**3GPP TSG-SA3 Meeting #101-e *S3-20xxxx***

**e-meeting, 9th – 20th November 2020 *revision of S3-203113***

|  |
| --- |
| *CR-Form-v12.0* |
| **CHANGE REQUEST** |
|  |
|  | **33.926** | **CR** | **DraftCR** | **rev** | **-** | **Current version:** | **16.3.0** |  |
|  |
| *For* [***HE******LP***](http://www.3gpp.org/3G_Specs/CRs.htm#_blank)*on using this form: comprehensive instructions can be found at* [*http://www.3gpp.org/Change-Requests*](http://www.3gpp.org/Change-Requests)*.* |
|  |

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| ***Proposed change affects:*** | UICC apps |  | ME |  | Radio Access Network |  | Core Network | **X** |

|  |
| --- |
|  |
| ***Title:***  | Threat of bidding down attack on security association  |
|  |  |
| ***Source to WG:*** | Nokia, Nokia Shanghai Bell |
| ***Source to TSG:*** | S3 |
|  |  |
| ***Work item code:*** | SCAS\_IMS  |  | ***Date:*** | 30-10-2020 |
|  |  |  |  |  |
| ***Category:*** | **B** |  | ***Release:*** | Rel-17 |
|  | *Use one of the following categories:****F*** *(correction)****A*** *(mirror corresponding to a change in an earlier release)****B*** *(addition of feature),* ***C*** *(functional modification of feature)****D*** *(editorial modification)*Detailed explanations of the above categories canbe found in 3GPP [TR 21.900](http://www.3gpp.org/ftp/Specs/html-info/21900.htm). | *Use one of the following releases:Rel-8 (Release 8)Rel-9 (Release 9)Rel-10 (Release 10)Rel-11 (Release 11)Rel-12 (Release 12)**Rel-13 (Release 13)Rel-14 (Release 14)Rel-15 (Release 15)Rel-16 (Release 16)* |
|  |  |
| ***Reason for change:*** | In SA3#100e meeting, the threats related to set-up of security associations were proposed and the bidding-down during security association set-up was added as one of the threats. The added bidding-down threat focuses on the integrity and encryption algorithms list received by the P-CSCF that may be tampered by attackers with weaker security algorithms or by turning off the security protection. In addition to the tampering with weaker algorithms, attackers can also endanger the security protection with a different attempt of bidding down attack. According to current IMS operation, the P-CSCF may be configured to never apply confidentiality, because e.g. it trusts the encryption provided by the underlying access network. But when the P-CSCF is configured to apply confidentiality whenever the UE supports it, confidentiality needs to be provided for the security association. By exploring such configuration options, an attacker can tamper the algorithms list of the UE by removing the encryption algorithms supported by the UE. Then bidding down attack for no confidentiality protection can be launched as follows. During security associateion set-up, the first message SM1 “Register” may not be protected, hence the information within SM1 could be tampered by an attacker, e.g. by removing the encryption algorithms in the “*UE integrity and encryption algorithms list*”. In such case, the P-CSCF will not receive the encryption algorithms supported by the UE and may mistakenly believe that the UE does not support any encryption algorithm, hence will select NULL algorithm for encryption. If the P-CSCF configured to apply confidentiality does not includes the encryption algorithms it supports in SM6 when receiving no supported encryption algorithms from the UE, the UE may mistakenly believe that the P-CSCF is configured to not apply confidentiality when receiving SM6 and will select NULL algorithm for encryption. Therefore, NULL encryption algorithm is negotiated between the UE and the P-CSCF and confidentiality will eventually not be provided for the security association, in which way the attacker can launch the bidding down attack.Based on above analysis, it is proposed to extend the current threat analysis in Annex X.2.2.2 of TR 33.926. |
|  |  |
| ***Summary of change:*** | Extended the current threat analysis in Annex X.2.2.2 of TR 33.926 by analysing more possible threat of bidding down. |
|  |  |
| ***Consequences if not approved:*** | Current threat analysis in Annex X.2.2.2 of TR 33.926 is not complete. |
|  |  |
| ***Clauses affected:*** | Annex X.2.2.2 |
|  |  |
|  | **Y** | **N** |  |  |
| ***Other specs*** |  | **x** |  Other core specifications  | TS/TR ... CR ...  |
| ***affected:*** |  | **x** |  Test specifications | TS/TR ... CR ...  |
| ***(show related CRs)*** |  | **x** |  O&M Specifications | TS/TR ... CR ...  |
|  |  |
| ***Other comments:*** |  |
|  |  |
| ***This CR's revision history:*** |  |

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* Start of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*

# X.2 Assets and threats specific to the P-CSCF

## X.2.1 Critical assets

In addition to the critical assets of a GNP has been described in clause 5.2 of the present document, the critical assets specific to the P-CSCF to be protected are:

- P-CSCF Application;

- IMS signalling;

- Security data, i.e. cryptographic materials for Gm, Mw, Mx, and Iq interfaces

- The interfaces of the P-CSCF to be protected and which are within SECAM scope:

- Gm interface between the P-CSCF and UE

- Mw interface between the P-CSCF and the C-CSCF/I-CSCF

- Mx interface between the P-CSCF and IBCF

- Iq interface between the P-CSCF and IMS AGW

- Console interface, for local access: local interface on the P-CSCF

- OAM interface, for remote access: interface between the P-CSCF and the OAM system

NOTE 1: The detailed interfaces of the P-CSCF class are described in clause 4 of the present document.

- P-CSCF Software: binary code or executable code

NOTE 2: P-CSCF files may be any file owned by a user (root user as well as non-root users), including user account data and credentials, log data, configuration data, OS files, P-CSCF application, user plane security mechanism, or cryptographic materials.

## X.2.2 Threats related to set-up of security associations

### X.2.2.1 High-priority algorithm selection

- Threat name: High-priority algorithm selection

- Threat Category: Tampering of data, Information Disclosure, Denial of Service

- Threat Description: If the P‑CSCF does not select the highest priority algorithm combination on its own list which is also supported by the UE to protect the messages between the P‑CSCF and the UE, the P‑CSCF could end up using a weaker algorithm forcing the system into a lowered security level making the system easily attacked and/or compromised.

- Threatened Asset: IMS signalling

### X.2.2.2 Bidding down on security association set-up

- Threat name: Bidding down on security association set-up

- Threat Category: Tampering of data, Information Disclosure, Denial of Service

- Threat Description: The following behaviours may lead to bidding down attacks:

- If the P‑CSCF does not check whether the integrity and encryption algorithms list, SPI\_P and Port\_P received in SM7 is identical with the corresponding parameters sent in SM6, and check whether SPI\_U and Port\_U received in SM7 are identical with those received in SM1, the attacker can force the system to reduce the security level by tampering the integrity and encryption algorithms list. Then, weaker security algorithms may be selected, which will make the system easily attacked. Tampering the SPI will cause the negotiated SA cannot be indexed. As a result, the following security association fails to be established, leading to Denial of Service attack. The port number is generally used to identify different applications. Tampering the Port\_P number by the attacker will cause messages to be sent to the UE or P-CSCF through the tampered port. These messages including some sensitive parameters may be leaked to another application, which is not intended to receive this message.

- The P-CSCF may be configured to never apply confidentiality, because e.g. it trusts the encryption provided by the underlying access network. The P-CSCF may also be configured to apply confidentiality whenever the UE supports it. During security associateion set-up, the first message SM1 “Register” may not be protected, hence the information within SM1 could be tampered by an attacker, e.g. by removing the encryption algorithms in the “*UE integrity and encryption algorithms list*”. In such case, the P-CSCF will not receive the encryption algorithms supported by the UE and may mistakenly believe that the UE does not support any encryption algorithm, hence will select NULL algorithm for encryption. If the P-CSCF configured to apply confidentiality does not includes the encryption algorithms it supports in SM6 when receiving no supported encryption algorithms from the UE, the UE may mistakenly believe that the P-CSCF is configured to not apply confidentiality when receiving SM6 and will select NULL algorithm for encryption. Therefore, NULL encryption algorithm is negotiated between the UE and the P-CSCF and confidentiality will eventually not be provided for the security association, in which way the attacker can launch the bidding down attack. In another word, if the P-CSCF configured to apply confidentiality does not include its encryption algorithms in SM6 when receiving no encryption algorithms of the UE in SM1, such behavior of P-CSCF will fail to thwart the bidding down attack.

NOTE: The threat above applies to UEs supporting at least one encryption algorithm other than NULL algo, as an attacker cannot launch such bidding down attack on UEs only supporting NULL algo.

Editor’s Note: The handling of the P-CSCF in the case where the P-CSCF receives SM1 with no encryption algo of UE but receives SM7 protected by the UE with an encryption algo different than NULL algo is to be further analysed.

- Threatened Asset: IMS signalling, security data

\*\*\*\*\*\*\*\*\*\*\*\*\*\*\* End of the Change \*\*\*\*\*\*\*\*\*\*\*\*\*\*\*\*