SIP Record-Route/Route Hiding

1 Introduction

Some ISPs value the ability to limit topology knowledge that untrusted users can glean from network traffic transiting the ISP’s borders.

One example of this is configuration of ISP routers to not respond
to traceroute ICMP queries. Another example is usage of the SIP Via header hiding.

Although the SIP RFC (RFC2543) specifies Via hiding/encryption as a mechanism to prevent leakage of layer 5 routing information from Via headers, it does not address routing information leaked through Record-Route and Route headers.

This draft proposes a SIP extension which preserves the functionality of Route and Record-Route headers but prevents leakage of routing information through those headers.

The main difference between Via hiding and Record-Route/Route hiding is the directionality in which hiding needs to occur. Via header hiding/encryption is needed only unidirectionally (from caller to called party). Record-Route/Route header hiding is needed bi-directionally.

The approach proposed for Record-Route/Route header hiding is the same approach taken for Via header hiding: Each proxy protects its previous hop.

The diagram below illustrates the normal message flow when proxies P1, P2, and P3 add themselves to the Record-Route header.

```
UAC       P1       P2       P3       UAS
|--REQ-->  |        |        |        |
     |        |        |        |        |
     |        |--REQ-->|        |        |
     |        |  Record-Route: P1|        |        |
     |        |        |        |--REQ-->|
```
2.2 Algorithm for Record-Route header hiding:

The approach used to encrypt Record-Route and Route headers is the same approach used to encrypt Via headers: Each proxy protects its previous hop.

In the following logic "right" and "left" refer to the order of entries in a catted header. For example, in:


<sip:p1.cisco.com> is to the left of <sip:p2.cisco.com>.

2.2.1 Request handling logic:

Here’s the proxy logic to implement on a request PDU:

/* Record-Route header logic */
if (this proxy is introducing himself into Record-Route header) {
    if (a Record-Route entry already exists) {
        Using your secret key, encrypt and replace the left-most entry.

}
Add your FQDN to the beginning of the Record-Route header

/* Route header logic */
if (topmost Route entry is marked "hidden") {
    Remove the topmost entry of the Route header.
    Using your secret key, decrypt this entry and route this PDU to it.
}

### 2.2.2 Record-Route response logic:

Here’s the proxy logic to implement on a response PDU:

/* Record-Route header logic */
if (your plain-text FQDN is present in the Record-Route header) {
    if (a Record-Route entry exists to left) {
        Using your secret key, encrypt and replace the left entry.
    }
    if ((a Record-Route entry exists to right) && (the entry is marked "hidden")) {
        Using your secret key, decrypt and replace the right entry.
    }
}

### 2.3 Reusing Hide header

The Hide: [hop/route] header usage is extended to apply to Record-Route and Route headers (as well as Via headers).

The Hide: [hop/route] header usage is extended to be bi-directional. (i.e. The Hide header may be present in requests and/or responses).

See [RFC2543, Section 6.23 Hide] for more information on Hide header.

A client or proxy requesting "Hide: hop/route" can only rely on keeping the path private if it sends the request to a trusted proxy.

Hidden Record-Route and Route headers reuse the Via header "hidden" option as described in [RFC2543, Section 6.44].

### 2.4 Design tradeoffs/considerations

There is an advantage gained by encrypting the Record-Route/Route information instead of simply hiding the information in proxy control blocks. Storing the route information in a proxy would require the proxy to maintain long-duration state. Pushing the route state to the endpoints allows the proxy to remain stateless.
The disadvantage to encryption is that it requires more processing in SIP proxies and therefore impacts signalling latency. This results in increased call setup times.

When a proxy encrypts headers such as Via, State, and Record-Route/Route, the proxy is encrypting information for its own future use. In such cases, use of a private key suffices. (i.e. No key exchange operations are needed).

2.5 Message flow using encrypted Record-Route/Route

The diagram below illustrates the message flow when proxies P1, P2, and P3 add themselves to the Record-Route header using encrypted Record-Route/Route headers.

In the message flow below, K1 represents proxy 1’s secret key, K2 represents proxy 2’s secret key, and K3 represents proxy 3’s secret key. The E(X, Kn) syntax indicates the encrypted form of X using key n. REQ indicates a SIP request message (such as INVITE or ACK). RSP indicates a SIP response message (such as 200).

```
UAC      P1       P2       P3       UAS
|        |        |        |        |
|--REQ-->|        |        |        |
|        |        |        |        |
|        |--REQ-->|        |        |
|        | Record-Route: P1 |
|        | Hide: hop |
|        |        |
|        |--REQ-->|        |        |
|        | Record-Route: P2, E(P1,K2) |
|        | Hide: hop |
|        |        |
|        |--REQ-->|        |        |
|        | Record-Route: P3, E(P2,K3), E(P1,K2) |
|        | Hide: hop |
|        |<-RSP---|
|        | Record-Route: P3, E(P2,K3), E(P1,K2) |
|        | Contact: UAS |
|        |<-RSP---|
|        | Record-Route: P3, P2, E(P1,K2) |
|        | Contact: UAS |
|        | Hide: hop |
|        |<-RSP---|
```
Security Considerations

Security issues are the primary topic of this RFC.

This document proposes an extension to SIP to prevent leakage of layer 5 routing information to untrusted proxies and user agents through Record-Route and Route headers.

The use of Record-Route/Route and Via header hiding is discouraged unless path privacy is truly needed; Hide fields impose extra processing costs and restrictions for proxies.
4 Further Examples

Only the relevant headers have been included in the following examples.

4.1 Standard INVITE/200/ACK sequence using Record-Route/Route and Via header hiding

In this example, proxies P1, P2, and P3 are all configured to request Hide: hop.

<table>
<thead>
<tr>
<th>UAC</th>
<th>P1</th>
<th>P2</th>
<th>P3</th>
<th>UAS</th>
</tr>
</thead>
<tbody>
<tr>
<td>---[1] INV-&gt;</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>---[2] INV-&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record-Route: P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hide: hop</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>---[3] INV-&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record-Route: P2, E(P1,K2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hide: hop</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>---[4] INV-&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record-Route: P3, E(P2,K3), E(P1,K2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hide: hop</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;-[5] 200---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record-Route: P3, E(P2,K3), E(P1,K2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact: UAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;-[6] 200---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record-Route: P3, P2, E(P1,K2)</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact: UAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hide: hop</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;-[7] 200---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record-Route: E(P3,K2), P2, P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact: UAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hide: hop</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>&lt;-[8] 200---</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Record-Route: E(P3,K2), E(P2,K1), P1</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Contact: UAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Hide: hop</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>---[9] ACK-&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Route: E(P2,K1), E(P3,K2), UAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>---[10] ACK-&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Route: E(P3,K2), UAS</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>---[11] ACK-&gt;</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Route: UAS</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
[1] SIP UAC to SIP proxy server 1:

INVITE sip:bob@p1.isp.com SIP/2.0
Via: SIP/2.0/UDP alice-pc.isp.com
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[2] SIP proxy server 1 to SIP proxy server 2:

INVITE sip:bob@p2.isp.com SIP/2.0
Via: SIP/2.0/UDP p1.isp.com
Via: E(SIP/2.0/UDP alice-pc.isp.com, K1);hidden
Record-Route: <sip:bob@p1.isp.com;maddr=p1.isp.com>
Hide: hop
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[3] SIP proxy server 2 to SIP proxy server 3:

INVITE sip:bob@p3.isp.com SIP/2.0
Via: SIP/2.0/UDP p2.isp.com
Via: E(SIP/2.0/UDP p1.isp.com, K2);hidden
Via: E(SIP/2.0/UDP alice-pc.isp.com, K1);hidden
Record-Route: <sip:bob@p2.isp.com;maddr=p2.isp.com>,
<sip:E(bob@p1.isp.com;maddr=p1.isp.com, K2)>;hidden
Hide: hop
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[4] SIP proxy server 3 to UAS:

INVITE sip:bob@bob-pc.isp.com SIP/2.0
Via: SIP/2.0/UDP p3.isp.com
Via: E(SIP/2.0/UDP p2.isp.com, K3);hidden
Via: E(SIP/2.0/UDP p1.isp.com, K2);hidden
Via: E(SIP/2.0/UDP alice-pc.isp.com, K1);hidden
Record-Route: <sip:bob@p3.isp.com;maddr=p3.isp.com>,
<sip:E(bob@p2.isp.com;maddr=p2.isp.com, K3)>;hidden,
<sip:E(bob@p1.isp.com;maddr=p1.isp.com, K2)>;hidden
Hide: hop
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[5] UAS to SIP proxy server 3:

SIP/2.0 200 OK
Via: SIP/2.0/UDP p3.isp.com
Via: E(SIP/2.0/UDP p2.isp.com, K3);hidden
Via: E(SIP/2.0/UDP p1.isp.com, K2);hidden
Via: E(SIP/2.0/UDP alice-pc.isp.com, K1);hidden
Record-Route: <sip:Bob@p3.isp.com;maddr=p3.isp.com>,
              <sip:E(bob@p2.isp.com;maddr=p2.isp.com, K3)>;hidden,
              <sip:E(bob@p1.isp.com;maddr=p1.isp.com, K2)>;hidden
Contact: bob-pc.isp.com
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[6] SIP proxy server 3 to SIP proxy server 2:

SIP/2.0 200 OK
Via: SIP/2.0/UDP p2.isp.com
Via: E(SIP/2.0/UDP p1.isp.com, K2);hidden
Via: E(SIP/2.0/UDP alice-pc.isp.com, K1);hidden
Record-Route: <sip:Bob@p3.isp.com;maddr=p3.isp.com>,
              <sip:Bob@p2.isp.com;maddr=p2.isp.com>,
              <sip:E(bob@p1.isp.com;maddr=p1.isp.com, K2)>;hidden
Contact: bob-pc.isp.com
Hide: hop
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[7] SIP proxy server 2 to SIP proxy server 1:

SIP/2.0 200 OK
Via: SIP/2.0/UDP p1.isp.com
Via: E(SIP/2.0/UDP alice-pc.isp.com, K1);hidden
Record-Route: <sip:E(bob@p3.isp.com;maddr=p3.isp.com, K2)>;hidden,
              <sip:Bob@p2.isp.com;maddr=p2.isp.com>,
              <sip:Bob@p1.isp.com;maddr=p1.isp.com>
Contact: bob-pc.isp.com
Hide: hop
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp
[8] SIP proxy server 1 to UAC

SIP/2.0 200 OK
Via: SIP/2.0/UDP alice-pc.isp.com
Record-Route: <sip: E(bob@p3.isp.com; maddr=p3.isp.com, K2)>; hidden,
    <sip: E(bob@p2.isp.com; maddr=p2.isp.com, K1)>; hidden,
    <sip: bob@p1.isp.com; maddr=p1.isp.com>
Contact: bob-pc.isp.com
Hide: hop
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[9] SIP UAC to SIP proxy server 1:

ACK sip:p1.isp.com SIP/2.0
Via: SIP/2.0/UDP alice-pc.isp.com
Route: <sip: E(bob@p2.isp.com; maddr=p2.isp.com, K1)>; hidden,
    <sip: E(bob@p3.isp.com; maddr=p3.isp.com, K2)>; hidden,
    <sip: bob@p1.isp.com>
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[10] SIP proxy server 1 to SIP proxy server 2:

ACK sip:p2.isp.com SIP/2.0
Via: SIP/2.0/UDP alice-pc.isp.com
Via: E(SIP/2.0/UDP alice-pc.isp.com, K1); hidden
Route: <sip: E(bob@p3.isp.com; maddr=p3.isp.com, K2)>; hidden,
    <sip: bob@p1.isp.com>
Hide: hop
From: sip:alice@isp.com
To: sip:bob@isp.com
Call-ID: 12345600@alice-pc.isp.com
CSeq: 1 INVITE
Content-Type: application/sdp

[11] SIP proxy server 2 to SIP proxy server 3:

ACK sip:p3.isp.com SIP/2.0
Via: SIP/2.0/UDP alice-pc.isp.com
Via: E(SIP/2.0/UDP alice-pc.isp.com, K1); hidden
Via: E(SIP/2.0/UDP alice-pc.isp.com, K2); hidden
Route: <sip: bob@p1.isp.com>
Hide: hop
From: sip:alice@isp.com
To: sip:bob@isp.com
Outstanding issues/questions:
1) We are re-using the Hide: header to imply that
   Via headers AND Record-Route/Route headers should be hidden by proxies.
   Is this ok? Alternatively, another header (Hide-Route:) could be used.

   This draft redefines the Hide: header to mean that both Via headers AND Record-Route/Route headers should be hidden.

2) Can/should we use the State: header to store entries for Record-Route/Route?
   NOTES:
   - The State header itself leaks routing information unless each proxy encrypts all previously added State headers.

3) Can we do simple hiding of Record-Route/Route entries?
   NOTES:
   - This would appear to cause a proxy to maintain long-term route state.

6 Acknowledgements

We would like to thank David Williams, Nilesh Trivedi, and JC Ferguson of Cisco Systems for their insights, inputs, and comments.

7 References

Byerly/Daiker/Bhatnagar  draft-byerly-sip-hide-route-00.txt  Page 12

Internet Draft  SIP Record-Route/Route Hiding  October 2000

Authors’ Addresses

Bryan J. Byerly
Cisco Systems
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park, NC 27709
USA
Email: byerly@cisco.com

David Daiker
Cisco Systems
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park, NC 27709
USA
Email: ddaiker@cisco.com

Shailandra Bhatnagar
Cisco Systems
7025 Kit Creek Road
P.O. Box 14987
Research Triangle Park, NC 27709
USA
Email: shbhatna@cisco.com