**Offline Call #1- Rel-19 eZTS Kick-off Discussions to plan next steps**

# 1. Call Information

**Date:** 09 January 2024, Tuesday

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

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

**Organizer:** Sheeba Backia Mary B.

# 2. Call Participants:

|  |  |
| --- | --- |
| Name | Company |
| Adrian Buckley | MITRE |
| Andreas Kunz | Lenovo |
| Andreas Pashalidis | BSI |
| Candace Carducci | JHU/APL |
| Christine Jost | Ericsson |
| Cichonski, Jeffrey A. | NIST |
| David Gabay | MITRE |
| David Hasselquist | Sectra |
| Denisha Jackson | NSA |
| DJEMAI Tanissia | Irt Saint Exupéry |
| Dusty Hoffpauir | Charter Communications |
| Elizabeth Koser | NSA |
| Francois Ennesser | Huawei |
| Ge Yao | China Unicom |
| German Peinado | Nokia |
| Gino Scribano | JHU/APL |
| Hongyi Pu | Huawei |
| Imran Saleem | Huawei |
| Johannes Doerr | BMWK |
| John Ing | PSC |
| Jörg Andreas | BSI |
| Markus Hanhisalo | Ericsson |
| Michael Bilca | Trideaworks |
| Noamen | Huawei |
| PAULIAC Mireille | Thales |
| Peilin | ZTE |
| Sajid, Taha | Comcast |
| Sheeba Baskaran | Lenovo (Presenter) |
| Tim Woodward | Motorola Solutions |
| Tyler Hawbaker | OTD\_US |
| Venkata Rama Raju Chelle | Department of Telecom |
| Yuze Liu | ZTE |
| Zhibi Wang | Interdigital |

# 3. Agenda and Minutes

|  |  |  |
| --- | --- | --- |
| **No.** | **Agenda** | **Meeting Minutes** |
| 1 | Approved Objectives (20 mins)  1. WT1 - Next Steps  2. WT2 - Next Steps  Target Key Issue(s) [Count & Concept] | **1. WT1 Data exposure for Security evaluation and monitoring - Next Steps:**  Sheeba presented the WT1 next steps and the following discussions happened with respect to the threat and relevant data exposure analysis table template.  Comcast, Taha: Wants to add the impact; what data fields would be exposed, SNPI or PII information; wants to classify internal or external attack for threat/attack description.  Lenovo, Sheeba: PII is clear, but what is SNPI?  Comcast, Taha: Sensitive nonpublic information.  Lenovo, Sheeba: okay, on SBA layer/SBI what interprets the internal attack and external attack?  Comcast, Taha: Will come back on this.  MITRE, Adrian: Is this a component to capture the WT1 to facilitate the discussions? Tables could become unmanageable; how to use it?  Lenovo, Sheeba: The fields in this table can facilitate as part of analysis and security evaluation, identification of list of threats/attacks and identification of relevant data to be exposed for security monitoring; The table can be placed in a dedicated clause.  MITRE, Adrian: will there be a summary clause to help the reader?  Ericsson, Christine: do you want to have it in text form in a specific structure?  MITRE, Adrian: no issue at all; just about documenting.  Lenovo, Sheeba: Fine either way. These fields in the table can be converted as bullets of subclauses or paragraphs; for the tenet analysis we were missing the core point with too much text; as long we agree on the fields that really help us on the identification of relevant data, it is okay to have a non-tabular approach.  Nokia, German: the plan is to list the data and how this data is exposed under which conditions? Just the list of data that is relevant or also how to consume them? What is the intention what we are going to do with it?  Lenovo, Sheeba: The intension to have this analysis is mainly to identify and list the relevant data for exposure; Further we can also give more freedom to the operator(s) to invoke data collection in general considering the operator policies and then when an abnormality happens the relevant can be collected for exposure; When the list gets stable, we can also describe the exposure and consumption aspects in the security analysis and considerations clause.  Ericsson, Christine: Do we have common understanding to the endpoint of the exposure? Where is the data exposed to? Do we have to study it?  Lenovo, Sheeba: In Rel-18 we discussed and studied these things; the exposure point is to the function in the operator network, that is external to the 3gpp network, e.g., monitoring tool/ SIEM; we can discuss and cover these aspects in the ‘security assumptions clause’ in the TR; We can also cove the trust assumptions on the endpoint as a trusted entity.  Nokia, German: Yes, SIEM or SOAR, can be any tool in the operator network.  Ericsson, Christine: If we can capture in a clause, can have a common understanding.  **2. WT2 - Security mechanism for dynamic policy enforcement- Next Steps:**  [Telefonica Feedback received on SA3 email as the Diego couldn’t join the call due to another meeting - Suggest to consider as one of the mechanisms for dynamic policy enforcement, the use of ACME STAR (RFC 8739) as a way of simplifying revocation mechanisms for PKI. As far as I can tell, there is a SID focused on ACME use in 3GPP networks]  Sheeba presented the WT2 next steps, and the following discussions happened with respect to the Key Issue concept and count information.  Nokia, German: Its dangerous to open the floor to different KIs; we talk about concrete threats that can be addressed potentially by the dynamic policy enforcement on the SBA layer; it’s not outside the SBA layer; thinking that a good thing are concrete examples of the threat together with the potential dynamic policy on the SBA layer; would be more efficient; link the enforcement to the threat;  Comcast, Taha: Agrees with this; the threat classification should enforce a policy accordingly; there should be a correlation to the threat; we specify what policies needs to be enforced; if we use NRF or any SBA application and we enforce a policy on the certificate management, we have to come with some use cases why we enforce the policy;  Lenovo, Sheeba: Okay, Do you think we should start with the use case to map the threat to the policy enforcement?  Comcast, Taha: Yes;  Nokia, German: It’s a way, just a thought to organize it;  Lenovo, Sheeba: For this threat and security policy enforcement mapping, do we need to wait until we identify and agree on all data that needs to be exposed or can we start this exercise from the beginning?  Nokia, German: Don’t think so; first one is more generic; like endpoint discussion, could be just a consumer from the data; this here is to activate SBA with policy enforcement; proposal to run it in parallel;  Lenovo, Sheeba: okay, we can study the use case with the mapping between threats and necessary security policy enforcement. After agreement we can come to related key issues;  Huawei, Noamen: What do we want to do? If a NF is identified as compromised, do we want to terminate the connections or do we consider more of service level restrictions, what is the intension here?  Lenovo, Sheeba: Be it a termination or any restriction, they are all are certain actions; those are part of the dynamic policy enforcement; first any entity to perform the action should know the security evaluation & monitoring result (if it is available); So, for WT2 to enable the security policy enforcement first results need to be available if applicable, but what action is taken and that granularity is a solution kind of thing.  Comcast, Taha: First task we explain what are the threats, and classify them; if we have more clarity on all the threats then we have more clarity on the action like shutting down, isolating;  MITRE, Adrian: WT1 is identifying the threats, wants to have potential solutions in the end with recommendations; is this the outcome of WT2? Are you expecting a solution to come out?  Lenovo, Sheeba: For WT1 we will consider the R18 progress (i.e, key issue and solution discussed and agreed) and now R19 threat and data list identification outcome completements finalization; along with the clarifications in security assumptions, solution principles can be recommended for normative. For WT2 as we didn’t reach consensus on key issue in R18, now first we should agree Key issue with the security requirement. Then we will proceed and discuss on the possible solutions; and then based on the common agreement the recommendations for normative work will proceed.  MITRE, Adrian: When are the solutions coming?  Sheeba, Lenovo: We need to agree the key issue first and the solutions discussions will happen as a next step.  Ericsson, Christine: You need to clarify the scenario here; we didn’t have the assumptions;  Lenovo, Sheeba: Okay, we can discuss the scenario where the potential threats can happen in a dedicated sub-clause under security analysis clause 5;  Ericsson, Christine: If we don’t have a common understanding on the scenarios, this will take a lot of time later.  Nokia, German: Having a pre-analysis, an agreed list of use cases to further elaborate, can be constructive for the key issue discussions later;  Huawei, Noamen: Still not clear about the scenarios; commenting on the concept here; NF has been compromised here; do you want to go through the list of all services of that NF and the service coming from the compromised NF?  Lenovo, Sheeba: If the compromised NF is notified to the SBA and how to revisit the decision that has been made to give service access to the NF can be looked into;  Huawei, Noamen: I don’t understand the threat analysis of the compromised NF;  Lenovo, Sheeba: The scenarios that I was thinking is, if a service access is provided for a NF and if that NF is later identified to be compromised, and knowing this result how to revisit the decisions; another scenario can be registered NF, if identified to be compromised; if you get notified that its compromised how to revisit the decisions; what can be done in these case can be studied in the use case analysis. If you have other scenarios in mind, we can also discuss.  Noamen: Then my understanding is correct: how do you act when you get a request from the NF; If a NF is identified as compromised, how to terminate it.  Sheeba: Every company can bring a scenario specific discussion paper/contribution for this use case exercise, we can have a dedicated subclause (5.2) in security analysis clause and then we will know the level of divergence and we can clarify and work on it to bring a common understanding and consensus on the scenarios. |
| 2 | Structure of TR (40 mins)  #Scope Initial Draft | **TR table of contents:**  Sheeba presented the TR skeleton and scope text draft.  Huawei, Noamen: will there be a table in 5.1?  Lenovo, Sheeba: No, it will be in text form (e.g., paragraph with bullets for each field listed in the example table) based on MITREs comments and Ericsson’s suggestion.  5.1 exclusively for WT1 in a non-tabular fashion  5.2 for scenario and use case level discussions for WT2  Will update the TR skeleton accordingly.  **Scope Draft:**  No comments |
| 3 | Work Plan Vs TU Budget (20 mins) | **Work Plan:**  Sheeba presented the Work Plan for each meeting.  MITRE, Adrian: For normative work you need a WID approved; you should move it one meeting out;  Huawei, Noamen: Next meeting you expect KIs but this may have undesirable impact.  Lenovo, Sheeba: Following our WT2 discussions today, we can consider use cases and scenarios contributions for the first step and then we can move to key issues; I will refine the work plan table accordingly.  Nokia, German: Good to have the 5.1 and 5.2 as focus in the first meeting as basement for the rest; good to focus on the skeleton and assumptions.  Huawei, Noamen: Good content for 5.1 and 5.2 would be a good achievement for the TR;  **TU – Per Meeting Budget:**  Sheeba presented the TU budget (Options 1 and 2) to consume for each meeting.  Ericsson, Christine: Time is really scarce; we should use offline time  Huawei, Noamen: we assume the chair will help here; in 30min we can handle max 10 tdocs if we are fast; it really depends on the number of contributions.  Lenovo, Sheeba: In case of multiple contributions covering similar aspects, suggest discussing and merging offline to save time. Of-course all contributions can be submitted to the meeting, but the merger one can be opened for discussions in the meeting to save time and to bring progress. |
| 4 | Next Step – Offline Call#2 | **Dedicated for SA3#115 Contribution Drafts Discussion**  Lenovo, Sheeba: All interested companies are invited to provide contributions for WT1 and WT2 on the following for the next offline call #2 for SA3#115 preparations.  WT1: Contributions with information to identify 🡪list of threats/attacks, list of relevant data necessary for exposure and the associated details.  WT2: Use case Contributions - scenarios with mapping of threats that needs dynamic policy enforcement in SBA. |
| 5 | Any other business | MITRE (Adrian) made draft presentation on timeline: Wants guidelines when to finish a particular work task.  SA3#117 (Aug 2024)🡪 Last meeting for WT1.  SA3#118 (Oct 2024) 🡪 Last meeting for WT2. New WT1 scenario may be handled if accompanies WT2 solution.  SA3#119 (Nov 2024) 🡪 Wrap all Conclusions. WT2 Solution may be handled, but that solution needs to be part of the conclusion. If WT1 contributions handled, then SA3#118 recommendation also applies.  Huawei, Noamen: Do you assume certain dependencies between WT2 and WT1? Or just a choice?  MITRE, Adrian: There is no dependency, the work can proceed as needed before the guideline milestones. When a guideline is reached then the authors need to bring in multiple WTs per the guidelines. .  Lenovo, Sheeba: We should be bit careful in treating solution contributions in the last meeting. If such contributions are treated in advance, will be better for the progress. Conclusion closure and clean-up will take some time, so last meeting can help such discussions.  MITRE, Adrian: In SA2, there has been cases, where companies bring solutions with lot of supporting companies in the last meeting and that also has been agreed as part of the conclusion. |
| Call is closed | | |