POSH bof

# Session initiation protocol & TLS

Olle E. Johansson, IETF 87 Berlin, July 2013
oej@edvina.net * @oej

v 1.42

# Executive summary:

- SIP security filosophy:

  *"Let's put a nice and soft fluffy TLS wrapper around the connection and it's now secure"* (oej)

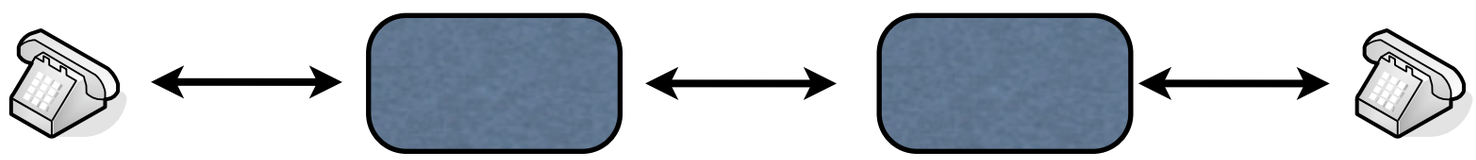
- There's no tradition of datacom-type security in the telco world.
  Customer requirements are <null>.

***"SIP end to end security is like a jumping bunny with a lock in the mouth"***

(old IETF draft)

# The problem with SIP security

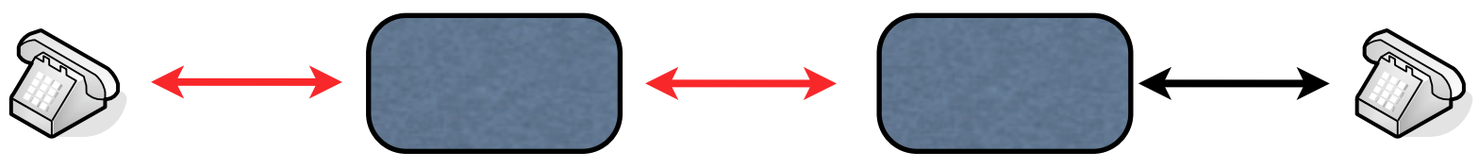
- A lot of servers - proxys and b2bua's - in the signalling path are designed to be man-in-the-middle attack platforms by default
- There's no way for a SIP client to verify remote servers (or authorize their usage).
- Very hard to make sure information integrity is intact for messages between endpoints
- Too much trust put into the network.



# RFC 3261

SIP 2.0

- Defines a SIPS: uri.
- Support for TLS for both SIP: and SIPS: uri's
- Requires SIP TLS server certificates to have canonical hostname. *How is this related to the URI?*
- For SIPS: TLS hop by hop, but not the last hop.
- Summary: *Confusing*.



# RFC 3263

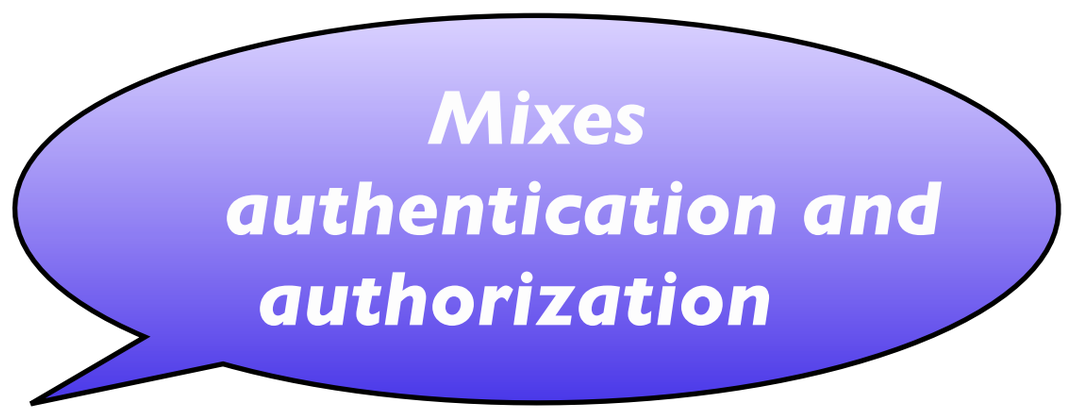
*Locating SIP servers using DNS*

- Requires that the DOMAIN NAME in the hostname part of the URI is in the certificate.
- Released at the same time as RFC 3261 that requires HOST NAME

# RFC 5922

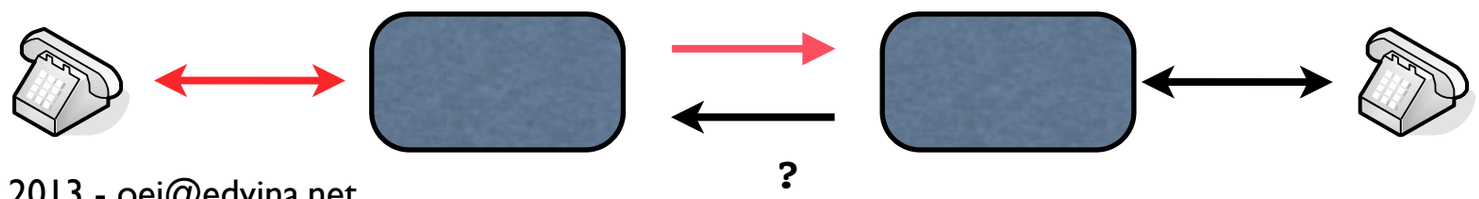
## Sip domain certificates

- Defines SIP Domain certificates and redefines matching between SIP URI and X.509 PKIX certificate. **Certificate now needs to match DOMAIN part of SIP URI.**
- Certificate can have multiple URI's as SubjAltName ext fields.
- Domain in CN is supported if no SAN extensions exists.



# RFC 5923 - Connection reuse

- Requires mutual TLS certificates for reuse of connection - for server2server connections.
- If no client cert, then server needs to open new TLS connection for requests in the other direction.
- Doesn't define how a server knows if a connection is a "client" or a "server"



# Mistakes

- Via and Route headers are in 99% of the cases **IP addresses**.
- Certificates are in 99% of the cases host names or domains == No match.
- RFC 5922 says that these headers needs to be domains (for SRV failover) or host names

# When bad things happen

- Client contacts SIP server over TLS. SIP server tries to reach another server using TLS. Bad stuff happens.
- No error codes, warnings or any other docs on how to signal this situation back.

# SIP Presence

*Funny enough named ”simple”*

- Lot’s of missing information about TLS usage.
  - Server has active role - but how does authorization work?
  - Client can only identify first hop TLS server, which in most cases is NOT the presence server.
- Since SIMPLE is used for certificate handling, phone provisioning, personal presence and chat there are a lot of **serious** security issues here.

# RFC 6072

## SIP certificate distribution

- Use presence to subscribe to another SIP uri's certificate
- Use presence to PUBLISH certificate
- Use presence to provision UA Cert and Key
- Puts a lot of trust in the network
- Requires TLS between ua and certificate handling presence server
- Not compatible with SIP outbound

# SIP & S/MIME

- Well. Yes. Hmmm.

# RFC 4474
# SIP identity

- Federated message integrity and identity assurance
- Protects headers and attachment
- Signed by domain cert
- Domain cert verified by https *(or something else like Dane)*.
- Uses HTTPS to fetch (self-signed) CA cert for SIP domain. ***A cool idea.***

# My draft on SIP DANE usage

- Use DNSsec protection of NAPTR and SRV records for **authorization**
- Use DNSsec/TLSA records for **authentication**
- Focuses on client to server connections
- Needs more work on server2server connection reuse

draft-johansson-dane-sip

# TLS usage

- Don’t mix authorization with authentication
- Encryption - confidentiality - is based on knowing who you are talking to. Without proper authentication you might as well forget it.
- Authorization is different for different protocols (I guess)

# Ahead

- Lots of work needed to clean up TLS requirements - for presence, outbound and more
- The same problem as XMPP with e2e security
- Is S/MIME the way to go, really?
- Where and what are the customer requirements?

# References

- A good overview: http://tools.ietf.org/html/draft-gurbani-sip-sipsec-00