

Identity In Asterisk (RFC 4474)

Sendilkumaar Durairaj
Graduate Student
IIT Rice Campus

Identity Problem

- How to be certain of identity of caller?
- SIP is easily spoof able,
- Caller ID, From fields can be easily modified
- End to End TLS/SSL solution is not feasible unless all the proxy support
- Proxy are notorious in modifying the SIP headers

% got a light?

No match.

RFC 4474 and implementing in **Asterisk**

- ❑ Mechanism to Assure the Identity of Caller
- ❑ Signature based authentication
- ❑ Uses private/public key pairs (RSA)
- ❑ Introduces new headers Identity and Identity-Info

% ^**What is saccharine?**

Bad substitute

Food for Techies

- ❑ digest-string = addr-spec "|" addr-spec "|" callid "|" 1*DIGIT SP Method "|" SIP-date "|" [addr-spec] "|" message-body
- ❑ Sign the digest-string using private key of user , signed string goes into [Identity] header in SIP
- ❑ Verify the digest-string using public key of user, End user or proxy uses the [Identity-Info] header in SIP to verify.

% drink < bottle; opener Bad substitute

bottle: cannot open opener: not found

Identity (Can you fake it)

□ Identity:

```
"ZYNBbHC00VMZr2kZt6VmCvPonWJMGvQTBDqghoWeLxJfzB2a1pxAr3  
VgrB0SsSAa  
ifsRdiOPoQZYOy2wrVghuhcsMbHWUSFxI6p6q5TOQXHMmz6uEo3svJsS  
H49thyGn FVcnyaZ++yRIBYYQTLqWzJ+KVhPKbfU/pryhVn9Yc6U="
```

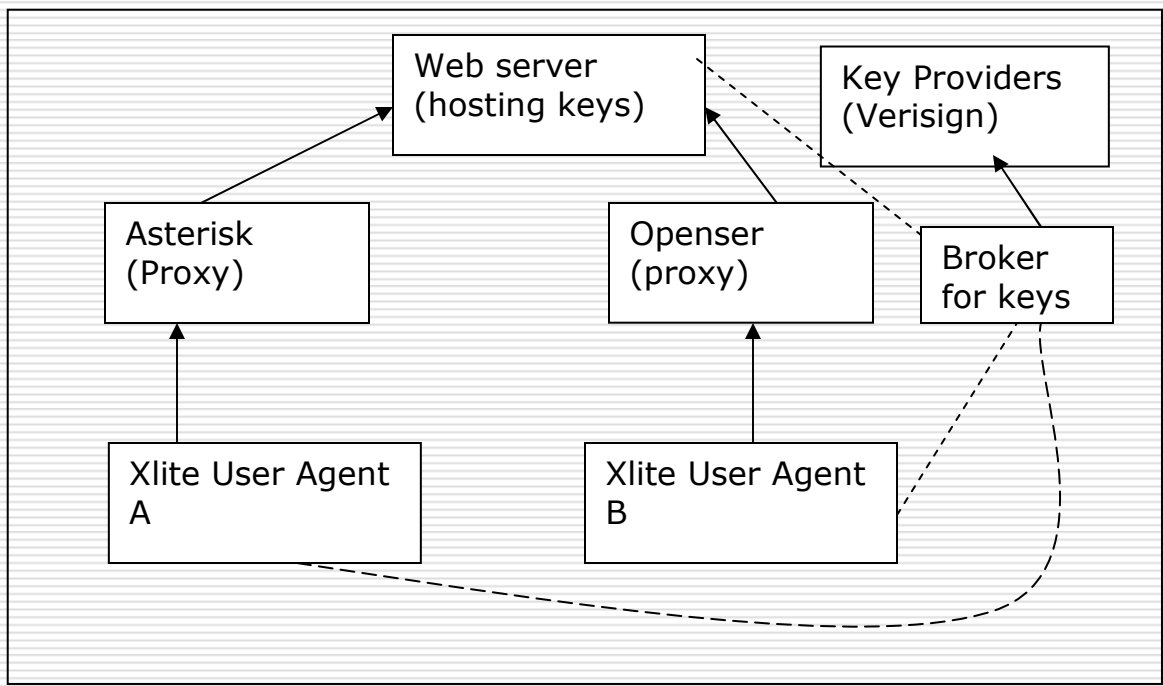
□ Identity-Info:

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

% man: why did you get a divorce?

man:: Too many arguments.

Big Picture (copyright protected 😊)

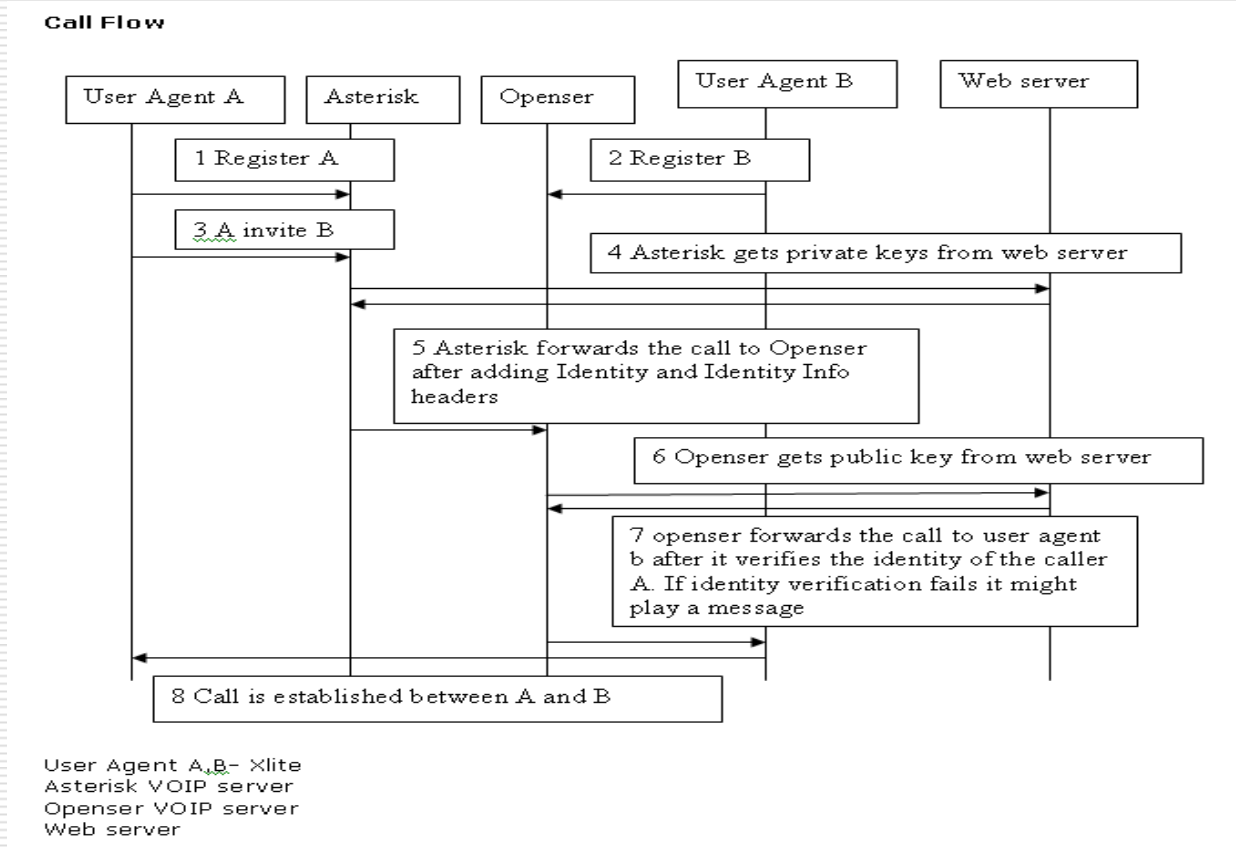


- ❑ Service provider acts as broker to provide keys to the user

% [Where is my brain?

Missing].

Call Flow – (find the missing link worth a chocolate)



% make love

Make: Don't know how to make love. Stop.

Wireshark Trace – Done in 1000 ms

Time	192.168.1.69	192.168.1.75	64.131.110.220	192.168.1.77	192.168.1.66	Comment
16.661	(39194)					SIP/SDP: Request: INVITE sip:5152015260@192.168.1.69
16.664	(39194)					SIP: Request: ACK sip:5152015260@192.168.1.75
16.666	(39194)					SIP/SDP: Request: INVITE sip:5152015260@192.168.1.69
17.364		(39287)				HTTP: GET /keys/keys/int/5152025020.pvt HTTP/1.1
17.390		(39287)				HTTP: HTTP/1.1 200 OK (text/plain)
17.395		(5060)		(5060)		SIP/SDP: Request: INVITE sip:5152015260@192.168.1.69
17.596		(80)		(49455)		HTTP: GET /keys/keys/int/5152025020.pub HTTP/1.1
17.636		(80)		(49455)		HTTP: HTTP/1.1 200 OK (text/plain)
17.739		(5060)		(5060)		SIP: Status: 100 Giving a try
17.741				(5060)	(26918)	SIP/SDP: Request: INVITE sip:5152015260@192.168.1.69
17.902		(80)		(3452)		HTTP: GET /keys/keys/int/5152025020.pub HTTP/1.1
17.932		(5060)		(5060)	(26918)	SIP: Status: 100 Trying
18.314		(5060)		(5060)	(26918)	SIP: Status: 180 Ringing
18.317		(5060)		(5060)		SIP: Status: 180 Ringing
19.523		(5060)		(5060)	(26918)	SIP/SDP: Status: 200 OK, with session description
19.526		(5060)		(5060)		SIP/SDP: Status: 200 OK, with session description
19.531		(5060)		(5060)		SIP: Request: ACK sip:5152015260@192.168.1.66:20
19.534				(5060)		SIP: Request: ACK sip:5152015260@192.168.1.66:20

192.168.1.69 – User Agent A with Asterisk

192.168.1.75 – Asterisk

192.168.1.77 – Openser

192.168.1.66 – User Agent B with Openser

64.131.110.220 – Webserver holding keys

% man woman

No manual entry for woman . Computer crashed!!!!!!!!!!!!!!

Problems

- ❑ Intermediate proxies might change the headers in SIP, in such case identity verification will fail
- ❑ Price for end user to get keys and maintaining it securely

Development Issues

- ❑ Routing logic based on verification of the signature

```
$ mkdir matter; cat > matter
```

matter: cannot create

Acknowledgments

- Professor **Carol Davids** (Hurray)
- **Incharge Systems**, Inc

% awk "Polly, the ship is sinking"

awk: syntax error near line 1

awk: bailing out near line

Q & A – **Pay Attention !**

- ❑ 2 cents per Question (Note you have to pay for it)
- ❑ Quick draw - Winner gets it all (**Identity** has to be verified for the winner)

\$ test my argument

test: too many arguments