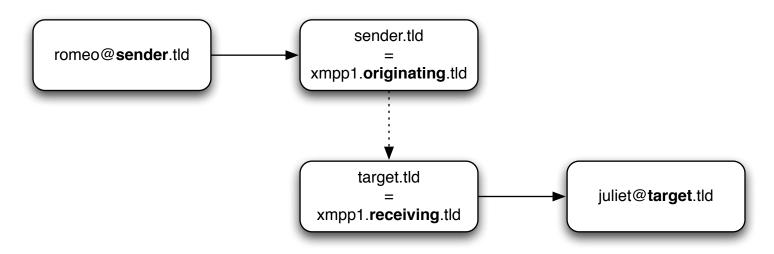
Domain Name Assertions

Richard Barnes
Jonas Lindberg
XMPP @ IETF80

Reminder: The Problem



- When XMPP services are delegated...
- How do you verify that a server is authorized to represent a domain?
- How can the providers in the middle re-use connections for many different customers?

High-level solution

- Authentication:
 - Use DNSSEC to verify SRV records
 - Keep an list of authorized domains per server
- Connection Sharing:
 - Keep a routing table that maps domain pairs to connections
 - Add some signaling to the XMPP stream to update this routing table

DNSSEC

_xmpp-server._tcp.target.tld. 400 IN SRV 20 0 5269 xmpp1.receiving.tld



_xmpp-server._tcp.target.tld. 400 IN RRSIG



Connection	Server Domain Names	Delegated Domain Names
XXX YYY AAA	<pre>xmpp1.receiving.tld xmpp2.receiving.tld paris.example</pre>	target.tld target.tld paris.example

Routing Table



Local	Remote	Connections
sender.tld	target.tld	XXX, YYY
laurence.example	capulet.example	AAA
laurence.example	paris.example	YYY, AAA

Overall Flow

ginating erver 	DNS Server	Receiving Server	
SRV target.tld	>	<	Look up DNSSEC -signed SRV
	 .ginating.tld' to='recei		Establish a stream between server domains
< <features><startt< td=""><td>eiving.tld' to='origina</td><td> i</td><td>STARTTLS, certificates for server domains</td></startt<></features>	eiving.tld' to='origina	i	STARTTLS, certificates for server domains
 <===================================	TLS	=====>	Request permission to send for delegated domains
 	ginating.tld' to='recei	> ting.tld'>	Verify authorization to represent delegated domains
•	sender.tld' to='target SRV sender.tl	> d	Grant permission to cond for delegated demains
	originating.t	>i	Grant permission to send for delegated domains

Status

- The current document is incomplete ...
 - Needs Security Considerations
 - Needs IANA Considerations
 - Needs Operational Considerations
- ... but we think the protocol spec is pretty much there
- Is this the right path?
 - Implementability?
 - Backward Compatibility?