**3GPP SA3 teleconference for ProSe security (2021.07.19)**

**Meeting topics:**

Discuss high-priority KIs and the potential baselines for these KIs.

**Content:**

Part1: Direct Discovery:

Part2: Direct Communication:

Part3: UE-to-Network Relay

Part4: Privacy and others:

Part5: UE-to-UE Relay:

The priority for a KI could be: **High**, **Low**, **Not consider**

(Preliminary conclusions discussed during the call are marked below).

**Part1: Direct Discovery**

**Key Issues:**

5.1 Key Issue #1: Discovery message protection

5.2 Key Issue #2: Keys in ProSe discovery scenario

5.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF

5.11 Key Issue #11: UE identity protection during ProSe discovery

**General background:**

SA2 reuses LTE discovery solution (Model A and Model B) in 5G.

**5.1 Key Issue #1: Discovery message protection**

**KI priority:** (rapporteur proposal：high)

**Potential security requirements:**

* The discovery messages in open discovery shall support integrity protection and replay protection. （rapporteur proposal：high）
* The discovery messages in restricted discovery shall support confidentiality protection, integrity protection, and replay protection. （rapporteur proposal：high）
* The entity which receives a restricted discovery message on the PC5 interface shall be able to verify the source authenticity. （rapporteur proposal：high）
* ~~The 5G System shall provide means to protect the discovery response message of a discoveree UE in the restricted direct discovery model B architecture from other discoveree UE(s). （rapporteur proposal：not consider）~~

**Solutions:** Sol#3, Sol#4, Sol#27, Sol#28

**Comments:**

Rapporteur：There are 4 solutions (Sol#3. Sol#4, Sol#27, Sol#28) related to this KI. Sol#3 reuses LTE open discovery. Sol#4 reuses LTE restricted discovery. Sol#27 and Sol#28 are not directly related to the discovery security. When establishing one-to-one communication that relies on the discovery process, these solutions try to improve performance. It has nothing to do with the discovery security itself. It is proposed to use Sol#3 and Sol#4 as the baselines for normative work.

**Decisions: Use Solution #3 and #4 as the baseline, solutions #27, #28 merging to be explored.**

**5.2 Key Issue #2: Keys in ProSe discovery scenario**

**KI priority:** (rapporteur proposal: high)

**Potential security requirements:**

Not applicable

**Solutions:** Sol#9, Sol#35

**Comments:**

Rapporteur：Sol#9 has impacts on existing security architecture. Sol#35, in general, follows LTE solution.

**Decisions: Potential solution is #35, but clarification needed from SA2 on the architecture impact.**

**5.10 Key Issue #10: Key issue on secure data transfer between UE and 5GDDNMF**

**KI priority:** (rapporteur proposal: high)

**Potential security requirements:**

* The ProSe-enabled UE and 5GDDNMF shall mutually authenticate each other for secure ProSe communication.
* The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be integrity protected.
* The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be confidentiality protected
* The transmission of data between 5GDDNMF and the ProSe-enabled UE shall be protected from replay attacks.

**Solutions:** Sol#2, Sol#5, Sol#11, Sol#35

**Comments:**

Rapporteur: TR 33.847 has concluded: For Key Issue #10, both Solution #5 and Solution #11 are adopted as the basis for the normative work.

**Decisions: As above, solution already captured in TR.**

**5.11 Key Issue #11: UE identity protection during ProSe discovery**

**KI priority:** (rapporteur proposal: low)

**Potential security requirements:**

* The 5GS shall provide means to mitigate against the use of the identity of a ProSe UE broadcasted during ProSe discovery to trace the ProSe UE.
* The 5GS shall provide means to mitigate against the use of the identity of a ProSe UE broadcasted during ProSe discovery to impersonate the ProSe UE.

**Solutions:** Sol#22, Sol#32

**Comments:**

Rapporteur: Current evaluation in the TR does not support these solutions.

**Decisions: FFS, No solution agreements yet.**

**Part2: Direct Communication**

**Key Issues:**

5.12 Key Issue #12: Security of one-to-one communication over PC5

5.17 Key Issue #17: Supporting security policy handling for PC5 connection of 5G ProSe services

**General background:**

The following text is copied from TS 23.304.

For the PC5 unicast link of the 5G ProSe direct communication, the principal for the PC5 unicast link of V2X communication described in TS 23.287 [2] clause 5.2.1.4 is reused with the following differences:

- V2X service is replaced by ProSe Application;

- V2X service type is replaced by Application ID;

- New data unit types are supported (including IPv4, Ethernet and Unstructured).

Huawe submitted a contribution for KI#12: S3-21xxxx\_Analyse of the necessity to set two security requirements as high priority security requirements

**5.12 Key Issue #12: Security of one-to-one communication over PC5**

**KI priority:** (rapporteur proposal: high)

**Potential security requirements:**

* The mutual authentication between two UEs during one-to-one communication shall be supported.
* The one-to-one communication link security establishment shall be protected from MitM attacks.
* The PC5 one-to-one communication signalling shall support confidentiality protection, integrity protection and anti-replay protection.
* The PC5 one-to-one communication user plane shall support confidentiality protection, integrity protection and anti-replay protection.
* The system shall support means of providing the signalling and user plane security policies to UEs for a particular PC5 one-to-one communication.
* The initiating UE and peer UE shall provide a means to mitigate establishing unprotected connection caused by bidding-down attack.
* The system shall support means for a secure refresh of the UE security context.

**Solutions:** Sol#7, Sol#23, Sol#27, Sol#28, Sol#33

**Comments:**

Rapporteur: V2X security defined in TS 33.536 shall be the baseline for normative work, plus some enhancements introduced in Sol#7, Sol#23, Sol#27, Sol#28, and Sol#33 if they are approved by SA3.

**Decisions: As above, need to solve the bidding down attack.**

**5.17 Key Issue #17: Supporting security policy handling for PC5 connection of 5G ProSe services**

**KI priority:** (rapporteur proposal: high)

**Potential security requirements:**

* 5G ProSe system shall support a means to configure PC5 security policies for 5G Prose services at the network.
* 5G ProSe system shall support a means to securely provision the configured PC5 security policies to the UE for 5G Prose services.
* 5G ProSe system shall support negotiation on the provisioned PC5 security policies for security enforcement by the UEs to meet security requirements of 5G Prose Services.

**Solutions:** no

**Comments:**

Rapporteur: New KI was approved in SA3#103-e. Corresponding solutions are expected in the upcoming meeting.

**Decisions: FFS, let us wait for solution proposals in the upcoming meeting.**

**Part3: UE-to-Network Relay**

**Key Issues:**

5.3 Key Issue #3: Security of UE-to-Network Relay

5.4 Key issue #4: Authorization in the UE-to-Network relay scenario

5.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication

5.5 Key Issue #5: Privacy protection over the UE-to-Network Relay

**General background:**

5G ProSe supports :

* Layer-3 based UE-to-Network Relay, including Layer-3 based UE-to-Network Relay with N3IWF support. In SA2, compared with LTE ProSe, the major improvement is QoS.
* Layer-2 based UE-to-Network Relay

InterDigital submitted a contribution for Part 3: S3-21xxxx\_U2N relay authorization security solutions analysis

**5.3 Key Issue #3: Security of UE-to-Network Relay**

**KI priority:** (rapporteur proposal: high)

**Potential security requirements:**

* The system shall support a secure means to establish a PC5 link between the remote UE and the UE-to-Network relay.
* Confidentiality protection, Integrity protection and replay protection shall be supported between the remote UE and the 3GPP network.
* 3GPP system shall provide means to protect security (i.e., the integrity and confidentiality) of information during UE-to-Network Relay path switch. (is this requirement part of Rel-17?)

**Solutions:** Sol#10, Sol#14, Sol#15, Sol#18, Sol#19, Sol#29, Sol#30

**Comments:**

Rapporteur: Sol#10（not align with SA2）, Sol#14 (L2 based), Sol#15 (not align with SA2), Sol#18 (reuse LTE solution), Sol#19 (L3 based with N3IWF support), Sol#29 (not align with SA2), Sol#30 (not align with SA2)

**Decisions: FFS, need solutions for L3 as well as L2.**

**5.4 Key issue #4: Authorization in the UE-to-Network relay scenario**

**KI priority:** (rapporteur proposal: high)

**Potential security requirements:**

* The 5GS shall support the authorisation of the UE as a UE-to-Network relay in the UE-to-Network relay scenario.
* The 5GS shall support the authorisation of the UE as a Remote UE in the UE-to-Network relay scenario.

**Solutions:** 6, 10, 13, 15, 18, 21, 24, 25, 29, 30, 34, 36

**Comments:**

**Decisions: FFS,** **need to converge from multiple solutions.**

**5.9 Key Issue #9: Key management in 5G Proximity Services for UE-to-Network relay communication**

**KI priority:** (rapporteur proposal: high)

**Potential security requirements:**

* 5GS shall support secure communication between the remote UE and the network via UE-to-Network relays.
* 5GS shall support the generation of separate security contexts for remote UEs for ProSe relay communication.

Solutions: 1, 6, 10, 15, 21, 29, 30

Comments:

**Decisions: FFS, need to converge from multiple solutions.**

**5.5 Key Issue #5: Privacy protection over the UE-to-Network Relay**

**KI priority:** (rapporteur proposal: not consider)

**Potential security requirements:**

* The 5G System should provide means for mitigating trackability attacks on the Remote UE during communications over a UE-to-Network Relay including during UE-to-Network Relay path switch.
* The 5G System should provide means for mitigating linkability attacks on the Remote UE during communications over a UE-to-Network Relay including during UE-to-Network Relay path switch.

**Solutions:** no

**Comments:**

**Decisions: Prefer solutions addressing privacy when selecting the solutions, even though there are no solution particular solution proposals.**

**Part4: Privacy and others**

**Key Issues:**

5.13 Key Issue #13: Security and privacy of groupcast communication

5.14 Key Issue #14: security for support of Non-IP traffic

5.15 Key Issue #15: privacy of ProSe entities while supporting Non-IP traffic

5.16 Key Issue #16: Privacy protection of PDU session-related parameters for relaying

**General background:**

**5.13 Key Issue #13: Security and privacy of groupcast communication**

**KI priority:**

**Potential security requirements:**

* 5G system shall ensure that the group IDs and L2 IDs are protected from linkability and traceability attacks for ProSe groupcast communications.
* One-to-many communications between ProSe-enabled UEs shall be protected by confidentiality and integrity.

**Solutions:** Sol#13

**Comments:**

**Decisions: FFS**

**5.14 Key Issue #14: security for support of Non-IP traffic**

**KI priority:** (rapporteur proposal: not consider)

**Potential security requirements:**

* 3GPP system shall provide means to protect security (i.e., the integrity, confidentiality, and replay protection) while supporting NoN-IP traffic for unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays.

**Solutions:** no

**Comments:**

**Decisions: No specific solution yet.**

**5.15 Key Issue #15: privacy of ProSe entities while supporting Non-IP traffic**

**KI priority:** (rapporteur proposal: not consider)

**Potential security requirements:**

* 3GPP system shall provide means to preserve the privacy of entities and identities while supporting NoN-IP unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays.
* NoN-IP traffic unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays.
* unicast/multicast/broadcast communication between two UEs, and for communication via UE-to-UE and UE-to-Network relays

**Solutions:** no

**Comments:**

**Decisions:** **No specific solution yet.**

**5.16 Key Issue #16: Privacy protection of PDU session-related parameters for relaying**

**KI priority:**

**Potential security requirements:**

* The 5G System shall provide a means to mitigate tracing and tracking privacy attacks on Remote UEs based on potential exposure of slicing information, DNN information, and other PDU session related persistent information.

**Solutions:** Sol#26, Sol#32

**Comments:**

**Decisions: For L2 use Sol#26? For L3, it is FFS**

**Part5: UE-to-UE Relay**

5.6 Key Issue #6: Integrity and confidentiality of information over the UE-to-UE Relay

5.7 Key issue #7: Authorization in the UE-to-UE relay scenario

5.8 Key Issue #8: Privacy of information over the UE-to-UE Relay

**General background:**

5G ProSe will not support UE-to-UE Relay.

**Decision: Out of scope for Rel-17?**

(Rapporteur proposal: SA3 will not consider UE-to-UE Relay's KI and related solutions in R-17)