**Offline Call #3 - SA3#115-Adhoc-e FS\_eZTS Preparations**

# 1. Call Information

**Date:** 19 March 2024, Tuesday

**Time:** 15:00-16:30 CET

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

**Organizer:** Rapporteur, Lenovo (Sheeba Backia Mary Baskaran)

# 2. Call Participants:

|  |  |
| --- | --- |
| **Name** | **Company** |
| Andreas Kunz | Lenovo |
| Candace Carducci | JHU/APL |
| Christine Jost | Ericsson |
| David Gabay | MITRE |
| DJEMAI Tanissia | Irt Saint Exupéry |
| Dr. DJ Shyy | MITRE |
| Ferhat Karakoc | Ericsson |
| Francois Ennesser | Huawei |
| Greg Schumacher | Peraton Labs |
| Grewal, Rajpreet | NTIA |
| Noamen | Huawei |
| Imran Saleem | Huawei |
| John Ing | PSC |
| LOUSHINE, MIKE | AT&T |
| Parsel, Mike | T-Mobile |
| Peilin | ZTE |
| Rakshesh P Bhatt (Nokia) | Nokia |
| Robert Edwards | Matrixx |
| Sheeba Baskaran | Lenovo |
| Vlasios Tsiatsis | Ericsson |

# 3. Agenda and Minutes

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **No.** | **Agenda** | **Draft Tdoc for discussion** | | **Meeting Minutes** |
| 1 | Security Assumptions (To be stable)  🡪 ENs to be resolved & additional assumption(s) if any to be treated | 1.1 S3-24aaaa\_Resolving EN on data exposure | | Sheeba (Lenovo) presented the contribution.  David (MITRE): Natural way forward, NWDAF does it already; proposed wording “exposing” instead “provide”  Greg (Peraton Labs): OAM already accessed by NWDAF; the OAM does the ultimate analysis. We assume the security functions of some part of overall OAM structure then part of NWDAF providing input to the OAM? A little bit backwards;  Sheeba (Lenovo): if we want the OAM to do security analytics; this is going beyond what we discussed in the Rel-18; we are in the closure of the 5G-A features and integrating all these security features in a standardized way may not be feasible in one release; we have to utilize the operators functions external to the 3GPP networks like SIEM tools etc to keep the solution light weight for the 5G advanced feature; and those can be reused for the 5G-A features, may be in 6G the actual security evaluation/monitoring functions can be done by OAM or any function inside the 3GPP network;  Greg (Peraton Labs): Seems confusing; if you expose the NWDAF, is that also duplicate to exposing the NWDAF to OAM?  Sheeba (Lenovo): We don’t need to define completely new features for collection or exposure, instead we can try to reuse the existing features maximum and can extend minimal things where needed;  Greg (Peraton Labs): but additions to NWDAF, or can it be normal NWDAF exposure?  Sheeba (Lenovo): it can be a normal exposure; SA5 defined the means to subscribe and get the data for OAM based data collection; we can reuse and cite those references for any OAM based operations;  Rakshesh (Nokia): support to change the word from provide to expose.  Greg (Peraton Labs): probably OK  Vlasios (Ericsson): hesitant with the sentence that NWDAF is the suitable function. We also said in the use cases of the related data that NFs are providing this information and possible indicators of compromise and security breaches; with this assumption do we conclude that the NWDAF is doing all the aggregation to the OAM? Do we reach that conclusion?  Sheeba (Lenovo): For example, let us pick up one existing data like performance data; in the NWDAF to do analytics, the NWDAF gets performance data from OAM, where there are many metrics that OAM generates as part of performance data; then it provides them to the NWDAF; on SA3 level we only identify the data needed to identity the threat and NWDAF can fetch those data from OAM like in the existing system; then any additional metrics for the identified data, like SA5 things they can discuss; the main data is identified from SA3; SA5 may come up with additional metrics if any needed;  Vlasios: the data flow; the use case we say the NFs are generating the information and sending them to the security function; now we are concluding and we send everything to the NWDAF and to the OAM; not sure here about the data flow;  Sheeba (Lenovo): we will identify the data to be provided to the security function; we can just reuse the OAM data collection;  Vlasios: this is when the NWDAF is under attack?  Sheeba: this is when it happens in any NF; OAM collects data based on subscription from NWDAF like in existing system; then NWDAF can provide it to the operator’s security function. The only difference from the existing system is that, security analytics job is offloaded to the operators security function; Rest all is same like the flow in existing system.  Vlasios: everything is sent to OAM? And from OAM the NWDAF will take the data?  David (MITRE): there is a misunderstanding; the NWDAF will collect from the NF and pass to the OAM:  Sheeba (Lenovo): no no; in Rel-18 we discussed both options; (i) NWDAF collects directly from NF and (ii) NWDAF collects from NF via OAM; there is feedback to not impact all NF exposure services, so then we just moved forward with (ii) i.e., NWDAF collects data from NF via OAM (i.e., OAM based data collection method); Fine to consider now NF based data collection if all involved stake holders are fine with that option; Christine do you remember the discussions in R18 eNA study, where it was asked not to impact the event exposure services of NF, so that part was removed and only OAM based data collection was retained finally. So refrained from reopening that discussions.  Christine (Ericsson): do not remember such an agreement.  Sheeba (Lenovo): Think the SA3 mail reflector will have those discussions which happened during eNA Rel.18 study. Anyway, it okay to go use any of these two options, if all are fine.  Rakshesh (Nokia): the way Rel-18 functionality work: performance data example, it goes to OAM and NWDAF subscribes to the relevant information it needs and provides the analytics; it falls in line; SA5 would be also in line; if NF provides security information it goes to OAM; we discuss data exposure for continuous monitoring; NF to OAM and NWDAF takes what it needs for security related analytics;  Sheeba (Lenovo): Yes exactly. OAM collecting data from the NF is not shown in the figure, but it happens as described in TS 23.288; aligned with Rakshesh. Vlasios, are you fine to collect directly or indirectly.  Vlasios: needs to think about it; the data flow is not clear;  Sheeba (Lenovo): the data collection part is there; fine either way for the solution discussions;  Christine (Ericsson): comment on Rel-18 and eNA: specific security related events and logs, this is a very different type of data, not done today in 23.288; wants to clarify here, it leads to misunderstanding here;  Sheeba (Lenovo): Sure we can add clarifications. OAM data collection is preferred only based on Rel.18 discussions. But if involved companies want to go with NF based data collection it can be considered; That’s okay.  Vlasios (Ericsson): this model will be subject to the conclusions to solutions? Will it be in the assumption or part of the conclusions for the solutions?  Sheeba (Lenovo): this is to facilitate the discussion on the initial building blocks before jumping into the solutions; this can act as a fundamentals to be used as baseline to bring some convergence. If not, we may end up with much diverse things and consensus will be difficult during conclusion phase.  Vlasios (Ericsson): okay, thanks  Greg (Peraton Labs): it is worth to clarify whether this choice is either or, or both to be supported? One possibility of the choice is operator policy then you provide the choice to the operator which way to go; if supporting both you need to clarify whether they can be operational in the same network.  Sheeba (Lenovo): depending on the type of data then need to be collected, there may be done differently; we can give the flexibility to the operator; we can have a note on this to say it is upto operator policy like suggested by Greg; |
| 1.2 S3-24bbbb\_Resolving EN on dynamic security policy enforcement | | Sheeba (Lenovo) presented the contribution.  No comments. |
| 2 | Use cases for security evaluation and monitoring (To be stable)  🡪 4 existing usecases (ENs to be resolved) | 2.1 S3-24cccc\_Updates to Malformed message usecase | | Sheeba (Lenovo) presented the contribution.  Greg (Peraton Labs): For malformed message details can be done by CT groups; the CT groups will define what a malformed message is; the concern about recording the malformed messages because it may be that the aspects that its malformed is to utilize some internal vulnerability so we want to say the analysis of the malformed message needs to be done in some isolated fashion; you don’t want to apply a normal processing; the vulnerability may be else exploited;  Sheeba (Lenovo): kind of best practice to be stated in a note. We also can add a NOTE for the latter comment here to say, the further details on malformed message can be upto the CT. |
| 2.2 S3-24dddd\_Updates to Massive number of SBI messages | | Sheeba (Lenovo) presented the contribution.  Greg: context of overload control; this use case, is this a service attack coming from overload control? This is distinguishing overload control of legal traffic and DoS traffic?  Sheeba (Lenovo): we have overload control in place; whether this is a security threat that is ‘intentionally done or not’ is not done currently; we have a placeholder for this security threat discussion here;  Greg (Peraton Labs): we haven’t talked about max numbers; the NWDAF would determine whether it’s a DoS attack or a non DoS overload to trigger DoS mitigation or not;  Sheeba (Lenovo): Currently NWDAF support DDoS identification for UE but not for NF triggered scenarios. If you have refinement suggestions, we can incorporate it.  Greg (Peraton Labs): Will take a look into it to provide some rewording.  Christine (Ericsson): Jumping for the previous document, on the last EN: it is very difficult to decide which data to expose; it requires a lot of thinking; for the malformed messages; the actual message, the event or the message itself needed to be decided further? Very difficult problem; we cannot decide on the 2nd meeting;  Sheeba (Lenovo): two category you are thinking; the actual message or about the message the event;  Christine (Ericsson): only examples what you could do, but it’s a wide scope what is possible to do right?;  Sheeba (Lenovo): if we have pending ENs how can we move on with KI and solutions?  Christine (Ericsson): that would be more the solution discussion?  Sheeba (Lenovo): would a note help to clarify the same like you stated now for. E.g., we can add a note that further details of data to be exposed related to malformed message scenario is upto the solution discussions?  Christine (Ericsson): can’t say now, need to think; |
| 3 | Security mechanism for dynamic policy enforcement (To be stable)  🡪 1 existing usecase (EN to be resolved) | 3.1 S3-24eeee\_Updates to Access control decision enhancement usecase | | Sheeba (Lenovo) presented the contribution.  Greg (Peraton Labs): proposal to talk about the malicious behavior to address the issue of the description;  Sheeba (Lenovo): Okay will reword like suggested by Greg. |
| 4 | KI#1 Security Requirement (To be Stable) | 4.1 S3-24ffff\_Updates to KI#1 | | Sheeba (Lenovo) presented the contribution.  Christine (Ericsson): companies that want to provide solutions know what solutions are expected from this requirement? What do we expect?  Sheeba (Lenovo): companies can share their solutions views; for the x nr of data we identify we say how they can be collected from the network and provided to the operator’s security function;  Christine (Ericsson): Vlasios had a question on the data flow; the same type of solution here? Where will the data flow be discussed?  Sheeba (Lenovo): Sure in the solutions you can cover the details on the data flow, that is fine; to clause 7 everyone can bring the solution proposal;  Christine (Ericsson): it makes more sense to be more specific on the solution we want to see; the floor is too open; we don’t know where we are heading;  Sheeba (Lenovo): For the security requirement is bit solution agnostic as it should not be specific to any type of solution. But if you think, it is super open ended, we can add little more clarity with additional security requirements to capture your suggestions like ‘on data flow’.  Greg (Peraton Labs): the notes are requirements for the solutions; we want to identify the elements and aspects the solutions needs to provide; the solutions need to do this and that; these can be recast as security requirements;  Sheeba (Lenovo): Sure, will update the document. |
| 5 | New KI(s) (if any) | 5.1 S3-24gggg\_New KI on dynamic security policy enforcement | | Sheeba (Lenovo) presented the contribution.  David (MITRE): for each use cases and threat use cases we have a separate KI for those kind of scenarios?  Sheeba (Lenovo): This KI is drafted exclusively for usecase 1 related to objective 2. We do not have any other usecase so far discussed or added in the TR for objective 2.  David (MITRE): Okay it is clear with access control scenarios example use case; what about DDos or DoS? You have a different KI for it;  Sheeba (Lenovo): Showed TR 33.794 and clarified. The DDoS/DoS usecases are scenario where we need to identify the potential data to consider for enable security evaluation and monitoring. For this we don’t need different KIs. The current KI#1 will be the placeholder to cover all the data related usecases to be considered for identification, collection, and exposure to operator’s security function. One the other side, for 5.2. only this one use case agreed so far; if new use case comes in the future meeting then we can see whether the current KI applies to the use case else we need a new KI; we have only very limited time;  David: for 5.2 scenarios?  Sheeba (Lenovo): yes for 5.2 if new usecase comes, new KI may be needed which we cannot say at this point of time, without knowing the usecase, for 5.1 is for data identification, that’s a different thing;  Greg (Peraton Labs): the first security requirement can be related to KI#1, but not KI#2; This is the monitoring part and not of the control; proposes to provide changes to take the NF out of the service chain and prevent it to spread the compromised elsewhere; this is not clear here; this is about spreading of the compromised; not about the taking out of the service;  Mike (T-Mobile): is this really about we detect something on the NF and a granular control; the NF is still 90% OK; not sure what we are trying to do here; thought we try to shoot it down; looks like we keep it running here;  Greg (Peraton Labs): that’s why we need to work on the language; we need to isolate it from the service chain;  Mike (T-Mobile): is that the misbehaving part only? Maximum utilization of NF is preferred.  Sheeba (Lenovo): those level of granularity like 90% misbehaving or what percentage means is part of the solution; like a range of results like 50%; it is possible to still keep it running; if the results are binary, like compromised or not; then still is it considered in offering services is part of the solutions; we can work on the KI to clarify further (like having max utilization as suggested by Mike) and leave the type of solution upto the solution discussions;  Mike (T-Mobile): just needs a better wording;  Sheeba (Lenovo): utilizing the NF to the most is the best thing to do.  Greg (Peraton Labs): take the NF offline until its repaired or replaced; that’s obviously the next step; isolate it and remove it, restart it etc.  Sheeba (Lenovo): different things that can be done, sure we can discuss them as part of the solution phase; |
| 6 | New additional usecase(s) (if any) for clause 5.1 or 5.2 | No Tdocs!!! | | Not applicable. |
| 7 | Any other business | Time Plan?! | | Sheeba (Lenovo) presented the over-all time plan in a quick nutshell as the time was already passed by 3mins.    In 2nd meeting we should complete the KI, only then we will have atleast 2 meeting cycles to discuss and stabilize the solutions. Then only we will be able to cleanup and complete the study in the last meeting of study phase.  So suggest offline discussions and refinement along with the involved companies to ensure the progress.  Mike (T-Mobile): proposes serious offline discussions; |
|  | | | Call is closed | |