**Offline Call #2- Rel-19 FS\_eZTS Draft Contribution Discussions - SA3#115 preparation**

# 1. Call Information

**Date:** 06 February 2024, Tuesday

**Time:** 14:30-16:00 CET

**Venue:** Microsoft Team Meeting (Online)

**Organizer:** Sheeba Backia Mary B.

# 2. Call Participants:

|  |  |
| --- | --- |
| Name | Company |
| Achari Kakinada | Charter Communications |
| Adrian Buckley | MITRE |
| Alexander Engström | NDRE |
| Andreas Kunz | Lenovo |
| Ben Lorenz | SZ31 | BSI |
| Candace Carducci | JHU/APL |
| Chaitanya Aggarwal | Nokia |
| David Gabay | MITRE |
| David Hasselquist | Sectra Communications AB |
| DJEMAI Tanissia | Irt Saint Exupéry |
| Dusty Hoffpauir | Charter Communications |
| Elizabeth Koser | US NSA |
| Francois Ennesser | Huawei |
| German Peinado | Nokia |
| Noamen | Huawei |
| Imran Saleem | Huawei |
| Jinsook - DISH | DISH |
| John Ing | PSC |
| Lee, Xiaoyang | CISA ECD |
| LOUSHINE, MIKE | AT&T |
| Martin Goldberg | US NSA |
| Michael Bilca | Trideaworks |
| Parsel, Mike | T-Mobile |
| Robert Edwards | MATRIXX |
| Rong wu-Huawei | Huawei |
| Saurabh Khare | Nokia |
| Sheeba Baskaran | Lenovo (Presenter) |
| Tao Wan | CableLabs |
| Tim Woodward | Motorola Solutions |
| Vlasios Tsiatsis | Ericsson |
| Warren Kim | JHU/APL |
| Zander Lei | Huawei |
| ZTE-Peilin | ZTE |

# 3. Agenda and Minutes

|  |  |  |
| --- | --- | --- |
| **No.** | **Agenda** | **Meeting Minutes** |
| 1 | TR 33.794 Draft Skeleton overview (Latest version-r1) | Sheeba presented the draft TR 33.794 skeleton.  Vlasios: Not clear: based on the skeleton structure we have the concept of threat and related data and the concept of use case scenario and KI and solutions; how are those all related? How do we use the use cases and threats e.g. for evaluating solutions? In the HONTRA study we had this and it was not clear; what are your thoughts about it, one use case has multiple threats and related to one piece of data?  Sheeba: Clause 5.1 helps to collect threat and relevant data, its related to WT1; For WT1, we don’t need to do another KI as it is stable in Rel.18 TR 33.894; we can just cite that KI here in TR 33.794; In Clause 5.1, if we identify potential data to be exposed to operator’s security function, then we need one solution that helps to collect and provide the identified data to the operator’s security function and to fetch the results (if any). Here solution from TR 33.894 can be used as baseline as it was agreed after several revision (over several meetings) to address all the involved stakeholders’ feedback. Of course, if companies would like to refine further, we can work on it to consolidate. This can save some time in Rel.19. On WT2 we have studied the KI but we couldn’t agree any in Rel.18; In the last offline call#1 there was the suggestion to first study the potential scenario/usecase in SBI that gets beneficial with the dynamic enforcement (when there is a result available from the security function e.g., if any threat or attack is identified); So clause 5.2 helps to collect such scenarios where we can discuss and agree what is that use case that benefit from the dynamic access control; with the agreed use case as a next step we can come up solid KI for WT2. Then we also need to discuss and agree potential solution(s) for WT2 KI;  Noamen: Clauses and title of Clauses: 5.1 is security evaluation and monitoring; this is more to find use cases; 5.1.x title does not need to be threat; it’s a use case;  Sheeba: Currently its formulated based on the study objectives of WT1. your suggestion is to name it use case?  Noamen: Yes;  Sheeba: WT1 is about identifying threats and attacks.  Noamen: Not questioning the scope of the objective; only the title; in 5.1.x.2 there are 2 subclauses; they seem redundant; do you need this?  Sheeba: There will be the main data to be collected; the additional data can be like who is the originator of the data, time etc.; e.g., contextual data or secondary information may form the additional data;  Noamen: No strong opinion;  Warren: 5.1.2 if we have a 2nd threat where does it go?  Sheeba: It should be 5.1.X like initial version or the header need to have a suffice with X to add more threats subclause, will take care of the clause number in the revision.  Tao: 5.2 security mechanism; I expect multiple security mechanisms?  Sheeba: It is exclusive for WT2, for use case identification;  Noamen: It should be plural what Tao thinks;  Sheeba: Yes of course; you can come up with any number of use cases (if you identify relevant ones).  Tao: 5.1 is like a mini TR?  Sheeba: We try to identify the related data;  Tao: what is 5.1.Y?  Sheeba: If we see WT1, it says we have to identify the threats and attacks, so we will identify the data in 5.1.X; then in 5.1.Y we discuss and agree on security considerations for a solution that can help to securely collect and provide the identified data to the operator’s security function;  Noamen: The level seems to be wrong, it’s the same one as the threat X; this is not the template;  Tao: yes, it should be 5.x.2 or so  Noamen: is this related to the threat?  Sheeba: it should be the solution to the threat….  Noamen: then it should be under the 5.1.x  Tao agrees to Noamen;  Tao: if you have two threats then two procedures?  Sheeba: No, for all the identified data, there will be one common procedure to collect, and provide the identified data to the operator’s security function. No, it should be one procedure (that’s why it is listed as 5.1.2).  Noamen: its like a group clause for the threats; its becoming too complex;  Sheeba: Yes, this is to accommodate having a descriptive section for the threats and data identification process like suggested in the offline call#1.  Vlasios: Concept model; we have to record all threats and for each threat multiple data points; for each data point we identify which is exposed and which one needs to be exposed as new ones and the security procedures are related to one or multiple? But you answered its for multiple ones; are we looking for existing procedures or new types of solutions to expose the data?  Sheeba: Yes exactly. Don’t want to close the doors but very limited time we have; we should reuse what we have discussed and agreed in R18 i.e., that KI#1 solution can be used as baseline and if companies have refinement suggestion of course we can refine to reach an agreeable version. But we need to agree one solution only for WT1.  Vlasios: We should find other types of procedures;  Sheeba: We should not diverge largely; we discussed it two years and refined the solution proposal to reach the current state in Rel18 closure; using it as baseline will save time and specifically avoid redoing all the work we did in Rel.18; Required refinements can be considered.  Tao: Already provided the comments;  German: Chapter 5 in my view should support chapter 6 and 7; not the proper place to discuss solutions; we are in chapter 5; instead of threat put use cases; agrees to Noamen; proposes a similar structure in 5.1 and 5.2; we need to prepare the ground for the KIs and solutions and not to diverge; not easy to follow and to make contributions in each section is difficult; propose to simplify and not to have such a granularity; proposes use case, description and scope; very easy; solutions and KIs we will treat afterwards; security procedures happen afterwards;  Sheeba: For WT1, what’s your suggestion? Should we go into starting a completely new solution discussion?  German: No, proposal to take the existing solution as baseline is good; supports it; more the format to make it easy to read;  Noamen: Notice the EN under 5.1.Y now: its misleading but now I’m understanding the intention; there was no agreement in the TR;  Sheeba: There was agreed KI#1, solution and conclusion in TR 33.894, that is what is referred here like also stated in Rel.19 WT1 objectives;  Noamen: This is not my understanding of the outcome of the previous study;  Sheeba: That’s what we clarified here in the Rel.19 WT1 objective to reuse the progress from old TR as baseline; the solution is in line with the tenet evaluation; this is to facilitate to use the time effectively; any company can contribute, and it will be taken into account;  Noamen: This is about the solution in the TR; this is not clear; it is not clear that we only need to consider this solution;  Sheeba: That’s the one which has been discussed for several meetings, refined to address all the feedback received and so asking to use that as baseline like stated in the WT1 objective.  Vlasios: Question on the use case; if we rephrase 5.1.x to use case; then one use case has multiple threats and each threat has multiple data points?  Sheeba: It is better to come-up with threat and related data points per usecase (e.g., event or scenario). To avoid being complex.  Vlasios: It’s just reflected in the structure;  Sheeba: You can explain this in the threat details;  Tao: remove the X and replace with 1.  Sheeba: I will push a rev2 in the 3gpp shared space, feel free to comment. |
| 2 | Scope Draft | Sheeba presented the scope input.  Tao: just copied from the SID? Then it should be fine;  Vlasios: not sure the first sentence is needed;  Sheeba: The bullets are same as objectives. The fine sentence is a kind of limited introduction. |
| 3 | Introduction Draft | Sheeba presented the introduction input.  Tao: proposes for offline discussion. |
| 4 | Security Assumptions Draft | Sheeba presented the security assumptions input.  Tao: background, what do you assume here? This is just a description of background information; first paragraph on security function; you describe what’s there;  Sheeba: It’s based on the tenet 5 evaluation;  Tao: the section is about the security assumptions; what do you assume here?  Sheeba: The assumption is the security function will do security evaluation and monitoring and it’s a trusted entity; we used the general assumption of using the NEF in Rel.18; even its external to the 3GPP domain it is a trusted function in the operator domain so we do not need to use NEF; Made it clear and simple with these security assumptions.  Tao: This is scope constraints.  Sheeba: No, this is trust assumption;  Achari: does it include new NWDAF data types for the collection for the specific purpose?  Sheeba: only minimal new aspects for the SBI services like specific service operations with input/output; the data collection the NWDAF uses OAM based data collection  Achari: the NWDAF will not collect the new data types?  Sheeba: Like for analytics the NWDF uses either direct data collection or via OAM, here later approach is considered to be light weight; the new IEs exposed to the security function may be new.  Achari: Yes there is a chance of new data types;  Noamen: The assumption is not clear; the NWDAF is somehow involved but its not clear; you make the NWDAF as a central element; its yet another NF and yet target of the same threats; the assumption is not clear; what is exactly assumed here;  Sheeba: The particular three lines on the NWDAF is not directly coming for R19; what we agreed in the R18 after several meeting discussions is considered and listed here; yes NWDAF is another NF; the attempt that one NF maliciously sending data to another NF will not mean all NWDAF is compromised throughout the network all the time; The NF deployment will be distributed in nature ranging from few deployed in locations (e.g., geographical locations or hosted platform/data center) which are considered bit more secure over the rest deployed in locations which are bit less reliable; currently different instances of NWDAFs are serving different functionalities over the basic analytics task; based on operator policy the operator can decide and deploy the NWDAF with the WT1 specific functionalities;  Noamen: My comment is about what is written here and your reply is what we did in the past; you have a solution in your mind but this clause is about security assumptions; if all data needs to go through the NWDAF then it needs to be written here; it needs to be clear;  Sheeba: It is not about having solution in mind. I am trying to reuse R18 progress as baseline and use as security assumptions in R19, so that we can avoid much divergence and progress with this limited time. This is not written in hard stone; tries to clarify; based on the work in R18; if you want to refine things just push revision on the shared space;  Tao: Rewrite to clarify the assumptions, like no new function etc., what you wrote her doesn’t reflect what you say now; the clarifications will help the other companies;  Sheeba: Tried to keep limited text. But will push a revision. Feel free to revise the uploaded version; |
| 5 | WT-1 Data to be collected (2 Docs) – Draft  • Doc 1 – NF crash attempt with malformed message  • Doc 2 – NF DoS with Service request flooding attempt | • Doc 1 – NF crash attempt with malformed message:  Sheeba presented the Doc 1  Tao: title should not be crash; maybe just malformed message for the NF;  Sheeba: Okay, will write it in the heading;  Tao: Change the clause numbers based on the skeleton changes;  Sheeba: Consider it as a minimal draft; will push a revision, then feel free to update;  Vlasios: Is this mainly about fuzz tests of NFs? Who is going to collect it? The NF itself will report it crashed? How is it related to fuzz test in SCAS?  Tao: Fuzz test is different; this is receiving something malformed and it may crash;  Sheeba: Thought same thing: name is misguiding; It is potential attempt to attack e.g., to make a NF crash by sending a malformed message; the NF crash is just one kind of thing; the intension can be anything, like to crash/hijacking the NF; If a malformed message is received, in this event, the event related data should be collected from the NF which received the malformed message and the event related data should be provided to the operator security function; let the security function decide if it’s an attack or not. It is not about letting the NF to crash; if its just discarded, then we will not know attack attempt and the threat surface;  Vlasios: the title should not say crash; some of it may be covered by fuzz tests;  Sheeba: Okay, will fix it;  Candace: Can you expand on the word crash and what are the impacts and put that in the details itself;  Sheeba: There are lot many aspects we can see on the NF attacks like added in reference but tried to cover with limited text in TR not to sound negative on the current system. So refrained from writing in detail as we document in the TR to not impact the belief in things. But will see how to articulate.  Noamen: The technical proposal or impact in the new logic in the NF instead of dismissing it you send it to the NWDAF?  Sheeba: Yes, sending to the operator security function with the assistance of NWDAF.  Noamen: If this is going to the standard it needs to be clear how the NF will act on it; from security perspective this is not a good approach; if you receive a message with malicious intend that you send messages; this has impact on NFs;  Sheeba: The logs you currently do, we expect that you collect the data, when the incident happens- only difference is here we say exactly what event need to be considered to be collected in standard way; what is your suggestion when a malformed packet is received; if its dropped then this does not help to understand why its happening and from where its happening;  Noamen: messages that doesn’t pass certain checks will be silently dropped; some events are logged and stored; now you want to propagate that information;  Sheeba: for e.g., it can be a transparent container; its given to the right security function; if you see NWDAF specs, it collects number of data; SBI message violations can be also provided to the NWDAF; the NWDAF don’t touch it and just assists the security function to get the data;  Tao: This particular clause just talks about what data to be collected; the mechanism to expose to the security function should be the same for all data; just revise to clarify;  Sheeba: A massive Number of malformed messages are coming in; right from the first ones the operators security function will know, if the data is collected and provided right at the first incident itself;  Tao: Every time you send something it can be misused; this is a threat to the entire monitoring system itself;  German: Comment to the SCAS document in which we had a test case on the security event logging; we have several event types to log; this is a new thing; the SCAS is more access control to the NF; the functionality of security logs should be there; the assumption is which types of events we would like to treat and instruct and not necessarily security events; you don’t collect security events but also KPIs from different characters, we need to make a reference to the SCAS documents or is it completely in parallel? It has to be clear what is the add on here;  Vlasios: This malformed in the context of SCAS is a assurance test; it will have malformed input tests in SCAS to test that the NF is dropping and not crashing; this was the main comment; if we collect data from malformed input then its different from SCAS; the SCAS is just ensuring that the NF is not crashing with the malformed input; two different things;  German: What is malformed, a parsing error or a protocol error? Malformed has a lot of meanings; probably convenient to go ahead with it and to have a definition what is a malformed packet;  Vlasios: yes, we need to state a clear definition for this malformed message.  • Doc 2 – NF DoS with Service request flooding attempt:  Sheeba presented the Doc 2  Tao: those denial of service can be done without involving the NF, can be other ways to do it;  Sheeba: If no other comments, in the interest of time, let us rush to Revised SID. |
| 6. | Revised SID (Scope to include RAN) | Vlasios presented the Revised SID proposal  Tao: What do you expect from this? New requirement for RAN in the TS?  Vlasios: The level of fulfillment of the tenets evaluations for the RAN;  Tao: No TS impact then?  Vlasios: For each tenet we try to evaluate what are the resources and what is the authentication and the level of fulfillment;  Tao: Do you consider O-RAN?  Vlasios: The RAN nodes could have interfaces outwards to the core and inwards to the ORAN nodes, we only take care of 3GPP like CU/DU interfaces.  Noamen: What do you expect to do with it; you cannot do O-RAN and 3GPP RAN here; they are not on the same principles; this is not supposed to be dynamic; this is not applicable for the 3GPP core;  Vlasios: Inside the CU/DU the interfaces are specified by 3GPP;  Noamen: Bring a discussion paper on the intention; if this is about communication security, we specified that; it would be good to elaborate this more; Now revising and extending the scope of the study is not a good approach; good to clarify what you expect out of it; |
| 7. | Any other discussions  General Plan | Sheeba: For the upcoming meeting let us assume we have 45 mins time slot for now. We need to have good preparation for WT1 and WT2 to best utilize the 45mins slot. If we have a smaller number of contributions, then still 45 mins slot will be considered as consumed. If more of contributions comes in, we will consider the merged ones to be opened for discussion.  We have very limited TUs over-all, so for Athens meeting at least we should be able to progress with WT1 and WT2 for the aspects discussed. Contributions are welcome.    Tentative Plan |
| Call is closed | | |