Identity based Authentication in Session Initiation

by
Harsh Kupwade
Southern Methodist University
Dean Willis
Softarmor LLC
Thomas M. Chen
Swansea University
Nhut Nguyen
Samsung Telecommunications

Session Initiation Protocol

1. INVITE
3. 100 Trying
8. 180 Ringing
11. 200 OK

2. INVITE
5. 100 Trying
7. 180 Ringing
10. 200 OK

4. INVITE
6. 180 Ringing
9. 200 OK

12. ACK
13. Media Session
14. Bye
15. 200 OK

INVITE message in SIP

INVITE sip:bob@biloxi.com SIP/2.0
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bK776asdhds
Max-Forwards: 70
To: Bob <sip:bob@biloxi.com>
From: Alice <sip:alice@atlanta.com>;tag=1928301774
Call-ID: a84b4c76e66710@pc33.atlanta.com
CSeq: 314159 INVITE Contact: <sip:alice@pc33.atlanta.com>
Content-Type: application/sdp Content-Length: 142
(Alice’s SDP not shown)


RFC 4474

INVITE sip:bob@biloxi.example.org SIP/2.0
Content-Id: "ZYNBbHC00VMz2k2t6VmCvPonWJMGvQTBDbgghoWeLxJfzB2a1pxAr3VgrB0SsSAa
IfsRdiOPOqZYOy2wrVghuhsCBmtWUSFxI6p6qSTOQXHMpz6uEo3svsSH49thyGn
FVCnyaA++yRIBYYQTLqWzJ+KVhPKbfU/pryhVn9Yc6U="
Identity: <https://atlanta.example.com/atlanta.cer>;alg=rsa-sha1
Identity-Info: <https://atlanta.example.com/atlanta.cer>;alg=rsa-sha1
Contact: <sip:alice@pc33.atlanta.example.com>
Content-Type: application/sdp
Content-Length: 147
(Alice’s SDP not shown)

We cannot apply RFC 4474 to SIP responses

- Response messages cannot be challenged.
- SIP response messages may not encode the identity of the responder


Rogue Proxy sends a falsified 200 OK

1. INVITE
2. Biloxi.com
3. Falsified 200 OK
4. INVITE
5. Rogue Proxy
6. Trudy
7. ACK
8. Media Session
Trudy sends a falsified 200 OK message to Alice

SIP/2.0 200 OK
Via: SIP/2.0/UDP server10.biloxi.com;branch=z9hG4bK4b43c2ff8.1;received=192.0.2.3
Via: SIP/2.0/UDP bigbox3.site3.atlanta.com;branch=z9hG4bK77ef4c2312983.1;received=192.0.2.2
Via: SIP/2.0/UDP pc33.atlanta.com;branch=z9hG4bKKnashds8;received=192.0.2.1
To: Bob <sip: bob@biloxi.com>; tag=a6c85cf
From: Alice <sip: alice@atlanta.com>; tag=1928301774
Call-ID: a84b4c76e66710
CSeq: 314159 INVITE

Contact: <IP address of the Rogue Proxy>
Content-Type: application/sdp
Content-Length: 131
v=0
o=bob 2890844527 2890844527 IN IP4 client.biloxi.example.com
s=IN IP4 < IP Address of the Rogue Proxy>
t=0 0
m=audio 49172 RTP/AVP 0
a=rtpmap:0 PCMU/8000

Approach: Transform Response Identity problem into Connected Identity Problem

Messages 1-3 convey Alice’s Identity to Bob
Messages 7-9 convey Bob’s Identity to Alice

J. Elwell, “Connected Identity in the Session Initiation Protocol (SIP)” IETF draft
Unanticipated Response Problem

SIP/2.0 200 OK
From: <sip:Alice@example.com>;tag=13adc987
To: <sip:Bob@example.com>;tag=2ge46ab5
Contact: <sip:Carol@ua2.biloxi.com>

Drawbacks

• Self signed certificates
• Dependence on PKI
  – Discovery of a public key certificate [Linn,Brancaud04]
  – Complex path construction process

Identity based signature algorithms

- Single domain environment
  - Hess’s Algorithm (Digital Signature)
  - Lynn’s Algorithm (Signcryption Scheme)

- Hierarchical domain environment
  - Gentry and Silverberg’s algorithm (Digital Signature)
  - Chow’s Algorithm (Signcryption Scheme)

Signature and Key Size

<table>
<thead>
<tr>
<th>Criteria</th>
<th>RFC 4474</th>
<th>IBS Schemes</th>
</tr>
</thead>
<tbody>
<tr>
<td>Signature Size</td>
<td>175 bytes(sig) + 512 bytes + CA certs</td>
<td>Hess’s algorithm 511 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Lynn’s 434 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Gentry &amp; Silverberg algorithm 434 bytes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chow et al’s algorithm 434 bytes</td>
</tr>
<tr>
<td>Key size</td>
<td>1024 bits</td>
<td>160 bits</td>
</tr>
</tbody>
</table>
### Computational Time

<table>
<thead>
<tr>
<th>Scheme</th>
<th>Generation time in sec</th>
<th>Verification time in sec</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open SSL (RFC 4474)</td>
<td>0.109s</td>
<td>0.110s</td>
</tr>
<tr>
<td>PBC library Hess’s algorithm</td>
<td>0.078s</td>
<td>0.051s</td>
</tr>
<tr>
<td>PBC library Lynn’s algorithm</td>
<td>0.269s</td>
<td>0.238s</td>
</tr>
<tr>
<td>PBC library Gentry and Silverberg’s algorithm</td>
<td>0.093s</td>
<td>0.063s</td>
</tr>
<tr>
<td>PBC library Chow et. al’s algorithm</td>
<td>0.160s</td>
<td>0.162s</td>
</tr>
</tbody>
</table>


---

### IBS to Response Identity Problem

1. **INVITE**
   - **SIP/2.0 200 OK**
   - From:<sip:Alice@example.com>;tag=13adc987
   - To: <sip:Bob@example.com>;tag=2ge46ab5
   - Identity: <Signcrypted message>
   - Identity-Info: alg=chow;IBS;sip:carol@biloxi.com+Date
   - Content-Type: application/sdp
   - Content-Length: 131
   - Contact: <sip:Carol@ua2.biloxi.com>

2. **INVITE**

3. **INVITE**

4. **200 OK**

5. **200 OK**

Bob would provide private keys for a week to Carol.

Bob not available for a week.

H. Kupwade Patil and D. Willis, “Identity based signcryption scheme to the connected identity problem in the SIP”
Key Distribution in IBE

[B. Lee et al. 2004]

e : G_1 \times G_1 \rightarrow G_2
\quad H_3 : \{ G_2 \} \rightarrow F_p
\quad X = xP \text{ where } x \in Z \text{ and } P \in G_1

1. Request for partial private key X, ID

2. \quad Q_{ID_A} = H_1(\{ID_A\})

3. \quad Q_{bl_A} = H_2[\{e(xP_0, P_0)\}]s_0Q_{ID_A}

4. \quad \text{Sig}(Q_{bl_A}) = s_0Q_{bl_A}

5. Partial private key \text{Sig}(Q_{bl_A})

D_{ID} = \frac{Q_{bl_A}}{H_3[\{e(P_0, P_0)\}]^x}


Revocation issues

• Expiration

1. Request for partial private key X, ID = alice@atlanta.com + June 2, 2008

2. Partial private key

3. Digital Signature + UUID

4. Public key = alice@atlanta.com + UUID

• Using Universally Unique User ID (UUID)
Conclusion

- Identity based signature/sigcryption schemes
  - Reduces the complex path construction process used by PKI
  - Faster processing speed compared to the RSA based schemes (RFC 4474)

Future Work

- Identity based authentication in a peer to peer SIP environment

Thank You