3GPP TSG SA WG3 Security — S3#21 **S3-010586**

27 - 30 November, 2001

Sophia Antipolis, France

Source: **AT&T Wireless**

Title: **CR to 33.203: Network Hiding Mechanism**

Agenda item: Hiding

Document for: APPROVAL

INTRODUCTION

The existing text on network hiding mechanisms in 33.203 is very brief. This contribution provides some detailed description of the network hiding mechanisms.

DISCUSSION

In SIP protocol, some of the headers, such as Via, Record-Route, Route and Path, contain addresses of the network elements. By sending those headers outside of a network/operator's domain may reveal the network topology information about that operator's network. Therefore a mechanism is needed to restrict the above information being passed outside the operator's network if the operator chooses to implement network hiding. The current working assumption is that encryption based mechanism will be implemented in I-CSCF to perform network hiding, i.e., when I-CSCF forward SIP Request or Response messages outside the operator's domain, the I-CSCF shall encrypt those information elements in Via, Record-Route, Route and Path headers that the operator wishes to hide; when an I-CSCF receives a SIP Request or Response message from outside the operator's domain, the I-CSCF shall decrypt those headers that were encrypted by I-CSCF in this operator domain. This contribution discusses some aspects of network hiding.

1. Hiding Information Elements

Hiding information elements are entries in those SIP headers, such as Via, Record-Route, Route and Path, which contain addresses of the network elements in hiding network. Hiding information elements may be some specific SIP proxy addresses in hiding network; or they may be all the SIP proxy entries that have the same domain name as the hiding network. The current CN1 working assumption is that the I-CSCF shall encrypt all the SIP proxy entries that have the same domain name as the hiding network. In the following example, home1.net is the hiding network.

Via SIP/2.0/UDP pcscf1.visited1.net SIP/2.0/UDP CIPH(SIP/2.0/UDP scscf1.home1.net, SIP/2.0/UDP as.home1.net) SIP/2.0/UDP scscf2.home1.net

2. Encryption Algorithm

The purpose of encryption in network hiding is to protect the identities of the SIP proxies and the topology of the hiding network. Therefore, an encryption algorithm in confidentiality mode should be used. The network hiding mechanism will not address the authentication and integrity protection of the SIP headers. It is recommended that AES in CBC mode with 128-bit block and

128-bit key shall be used as the encryption algorithm for network hiding. In the CBC mode under a given key, if a fixed IV is used to encrypt two same plaintexts, then the ciphertext blocks will also be equal. This is undesirable for network hiding. It is therefore recommended to use random IV for each encryption.

3. Extra Parameters in SIP Header

Since a random IV will be used to encrypt the hiding information elements, the same IV is required to decrypt the information. One way is to have I-CSCF maintain a hiding encryption state and have IV be one of the state elements being kept at I-CSCF. This is undesirable since it makes hiding I-CSCF a stateful proxy. A preferred way is to include the IV in the same SIP header that includes the encrypted information. For example, an encrypted entry in Via header will look like:

Via SIP/2.0/UDP CIPH(SIP/2.0/UDP scscf1.home1.net);IV=45FE336A552C442B

And an encrypted Record-Route header will look like:

Record-Route sip:CIPH(sip:scscf1.home1.net);IV=25FE336A552C442F

PROPOSAL

It is proposed that following modifications to be made in section 6.4 of 33.203.

6.4 Hiding mechanisms

The Hiding Mechanism is optional for implementation. All I-CSCFs in the HN shall share the same encryption and decryption key Kv. If the mechanism is used and the operator policy states that the topology shall be hidden the I-CSCF shall encrypt the ~~address of the S-CSCF~~hiding information elements when the I-CSCF forwards SIP Request or Response messages outside the hiding network's domain. The hiding information elements are entries in SIP headers, such as Via, Record-Route, Route and Path, which contain addresses of SIP proxies in hiding network. When I-CSCF receives a SIP Request or Response message from outside the hiding network's domain, the I-CSCF shall decrypt those information elements that were encrypted by I-CSCF in this hiding network domain. ~~An IV of 128-bit is needed at the encryption and decryption phase and it shall be appended to the encrypted information. The information shall also be MAC protected with a block cipher in CBC-MAC mode.~~

~~When the I-CSCF decrypts the information it shall verify the integrity.~~

The purpose of encryption in network hiding is to protect the identities of the SIP proxies and the topology of the hiding network. Therefore, an encryption algorithm in confidentiality mode shall be used. The network hiding mechanism will not address the issues of authentication and integrity protection of SIP headers. The AES in CBC mode with 128-bit block and 128-bit key shall be used as the encryption algorithm for network hiding. In the CBC mode under a given key, if a fixed IV is used to encrypt two same plaintexts, then the ciphertext blocks will also be equal. This is undesirable for network hiding. Therefore, random IV shall be used for each encryption. The same IV is required to decrypt the information. The IV shall be included in the same SIP header that includes the encrypted information.