TSG-SA WG3-WG2 joint session
26 April 2001
Madrid, Spain

S3z010052
Hiding Requirements
Agenda item: 7.1

Source: AT&T

Title: Network hiding mechanism

Document for: Approval

1 Introduction

This contribution addresses the Security needs of Configuration Independence (aka Network Hiding). It includes mechanisms needed to route SIP requests and responses, ensuring that information about the S-CSCF is not provided to those not authorized to receive it.

2 Discussion

The design for Configuration Independence has been discussed in both SA2 and CN1. The mechanism being studied is to encrypt the SIP Via, Record-Route, and Route headers at an I-CSCF, and then de-crypt them in handling the response to the SIP request. Further, the routing information given to P-CSCF during Registration may contain encrypted information, which would be de-crypted by an I-CSCF in handling a SIP request.

Since packets may not return via the same I-CSCF that encrypted the aforementioned headers, all I-CSCFs of an operator should have the ability to decrypt each other's data. In the simplest conceivable implementation, all I-CSCFs share a key, which is distributed by whatever provisioning mechanisms already exist for the purposes of setting up security-related information on the CSCFs. This key could also be established by running any number of shared-key generation protocols. This key, which we shall call Kv, will need to be regenerated periodically. When that happens, the previous key is also kept for a small fraction of the key lifetime in case there are still sessions using the old key. With a modern algorithm such as AES, with a 128-bit block and a 256-bit key, there is no real reason to ever rekey during the lifetime of the system, unless, of course, the key gets compromised or otherwise exposed.

The information to be encrypted is prepended with a random 128-bit Initialization Vector, and padded to a multiple of 128 bits. Most likely, the information will actually be padded to the longest possible length, so that the adversary cannot even learn the number of CSCFs the message has been though. The information is encrypted and MAC-protected with a block cipher (e.g., AES), in CBC-MAC mode. One of the proposed new modes for AES is a one-pass integrity-protection and encryption mode, and that should be used once it is standardized by NIST. All this is base-64 encoded and transmitted as a single Via header. This information is treated opaquely by the other CSCFs. When an I-CSCF receives this opaque header, it decrypts it with the shared key, verifies the integrity, and reconstructs the headers.

The IV shall be a random number; it cannot be a counter, because multiple CSCFs are using the same key. With a random value and a 128-bit IV, the probability of two CSCFs picking the same IV is roughly 2^{-64}, which is more than adequate. The information does not need to be authenticated, as the threat model does not include malicious tampering of its contents; what is being protected is the identities of all the CSCFs of the home network.

3 Proposal

It is proposed that SA3 endorse the following change to Section 5.2.2.3 of TS23.228, as a method of implementing the network configuration independence requirement.

5.2.2.3 Registration information flow – User not registered

The application level registration can be initiated after the registration to the access is performed, and after IP connectivity for the signalling has been gained from the access network. For the purpose of the registration information flows, the subscriber is considered to be always roaming. For subscribers roaming in their home network, the home network shall perform the role of the visited network elements and the home network elements.

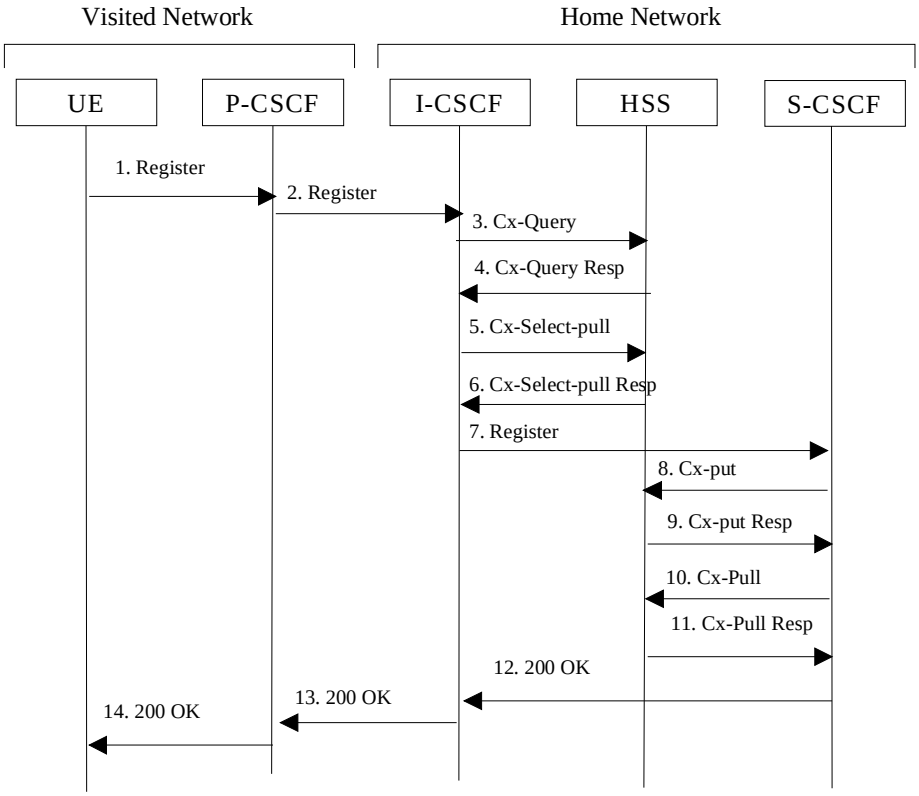

Figure 5.1: Registration – User not registered

1. After the UE has obtained a signalling channel through the access network, it can perform the IM registration. To do so, the UE sends the Register information flow to the proxy (subscriber identity, home networks domain name).

2. Upon receipt of the register information flow, it shall examine the “home domain name” to discover the entry point to the home network (i.e. the I-CSCF). The proxy shall send the Register information flow to the I-CSCF (P-CSCFs “name” in the contact header, subscriber identity, visited network contact name). A name-address resolution mechanism is utilised in order to determine the address of the home network from the home domain name. When the I-CSCF receives the registration information flow from the proxy, it shall examine the subscriber identity and the home domain name, and employ the services of a name-address resolution mechanism, to determine the HSS address to contact.

3. The I-CSCF shall send the Cx-Query information flow to the HSS (P-CSCF name, subscriber identity, home domain name, visited network contact name). The P-CSCF name is the contact name that the operator wishes to use for future contact to that P- CSCF.

Editors Note: It is FFS whether the terminal name, or proxy name, or both is included within this and subsequent register messages.

The Cx-query (P-CSCF name, subscriber identity, home domain name, visited network contact name) information flow is sent to the HSS. The HSS shall check whether the user is registered already. The HSS shall indicate whether the user is allowed to register in that visited network according to the User subscription and operator limitations/restrictions if any.

4. Cx-Query Resp is sent from the HSS to the I-CSCF. If the checking in HSS was not successful the Cx-Query Resp shall reject the registration attempt.

5. At this stage, it is assumed that the authentication of the user has been completed (although it may have been determined at an earlier point in the information flows). The I-CSCF shall send Cx-Select-Pull (serving network indication, subscriber identity) to the HSS to request the information related to the required S-CSCF capabilities which shall be input into the S-CSCF selection function.

6. The HSS shall send Cx-Select-Pull Resp (required S-CSCF capabilities) to the I-CSCF.

7. The I-CSCF, using the name of the S-CSCF, shall determine the address of the S-CSCF through a name-address resolution mechanism and then shall send the register information flow (P-CSCFs "name" in the contact header, subscriber identity, visited network contact name) to the selected S-CSCF.

8. The S-CSCF shall send Cx-Put (subscriber identity, S-CSCF name) to the HSS. The HSS stores the S-CSCF name for that subscriber.

9. The HSS shall send Cx-Put Resp to the I-CSCF to acknowledge the sending of Cx-Put.

10. On receipt of the Cx-Put Resp information flow, the S-CSCF shall send the Cx-Pull information flow (subscriber identity) to the HSS in order to be able to download the relevant information from the subscriber profile to the S-CSCF. The S-CSCF shall store the P-CSCFs name, as supplied by the visited network. This represents the name that the home network forwards the subsequent terminating session signalling to for the UE.

11. The HSS shall return the information flow Cx-Pull Resp (user information) to the S-CSCF. The user information passed from the HSS to the S-CSCF shall include one or more names/addresses information which can be used to access the platform(s) used for service control while the user is registered at this S-CSCF. The S-CSCF shall store the information for the indicated user. In addition to the names/addresses information, security information may also be sent for use within the S-CSCF.

12. The S-CSCF shall determine whether the home contact ~~name~~ information is the S-CSCF name or an I-CSCF name and encrypted information for that I-CSCF. If an I-CSCF is chosen as the home contact name, it may be distinct from the I-CSCF that appears in this registration flow, and it will be capable of decrypting the S-CSCF name from the home contact information. The home contact ~~name~~ information will be used by the P-CSCF to forward signalling to the home network. The S-CSCF shall return the 200 OK information flow (serving network contact ~~name~~information, S-CSCF name) to the I-CSCF.

13. The I-CSCF shall send information flow 200 OK (serving network contact ~~name~~information) to the P-CSCF. The I-CSCF shall release all registration information after sending information flow 200 OK.

14. The P-CSCF shall store the serving network contact ~~name~~information, and shall send information flow 200 OK to the UE.