meeting.

10. Presentations

None.

11. Tentative Schedule of Meetings

Date	Time	Location	Hotel	Rate	Cut-off	Co-Located
July 18-19	9-5	Colorado Springs	TBD			
Aug. 15-16	9-5	Calgary, Alberta	TBD			TR-45.2
September 12-13	9-5	Washington, DC (tentative)	TBD			3GPP S3
Oct, 24-25	9-5	Phoenix, AZ	TBD			
Nov. 14-15	9-5	Boulder, CO	TBD			TR-45.2

12. Assignments

- AHAG to consider guidelines for interaction with 3GPP, and be prepared to discuss at the next meeting.
- Chair to determine whether a meeting summary for the conference call will be available.
- Chair to check with TIA on web site posting of contributions.
- Chair to distribute all approved liaisons by email.

13. Open Discussion

None.

14. Adjournment

The meeting was conducted in accordance with the TIA Manual and adjourned at 8:55 AM EDT on June 21, 2000.

_____

Vice Chair, Frank Quick