3GPP TSG SA WG3 Security — S3#21 **S3-010653**

27 - 30 November, 2001

Sophia Antipolis, France

Source: Alcatel

Title: Mechanism to Hide Network Configuration

Document for: Discussion

Agenda item:

1 INTRODUCTION

TS 23.228 introduces various requirements around network configuration hiding. Basically, an operator should be able to hide the topology of its internal network, such as the addresses of its CSCF servers. AWS, in contribution S3-010323, suggests a mechanism by which the addresses of the CSCF servers are encrypted by the outgoing I-CSCF.

In this contribution, we discuss the problem space. We then discuss various solutions to determine one which would suit.

2 PROBLEM SPACE

As further described in TS 23.228, the I-CSCF which handles communications with SIP proxies in other domains (note that there may be more than one such I-CSCF) must be able to hide the list of SIP proxies/servers used within its own domain. Fields in SIP message header that are of concern are *Via*, *Record-Route* and *Route*.

2.1 Via Field

The *Via* field is used to record the sequence of SIP systems through which a SIP request message passes. The receiver copies the *Via* fields into the SIP response to provide the list of SIP systems through which the SIP response must pass. The list of *Via* fields therefore reveals the coordinates of the SIP proxies/servers (I/S-CSCFs) located in a domain once the SIP request is relayed to another domain by the border SIP proxy (I-CSCF).

2.2 Route Field

A list of *Route* fields is put into the SIP request message by the requester in order to force the sequence of SIP proxies through which the SIP request has to pass. Each such SIP proxy removes itself from the *Route* fields list prior to relaying the SIP request (possibly to the next system identified in the *Route* header fields if present).

The use of *Route* fields by the S-CSCF does not seem to bring any security issue related to hiding requirements. The coordinates of other SIP systems of the S-CSCF's domain will have been removed before the SIP request leaves the domain. The hiding requirement is therefore naturally fullfilled. This could not be the case if the receiver is located in the S-CSCF's domain and the SIP request is to be routed through a third-party domain before re-entering the S-CSCF's domain where the receiver is located.

The use of *Route* fields by the SIP UAC does not seem to be a common scenario. Nevertheless, it could require a hiding mechanism if the SIP UAC sets a route for its home domain part and the SIP request passes through a third-party domain (ie the SIP UAC is located outside its home domain). (Some of) the *Route* fields must then be hidden.

2.3 Route-Record Field

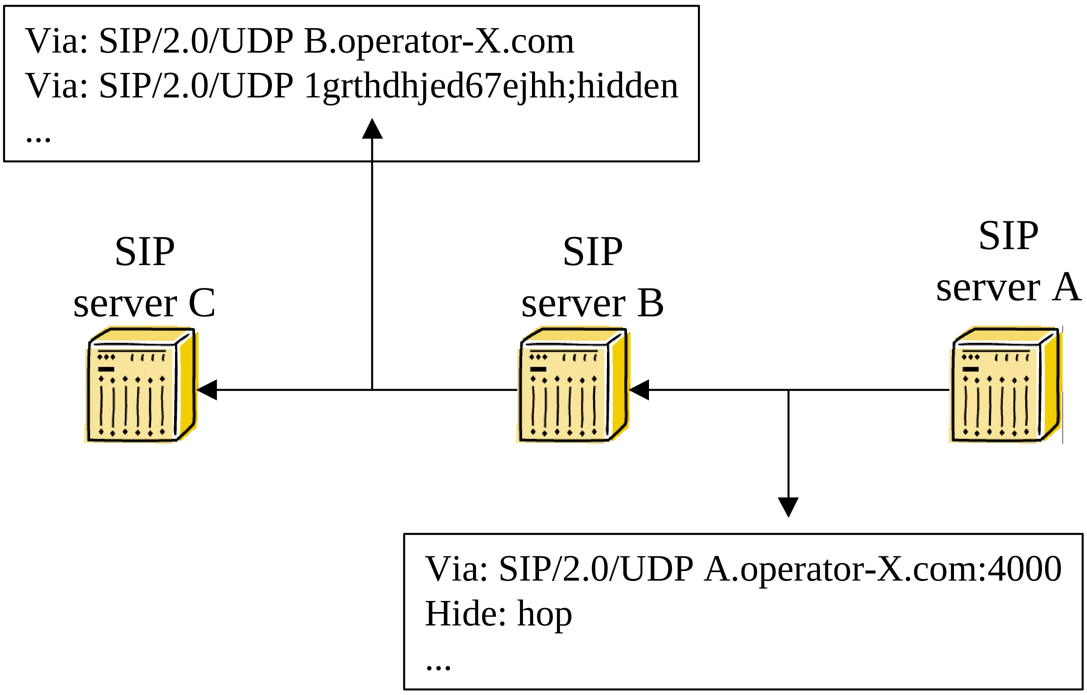
Route-Record header fields are added into the SIP request message to record the list of SIP proxies through which the SIP request has passed. This list is copied into the SIP response so that further SIP requests can take the same route (via the *Route* header fields). This therefore brings similar issues as with Via header fields since the list of SIP systems (I/S-CSCFs) is revealed outside the domain.

3 SOLUTIONS

3.1 RFC2543 Hiding Mechanism

3.1.1 Solution Overview

RFC 2543 originally defines a hiding mechanism for Via header fields. It basically works as follows, based on the configuration in figure 1.



```
Via: SIP/2.0/UDP B.operator-X.com
Via: SIP/2.0/UDP 1grthdhjed67ejhh;hidden
...
```

```
Via: SIP/2.0/UDP A.operator-X.com:4000
Hide: hop
...
```

By adding the *Hide* header field in the SIP message header, the SIP server A requests that server B hides server A's address before relaying the SIP message towards server C.

Before relaying the SIP message, server B hides server A's name or IP address and port number. The parameter *hidden* is added to the Via field to indicate that the field value has been encrypted (this is to make sure that on receiving back a response or the same SIP message, server B will know it must decrypt the field before processing the message such as for loop detection).

Two hiding mechanisms are specified in RFC 2543. The address or name and port number can be replaced by some random value or the address or name and port number can be encrypted. In the first case, the random value serves as an index into a table containing all the Via header fields processed by server B. It must therefore keep state information for every message it relays. In the second case, server B uses an encryption algorithm of its choice to encrypt the data. An appropriate salt must be included for encryption (such as a timestamp) so as to avoid server A's coordinates to always be encrypted the same way. Clearly, encryption seems the most viable option as it would not require server B to keep any information nor any conflict of random values chosen by different SIP proxies.

3.1.2 Basic Issues

This solution specified in RFC 2543 presents numerous issues and lacks.

When using encryption, most useful algorithms that could be used require an IV. Such an IV needs to be carried (possibly in clear) together with the encrypted data. An extra parameter to the Via header would be needed for this. We believe that this IV could play the role of the salt, provided the IV is changed for every Via field value encrypted by server B.

Additional parameters (such as *TTL* or *Branch*) are left in clear and not considered by the hiding (ie encryption) mechanism.

To be complete, the solution should provide a mechanism for server B to be able to identify which algorithm and secret key it used to encrypt a given Via field value. Indeed, the algorithm and, more probably, the secret key used to encrypt the Via field in the SIP message will change over time.

The value allowed for the cipher text in the Via header field must be an ASCII string excluding various special characters. Any encryption must be followed by an ascii-sation of the cipher text that produces an acceptable string (Base64).

3.1.3 Applicability to 3GPP

As such, this solution cannot be applied to 3GPP environments as it lacks basic features to make it really work in any case.

In the case of 3GPP, we believe there is no need for the *Hide* header field as hiding by the I-CSCF is a policy decision made at the I-CSCF, not requested by any other CSCF (typically S-CSCF) within the domain.

4 RFC2543BIS HIDING MECHANISM

RFC2543bis, as currently described in draft version 5, does not contain any provision for network hiding.

5 NEW HIDING MECHANISM

The hiding mechanism we are suggesting is derived from the mechanism originally presented in AWS contribution S3-010323. This solution requires modifications to the current draft RFC2543bis.

The hiding mechanism is based on the use of a symmetric encryption algorithm to encrypt the Via, Route or Route-record field value. Extra parameters are defined for each of those header fields to carry the IV and a secret key identifier (which implicitly also identifies the algorithm used).

Before relaying a SIP message to another SIP system located outside the current domain, the SIP proxy (I-CSCF) encrypts each previous Via header field (ie the value therein) and adds extra parameters (IV and key identifier).

Format of the Via header should look as follows.

Via: <Base64 encoding of the encrypted value>; IV=<IV hexadecimal value>; key=<key identifier>

Format of the Route header should look as follows.

Route: <Base64 encoding of the encrypted value>; IV=<IV hexadecimal value>; key=<key identifier>

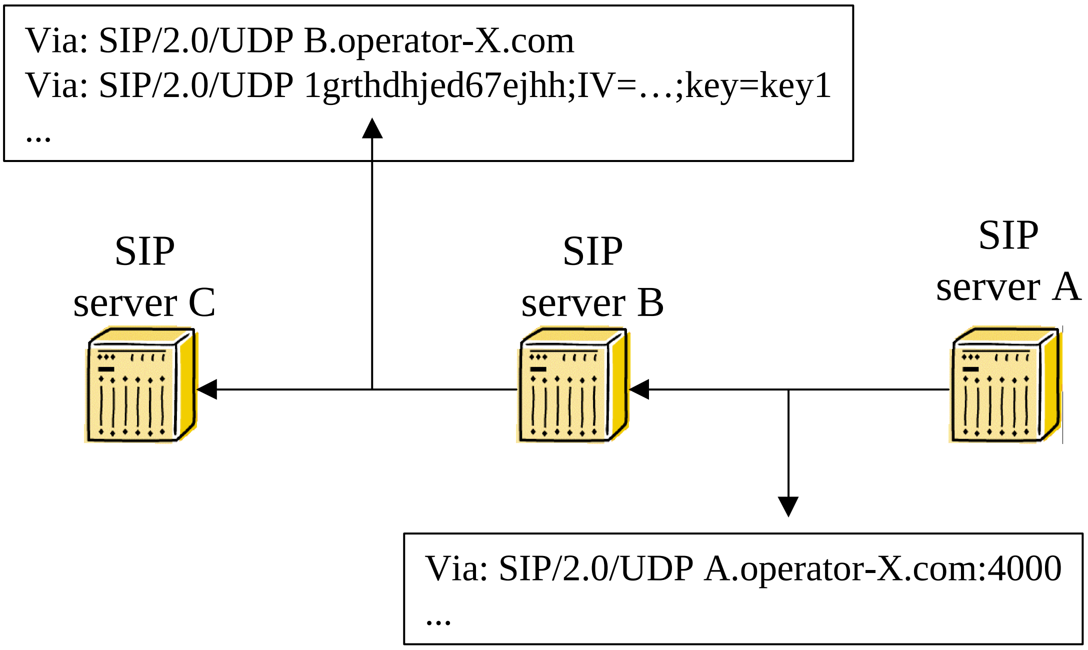
Format of the Route-Record header should look as follows.

Route-Record: <Base64 encoding of the encrypted value>; IV=<IV hexadecimal value>; key=<key identifier>

Extensions to the SIP header ABNF are required to cover cases where the field value is the result of a Base64 encoding. Two new parameters must also be defined to carry the IV and the key identifier.

Because some encryption mechanisms require extra protection using an authentication mechanism (eg. CTR mode), it may be necessary to envisage the use of a MAC algorithm in addition to the encryption of the header field value.

The following illustrates the result of the hiding mechanism applied to a Via header field.



Via: SIP/2.0/UDP B.operator-X.com
Via: SIP/2.0/UDP 1grthdhjed67ejhh;IV=…;key=key1
...

Via: SIP/2.0/UDP A.operator-X.com:4000
...

If more than one border SIP proxy (ie I-CSCF) is in place in a given domain, the *Via* mechanism normally ensures that the same SIP proxy is used for the response. However, in cases where another SIP proxy would be used for the response, this requires that all border SIP proxies share the same set of secret keys so that one can decrypt what was encrypted by another one (an alternative solution could be to asymmetrically encrypt the secret key and insert it into the SIP message header but this still requires all border SIP proxies to share the same private key).