2021-04-08

Minutes of the first teleconference for Authentication enhancements

Active participants: Apple, China Mobile, Huawei, Nokia, Qualcomm, Thales, Vodafone, Ericsson (rapporteur)

Agenda for this teleconference

a. Discuss the way forward for May and August meetings

b. Discuss input documents with respect to solution evaluations, comparison tables and conclusions. Please disseminate any input documents at least 1 day earlier.

- Input from Nokia

c. Go through the comparison tables in clause 7 and discuss the existing text.

d. AoB

--------------------------------------------------------------------------

--------------------------------------------------------------------------

Agenda item (a)

---

We discussed the plan of action below for the May and August meetings.

There was no objection from the participants about the plan.

[Nokia] commented that point #5 is premature since we don't have any conclusion yet.

[Ericsson] responded that this is true but the WID could only mention that the objectives to be covered are related to the concluded key issues and solutions. In any case we case see the progress of teleconferences and adjust the draft WID accordingly.

[China Mobile] asked about the timing of Rel-17

[Ericsson] responded that we would need to conclude the study and agree on a WID during the August meeting at the latest. Otherwise the CT groups will not have time to specify stage 3 specifications. Although the SA3 chair proposed a placeholder meeting in July, Ericsson would like to avoid having a meeting in July and try to conclude as many key issues as possible in May.

Plan

1) Participants are discouraged bringing new key issues and new solutions towards the SA3#103-e (May) and SA3#104 (August) meeting

2) Minor updates to the existing key issues, existing solutions and existing solution evaluations are expected in May and no updates in key issues or solutions are expected in August. If a solution does not have an evaluation at all, an evaluation contribution should be targeted for the May meeting.

3) Structure for comparison of solutions and assessing key issue importance is in place (clause 7). Clause 7 is also the placeholder for conclusions. Content needs to be filled in. Focus on the May meeting to converge on the content of clause 7 i.e. comparison tables and conclusions.

4) Time between March and May: Offline teleconference(s) in between meetings to converge on the solution comparison, the key issue importance and conclusions. For this purpose we could have ideally two conference call meetings, one in the beginning and one towards the end of April. Companies are expected to bring draft SA3#103-e contributions for discussion during these meetings. I propose to have one doodle poll for April and we can see if one or two conference calls are feasible. The doodle poll link is here: https://doodle.com/poll/9sv2tngebnqhzsr3?utm\_source=poll&utm\_medium=link

5) The rapporteur may bring a draft WID for the normative work in the May meeting to be discussed. If we converge already in May, the WID may be approved then.

6) The focus on the August meeting is to agree on a WID and/or possibly initial draft CR(s).

7) Time between June and August: Offline teleconference(s) or e-mail discussion on a WID and initial draft CR(s).

Agenda item (b)

---

There was only one input discussion paper from Nokia with respect to the evaluation of solution #4.1

[Nokia] presented the discussion paper

Discussion among the group started.

[Nokia] stated in the discussion paper, clause 3.4 that the MAC-S introduction to the calculation of AK introduces "...a new attack against UDM, as the attacker could influence the generation of AK in UDM". The paper also states the XMAC-S and MAC-S comparison is meaningless.

[Vodafone] commented that the statement in clause 3.4 that "the UDM comparison is meaningless" is not fair. The comparison takes place and it will fail if an attacker modifies MAC-S.

[Qualcomm] To say that this problem exists with the addition of the MAC-S in the calculation of AK is not correct. Why would the attacker go in such lengths to make the UE fail ?This is not a new attack, it exists with the current behaviour if one modifies the AUTS.

[Nokia] The attack scenario is a MiTM between the UE and the UDM can change the MAC-S and therefore changes the AK. The AK is no longer the same as it was intended.

[Ericsson] In Observation1 it is implied that the attacker can control the generation of AK in the UDM. Yes the attacker can modify the AK but not in a deterministic way. As a result it cannot really control the AK in the UDM.

[Qualcomm] commented that with the current specification an attacker can change AK in a known way. Why does changing the AK in an unknown way is an advantage for the attacker ?

[Nokia] The comparison is meaningless because AK is not dependable

[Vodafone] The UDM comparison is meaningful

[Huawei] supports Nokia. The MAC-S is used as input and output for verification

[Samsung] supports Nokia

[Nokia] what is the benefit of sol #4.1 ?

[Qualcomm] Sol. 4.1 destroys the relationship of the sequence number.

[Nokia] SAGE said that there is a leakage of AK

[Vodafone] this is not a significant concern

[China Mobile] Can this attack apply to the normal AKA. Agree with Vodafone that there is no new threat here.

[Nokia] commented that if MAC-S verification fails the UDM behaviour is undefined. It is worth investigating.

[Nokia] commented that they got the feedback for the discussion paper and they will make the necessary adjustments

Agenda item (c)

---

The rapporteur went through clauses 6.0, 7.0 and the comparison tables and asked companies to bring input documents for their positions on the comparison tables and conclusions towards the next teleconference on April 27.

The rapporteur also said that he will bring a v0.11.1 version of the TR as a baseline with editorial corrections and removal of Editor's Notes (EN)

[Thales] Solutions have ENs in them which are important for their evaluations and the study conclusions. They should not be removed.

[Ericsson] clarified that these ENs will not be removed. The ENs that have editorial nature will be removed.

[SA3 chair] maybe it is better to bring a pCR with the whole TR in it. A new version v0.11.1 may confuse people. Moreover editorial corrections could be applied after the TR is approved via CRs if there is very little time.

[Ericsson] will consider the best option for editorial corrections for the TR.