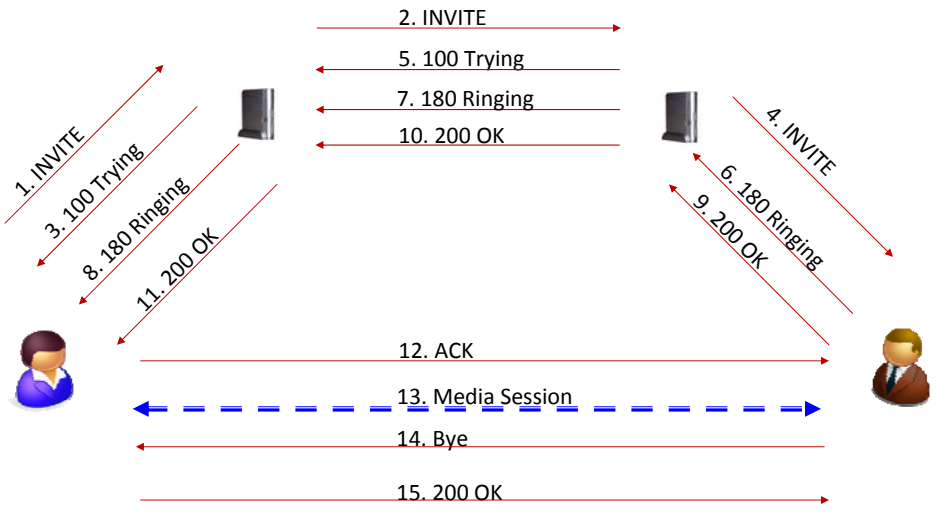
Identity based Authentication in Session Initiation

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

Session Initiation Protocol



[RFC 3261] J. Rosenberg et. al ,"Session Initiation Protocol" IETF RFC 3261

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>

Spoofed — 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 3261] J. Rosenberg et. al ,"Session Initiation Protocol" June 2002

RFC 4474

INVITE sip:bob@biloxi.example.org SIP/2.0

Contact: <sip:alice@pc33.atlanta.example.com>

Identity:
"ZYNBbHC00VMZr2kZt6VmCvPonWJMGvQTBDqghoWeLxJfzB2a1pxAr3VgrB0SsSAa
ifsRdiOPoQZYOy2wrVghuhcsMbHWUSFxI6p6q5TOQXHMmz6uEo3svJsSH49thyGn
FVcnyaZ++yRlBYYQTLqWzJ+KVhPKbfU/pryhVn9Yc6U="

Identity-Info: <https://atlanta.example.com/atlanta.cer>;alg=rsa-sha1

Content-Type: application/sdp
Content-Length: 147
(Alice's SDP not shown)

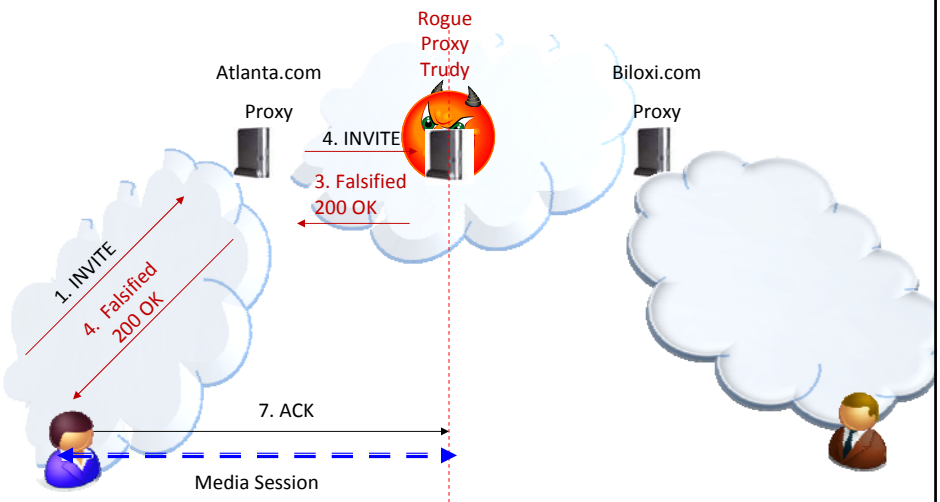
[IETF RFC 3261] C. Jennings and J. Peterson ,"Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP) " August 2006

We cannot apply RFC 4474 to SIP responses

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

[RFC 3261] J. Rosenberg et. al ,"Session Initiation Protocol" IETF RFC 3261

Rogue Proxy sends a falsified 200 OK



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=z9hG4bKnashds8 ;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=-

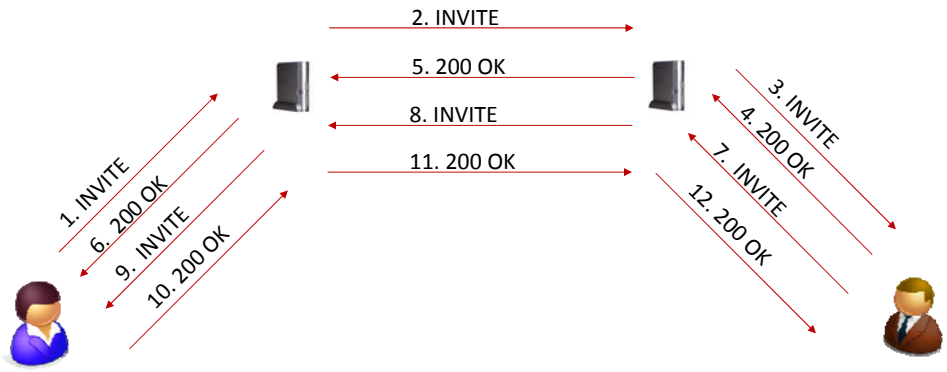
c=IN IP4 < IP Address of the Rogue Proxy >

t=0 0

m=audio 49172 RTP/AVP 0

a=rtpmap:0 PCMU/8000

Approach: Transform Response Identity problem into Connected Identity Problem

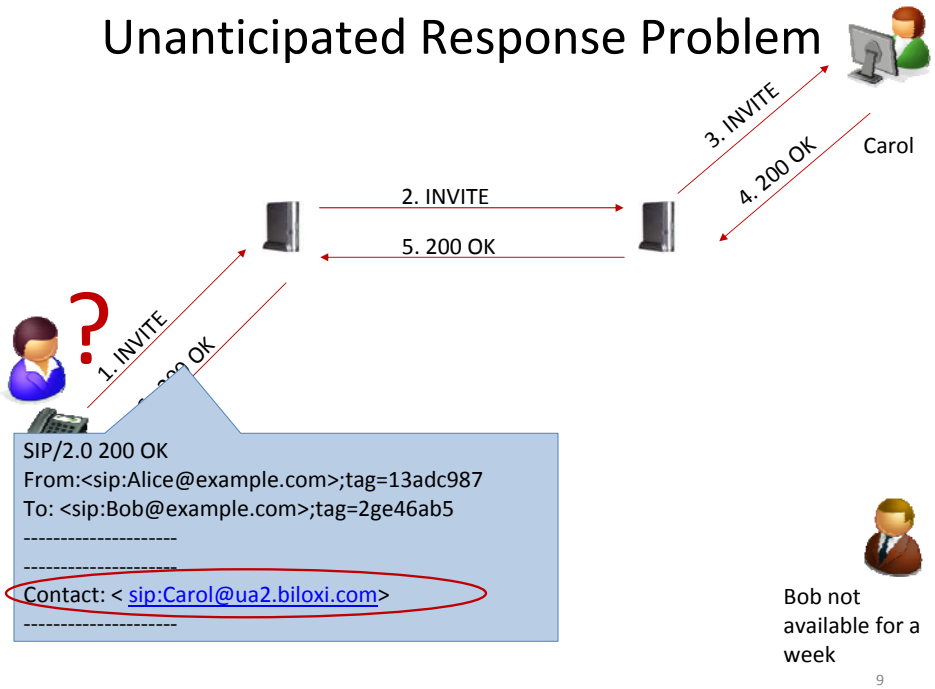


Messages 1-3 convey Alice's Identity to Bob

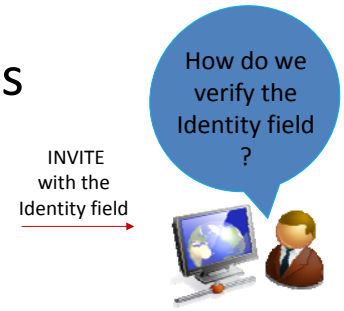
Messages 7-9 convey Bob's Identity to Alice

J. Elwell, "Connected Identity in the Session Initiation Protocol (SIP)" IETF draft

Unanticipated Response Problem



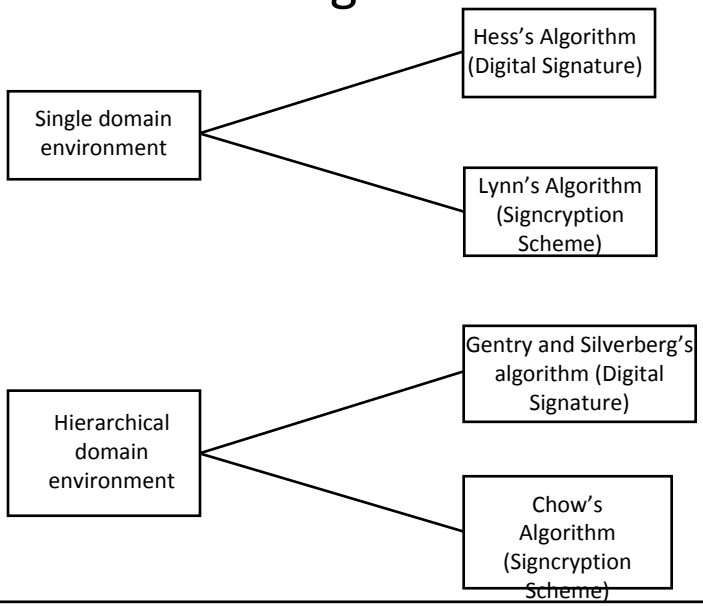
Drawbacks



- Self signed certificates
- Dependence on PKI
  - Discovery of a public key certificate [Linn,Branchaud04]
  - Complex path construction process

Di. Berbecaru, A. Lioy and M. Marian "On the Complexity of Public-Key Certificate Validation, " in Proceedings of the 4th International Conference on Information Security, Lecture Notes in Computer Science, Springer-Verlag, Vol 2200 pages 183-203, 2001

Identity based signature algorithms



Signature and Key Size

Criteria	RFC 4474	IBS Schemes
Signature Size	175 bytes(sig) + 512 bytes + CA certs	Hess's algorithm 511 bytes
		Lynn's 434 bytes
		Gentry & Silverberg algorithm 434 bytes
		Chow et al's algorithm 434 bytes
Key size	1024 bits	160 bits

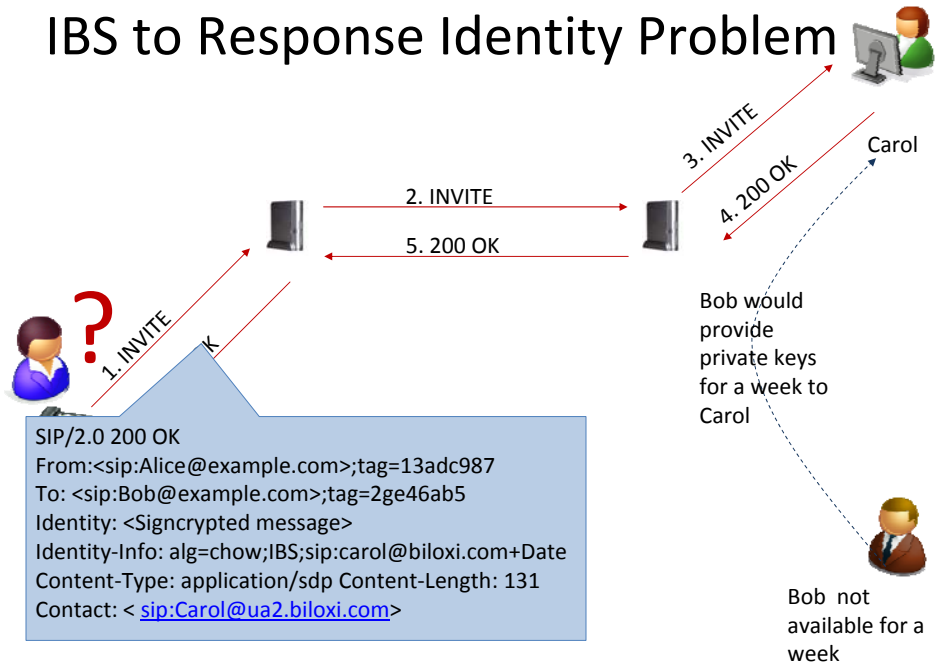
H. Kupwade Patil and D. Willis, " Identity based authentication in SIP" , IETF draft 2008.

Computational Time

Scheme	Generation time in sec	Verification time in sec
Open SSL (RFC 4474)	0.109s	0.110s
PBC library Hess's algorithm	0.078s	0.051s
PBC library Lynn's algorithm	0.269s	0.238s
PBC library Gentry and Silverberg's algorithm	0.093s	0.063s
PBC library Chow et. al's algorithm	0.160s	0.162s

H. Kupwade Patil and D. Willis, " Identity based authentication in SIP" , IETF draft 2008.

IBS to Response Identity Problem



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]

$e : G_1 \times G_1 \rightarrow G_2$

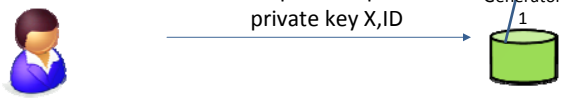
$H_3 : \{G_2\} \rightarrow F_p$

$X = xP$ where $x \in Z$ and $P \in G_1$

2. $Q_{ID_A} = H_1(ID_A)$

3. $Q_{bl_A} = H_3[e(s_0X, P_0)]s_0Q_{ID_A}$

4. $Sig(Q_{bl_A}) = s_0Q_{bl_A}$

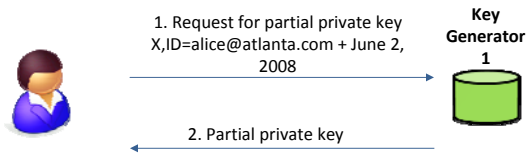


$$D_{ID} = \frac{Q_0}{H_3[e(P_0,P_0)^x]}$$

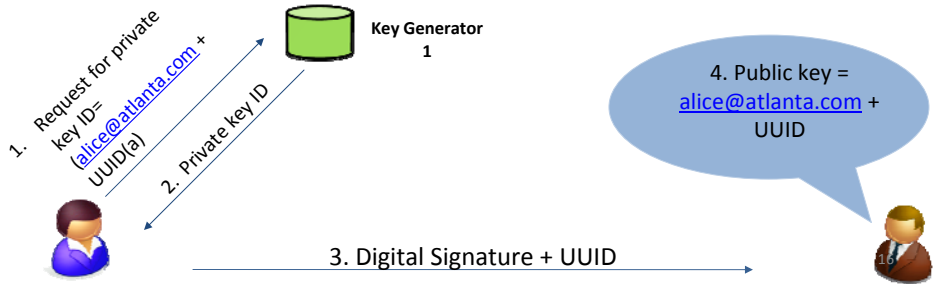
[B.Lee et.al 2004] B. Lee, C. Boyd, E. Dawson, K. Kim, J. Yang and S. Yoo, "Secure Key Issuing in ID-based Cryptography," in *Conferences in Research and Practice in Information Technology, 2004, vol. 32, pp. 69-74.*

Revocation issues

- Expiration



- 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