Title

Ad Hoc Authentication Group Meeting Summary
May 9-10, 2000 in Seattle, Washington

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 approved and sent correspondence to TR-45.2 on IP security.
- AHAG met jointly with TR45.2.2 Authentication Focus Group. A recommendation on AKA next steps was approved for submission to Committee TR-45.
- There was discussion of the relative merits of some of the ESP candidate algorithms.

1. Call to Order and Opening Remarks. TR45.AHAG met May 9, 2000 in Seattle, Washington. Frank Quick (AHAG Vice-Chair) called the meeting to order at 9:00 AM PDT, asking, "Does anyone present know of any patents, the use of which may be essential to any standards being considered by AHAG?" Certicom, Ericsson, AT&T, Lucent, Nokia, Qualcomm, CipherIT, GTE, and LG SANSYS have previously responded in the affirmative, indicating they have a letter on file with the TIA.

2. Meeting Attendance was:

1. Frank Quick (Qualcomm)	2. Dan Brown (Motorola)	3. Bob Patzer (Motorola)
4. Greg Rose (Qualcomm)	5. Bob Slocum (Ericsson)	6. Dan Robertson (Denso)
7. Jason Brown (SBC TRI)	8. Marcus Wong (Lucent)	9. David Crowe (ATT)
10. Michael Marcovici (Lucent)		

3. Meeting Agenda (2000.05.09.01, 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. CCA Security
    b. Enhanced Subscriber Authentication
    c. Enhanced Subscriber Privacy
    d. Export Issues
    e. UIM
    f. 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; Stockholm, Sweden (April, 2000)	-	Chair	5.0	
.03	Draft Correspondence to TR-45.2 on IP security	-	Chair	6.0	
.04	Relative Performance of Encryption Algorithms	-	Qualcomm	8.c	
.05	Analysis of the Joint Meeting with 3GPP S3	-	Qualcomm	8.b	
.06	SHA-based functions for AKA based ESA	**E**	Qualcomm	8.b	
.07	Options for the Use of AKA in ANSI-41 Systems	-	Qualcomm	8.b	
.08	Short term CMEA / ORYX replacements	-	Qualcomm	8.c	
.09	A Sobering History: The Break-and-Fix Cycles of SOBER	-	Lucent	8.c	
.10	SHA-based functions for AKA based ESA	**E**	Qualcomm	8.b	

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

5. The Meeting Summary.

The April 10-11, 2000 (Stockholm, Sweden) meeting summary (2000.05.09.02) was approved as modified.

Page	Line	Description
Global		Replace "TR-45.2 Enhanced Security Focus Group" with "TR-45.2.2 Authentication Focus Group".
Global		Replace "F0-F7" with "F0-F5".
1	16	Replace "tasked" with "tasks".
3	8	Refer to the March, 2000 Meeting Summary
5	19	Modify to read "KASUMI may be considered for the next revision of ESP if a subcommittee requests it".
9	29-31	Modify to read "S3 members expressed some concern about re-using IK and CK, that were created in a 3GPP network, in 3GPP2 networks."
10	9	Delete "possible".
10		Restart numbered list at item 1.

6. Correspondence

- Frank Quick (Vice-Chair) introduced contribution .03, draft correspondence to TR-45.2 on IP network security. This contribution included changes agreed to during the April, 2000 meeting. It was noted that "ANSI-41" is properly "TIA/EIA-41", but it was agreed that this change was not required in this correspondence. The correspondence was approved, and was delivered to Cheryl Blum, TR-45.2 Chair. The correspondence was assigned contribution number TR-45.2/2000.05.08.30, and was remanded to TR-45.2 WG3.

- The correspondence was discussed by TR-45.2 WG3 immediately following the joint AHAG/AFG meeting. A concern was expressed that the 3GPP2 all-IP group is not aware of the security issues described in the correspondence. It was suggested that if the correspondence text is to be used further, it should be modified to expand further on the hacker threat posed by open Internet access. The suggestion was made that the liaison be copied to 3GPP2 as well.

  The discussion also brought out the need for special-purpose gateways between an ANSI-41 IP network and the public Internet, with special security provisions required to combat the hacker threat.

  It was suggested that some of the liaison text should be incorporated in PN-4762, on IP transport. IT was suggested that the text be in an informative section entitled “security issues”.

- Michael Markovici (Lucent) stated that 3GPP SA WG3 has approved correspondence to AHAG, but these were not received before the start of this AHAG meeting. Mr. Markovici provided an informal copy of one of the liaisons.

7. Liaison Reports

7.a TR45 (Committee)

- There was no meeting of the Committee since the previous AHAG meeting. The next meeting of the Committee is in Chicago, IL, May 31-June 1, 2000.

7.b TR-45.1 (Analog)

- D. Brown (Motorola) provided the TR-45.1 liaison report. PN-4662 (IS-817 Geolocation) ballot text was approved. Next meeting will be May 15 in Quebec. There will also be a teleconference plenary meeting on May 25, to discuss PN-4662 publication.

7.c TR-45.2 (Intersystem)

- No report was received. TR-45.2 met concurrently with the AHAG in Seattle.

7.d TR-45.3 (TDMA)

- No report was received. Jason Brown (SBC TRI) reported that TR-45.3 has dropped ESA support from revision C because of time issues.

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

- Dan Brown (Motorola) provided the following report: The last TSG-A meeting took place April 10-14 in Seattle. An interim meeting was held April 26, for IOS ballot. The IOS version 4.0 ballot is nearly complete. The next meeting will be in May. Mr. Brown noted that a ballot comment to provide full support for the call history count was approved for inclusion in version 4.0. If approved by CDG, all IOS versions will support the call history count. Contributions for IOS Version 4.1 are being accepted. Text for this version should be frozen in May or June.

7.f TR-45.5 (CDMA)

- No report was received. It was stated that there is no work on ESP or ESA in progress at this time.

7.g TR-45.6 (CDPD)

- There was no report.

7.h TR-45.7 (OAM&P)

- Bob Patzer (Motorola) provided the following report: TR-45.7 has been "trying to get the attention of 3GPP2" without much success. The Subcommittee continues to have attendance problems, and has been told by TIA not to take on more work. Another year may be needed to complete the Stage 3 requirements. The Stage 1 and Stage 2 requirements have been completed but have not been balloted. The Subcommittee appears to be waiting for all stages to be completed before taking any formal action. The group is also investigating relevant management and code tools.

7.j 3GPP Security Group (S3)

- Michael Markovici (Lucent) provided the following report: Action items for SA3 and AHAG include providing a list of documents relevant to ESA; providing a list of specification areas where joint control will be needed; and to exchange meeting schedules. November is the target date for Release 2000, hence a joint meeting in September is requested.

8. Old Business

8.a CCA Security

- This Agenda item is complete, following the publication of Common Cryptographic Algorithms, Revision D, and will be closed.

8.b Enhanced Subscriber Authentication

- Greg Rose (Qualcomm) introduced contribution .06, SHA-based functions f0-f5 for AKA. This contribution includes a "family key" concept, which results from S3's compromise allowing SPs to have control over the algorithm output without changing the algorithm itself. The contents of the contribution are partially agreed with Lucent. In particular the whitening function is agreed, and has been made a GF(2**160) operation. Creation of the parameters A and B is still under discussion, but is near agreement.

  An open question is whether the function f0 should operate in output feedback or counter mode. This contribution has a counter in addition to the feedback chaining, hence it is claimed that the proofs still apply, because the addition of feedback does not affect the validity of the counter-mode proof. (In this contribution, the counter is the number of key bytes remaining to be calculated.) It was asked whether there is a possible requirement to reconstruct a RAND for lawful intercept use. The counter mode approach would allow the generation of an old RAND by saving the counter value, whereas the feedback mode could make it computationally infeasible to obtain an old RAND value.

  The AHAG needs to decide how it this document should be published. It was agreed that this issue should be raised with TR-45.

  It was agreed to send this document as a liaison to 3GPP, in fulfillment of the action item to do so, taken at the Stockholm meeting.

- Frank Quick (Qualcomm) introduced contribution .05, an analysis of the joint meeting with 3GPP. Discussion was deferred until the joint meeting with TR45.2.

- Frank Quick (Qualcomm) introduced contribution .07, options for the use of AKA in ANSI-41 networks. This contribution describes several ways to support broadcast challenge and/or SSD-like use of the keys CK and IK. Michael Markovici (Lucent) stated that CK, IK can be gotten from the UIM on power-up. This capability is present in GSM (with the key Kc) at present. This, however, contradicts statements made by Stefan Puetz during the joint meeting with 3GPP. It was agreed to check the 3GPP specifications on this subject.

- The joint meeting with TR45.2.2 AFG convened on 9-10-00 at 8 AM PDT.

- Terry Jacobson, chair of the AFG, handed out contribution 45.2.2/2000.05.08.17, liaison report for AHAG/S3 meeting. It was also agreed to discuss Qualcomm's contributions on analysis of the 3GPP joint meeting and use of AKA.

  Discussion of 45.2.2/.17: Mr. Jacobson stated that the joint meeting was a good meeting, and thanked AHAG for their participation. The joint meeting received a presentation on the structure of 3GPP, and on the organization of TR-45 and 3GPP2.

The TR-45 representatives presented the TR-45 issues, which are summarized in contribution .17. Mr Jacobson also presented a contribution on the use of global challenge for initial registration. Contribution .17 contains some proposed actions for the AHAG and TR-45.2:
Regarding revocation of the security association, it was noted that 3GPP SA3 has to request that the 3GPP core network group analyze the impact of this. Contribution .17 suggests that the TR-45 group refine the requirement. An open issue is whether the revocation of the security association can or must include a new authentication vector.

Regarding home system control of the duration of the security association: 3GPP are considering removal of the 24-hour timer in the VLR, which could make this requirement unpalatable to 3GPP. Robert Ephraim (GTE) asked why we have this requirement. Frank Quick (Qualcomm) proposed that we should decide whether we really need such control. If there is no timer, we need to decide whether HLR revocation of the security association is sufficient to meet TR-45 needs.

On reporting of success or failure of AKA, no action was proposed.

On the issue of UIM security, no action was proposed (but see below for further discussion).

On the use of SHA-1 as a hash function, it was noted that AHAG will submit information on this subject to 3GPP. Frank Quick (Qualcomm) clarified this submission is a proposed default algorithm for the non-standardized hash functions, over which SPs have complete control. For the standardized hash functions, TR-45 has agreed to use SHA-1, whereas 3GPP will use Kasumi.

On the working relationship between 3GPP and TR-45, it was noted that SA3 is willing to collaborate, and will accept specification changes as long as their security architecture and performance are not affected. It was felt that there is a need to approve the “rules of engagement” by the SA and TR-45 plenaries.

- Discussion: Robert Ephraim (GTE) stated that the UIM shell problem is a serious problem that is not adequately addressed by the 3GPP procedures, since it is not feasible to authenticate every call. Mr. Ephraim noted that GSM users rarely take UIMs out of phones, so the shell problem rarely arises. On the other hand, he expects CDMA users to move their UIMs between equipment, making them vulnerable to this attack. Michael Markovici (Lucent) suggested that AKA can be enhanced to eliminate the threat within ANSI-41 networks. Frank Quick (Qualcomm) suggested that the group recommend that TR-45 move ahead with AKA as-is for global roaming, but continue to investigate mitigation of the shell threat for ANSI-41. It was agreed to take that recommendation, noting that any enhancements would also be provided to 3GPP for their consideration. Terry Jacobson (Lucent) suggested that any carriers who disagree with the recommendation should be prepared to state their case at the TR-45 plenary. Cheryl Blum (Lucent) indicated that any changes to the

recommendation made by 45.2 in the closing plenary would be so noted. The same joint statement should be attached to the AHAG's report to TR-45. The final text of the recommendation is attached.

- After the joint meeting, Greg Rose (Qualcomm) introduced contribution .10, a revision of earlier contribution .06. This version will be sent to 3GPP. It was noted that this document may require further changes if 3GPP document 33-105 is modified.

8.c Enhanced Subscriber Privacy

- Frank Quick (Qualcomm) introduced contribution .04, which provides relative timing benchmarks for several encryption algorithms, including SSC-II, Sober-T16 and Shazam. Marcus Wong (Lucent) objected that the comparison of the algorithms cannot be accepted as valid, because details of the benchmarking were not presented. Qualcomm stated that the details were proprietary and could not be revealed. Lucent asked that the contribution be withdrawn. Qualcomm did not withdraw the contribution, but suggested that if others doubt the benchmarks they should perform their own measurements.

- Greg Rose (Qualcomm) introduced contribution .08, which provides source code for a "sliding-window" implementation of Sober for greater computational efficiency. This version was used for the benchmarking in contribution .04. The earlier reference code for Sober was not sliding-window, being written for clarity rather than speed. The reference code, however, was very inefficient in the benchmark measurements, so the sliding-window version was used for benchmarking.

- Marcus Wong (Lucent) presented contribution .09, which discusses the history of contributions on the Sober algorithm. Lucent feels it has been "doing a public service' in analyzing Sober, but it has been hard to deal with a moving target, since Qualcomm has made many changes to the algorithm. Lucent stated that Qualcomm's claims of the level of security of Sober have consistently not proved valid. Lucent stated that they do not believe Sober is complete and mature enough to be used in wireless systems.

8.d Export Issues

- There were no contributions for this Agenda item. Frank Quick (Qualcomm) noted that NSA has sent a letter to the Department of Commerce discussing the AHAG's desire to post contributions on a Web site. It is hoped that DoC will provide guidance to TIA by the TR-45 meeting at the end of May.

8.e UIM

- There were no contributions for this Agenda item.

8.f Transport Security using IP

- See Agenda Item 6.

9. New Business

None.

10. Presentations

None.

11. Tentative Schedule of Meetings

Date	Time	Location	Hotel	Rate	Cut-off	Co-Located
June 20-21	9-5	Ottawa, Canada	TBD			
July 18-19	9-5	Colorado Springs or Denver, CO	TBD			
August 15-16	9-5	Calgary, Alberta	TBD			TR-45.2
September 12-13	9-5	Washington, DC (tentative)	TBD			3GPP S3
October 24-25	9-5	Phoenix, AZ	TBD			
November 14-15	9-5	Boulder, CO	TBD			TR-45.2

12. Assignments

- Frank Quick, Vice-chair to send contribution .10 to 3GPP for their consideration.

- Frank Quick, Vice-chair to copy contribution .03 to 3GPP2 for their consideration.

13. Open Discussion

Dan Brown (Motorola) plans to make a presentation to TTC on joint TR-45/3GPP activities.

14. Adjournment

The meeting was conducted in accordance with the TIA Manual and adjourned at 2:00 PM PDT on May 10, 2000.

_____

Vice Chair, Frank Quick

TR-45 AHAG & TR-45.2.2 Authentication Focus Group
3GPP AKA Recommendation

The TR-45 AHAG and the TR-45.2.2 Authentication Focus Group met with the 3GPP TSG SA WG3 (S3) in Stockholm on April 12, 2000. As a result of that meeting and subsequent deliberations by TR-45.2 and the TR-45-AHAG, the following actions are recommended:

Enhanced Subscriber Authentication (ESA)

TR-45.2 and the TR-45 AHAG proceed with the development of AKA-based ESA.

TR-45.2 and the TR-45 AHAG investigate enhancements to AKA operation that would mitigate the security threat posed by "rogue" mobile equipment (i.e., MS shell).

- The rogue MS shell could retain Cipher Key (CK), Integrity Key (IK) and subscriber identity information after an R-UIM is removed. The rogue MS shell can obtain service fraudulently by using this information, or it could distribute this information.

TR-45.2 and the TR-45 AHAG present the enhancements to the AKA operation to 3GPP for their consideration

Working Relationship Between TR-45 and 3GPP S3

TR-45.2 and the TR-45 AHAG develop a proposed set of guidelines for the working relationship between TR-45 and 3GPP S3. The set of guidelines will include change control, responsibilities, communications, etc.

Forward the proposed guidelines to 3GPP S3 for review and concurrence.

Present the guidelines agreed to by 3GPP S3 and TR-45 AHAG/TR-45.2 for concurrence to TR-45 and 3GPP SA respectively.