

The Use of TLS in SIP

Vijay K. Gurbani and Alan Jeffrey

draft-gurbani-sip-tls-use-00

Discussion: vkg@lucent.com

65th IETF (March 19-24, 2006)

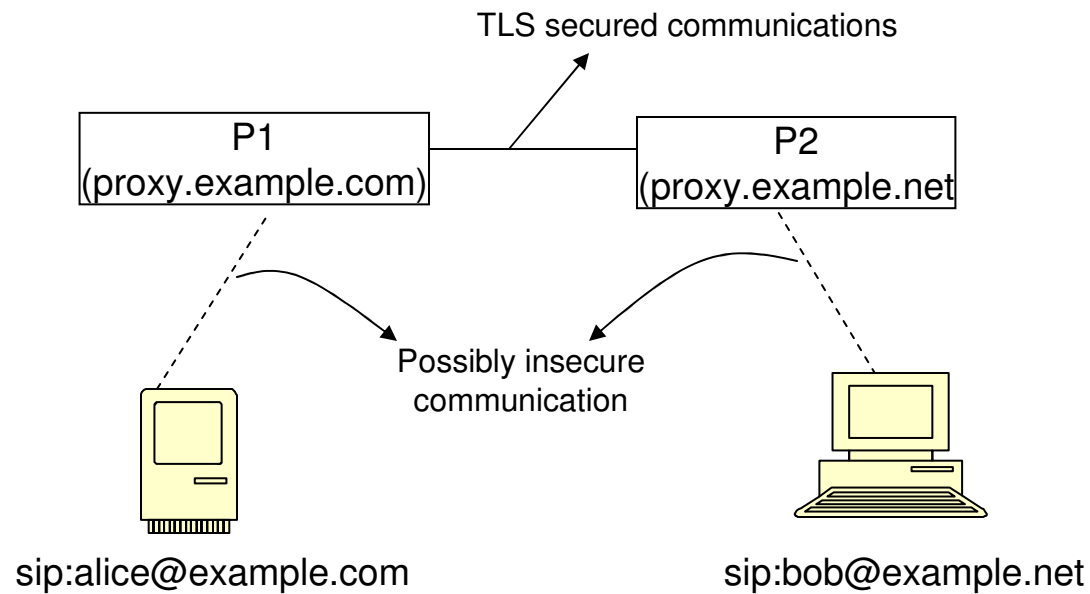
Dallas, Texas

Goals

- Explores the use of TLS in SIP.
- Appendix contains eight TLS test cases.
- A list of open questions for discussion.

Assumptions

Well known SIP trapezoid



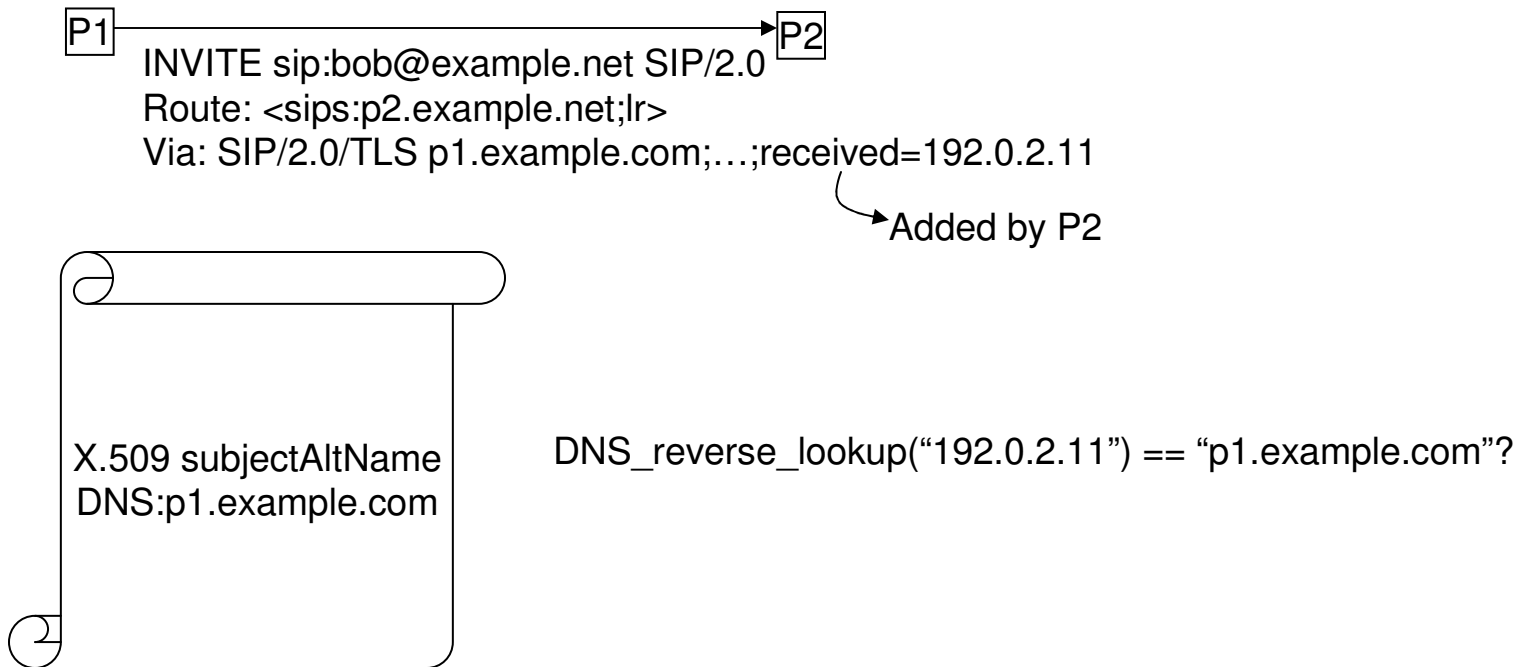
- Endpoints do not possess X.509 certificates.
- P1 and P2 support TLS and have certificates.

Open questions (#1)

- Authoritative Proxy.
 - P2 knows the request came from P1, but P2 does not know that P1 is indeed authorized to act as a proxy for the example.com domain.
 - How can this information be carried?
 - Attribute certificates (rfc3281)?
 - Trait-based authorization/SAML?
 - Existing X.509 fields?

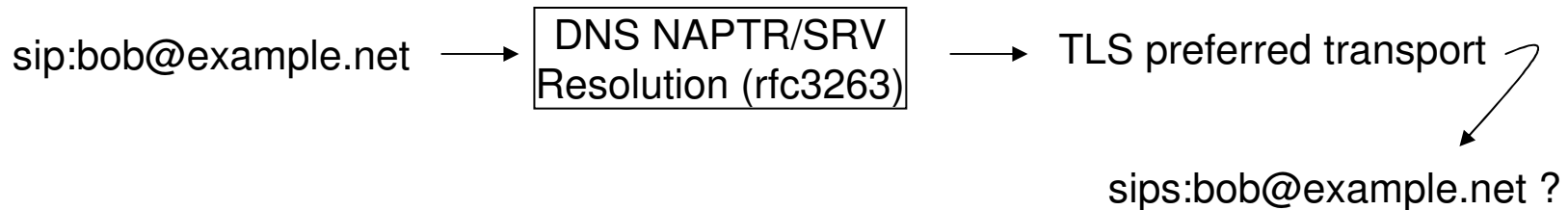
Open questions (#2)

- Mutual authentication.
 - Can rfc3261 do more on mut-auth?

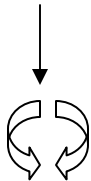
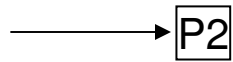


Open question (#3)

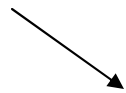
- URI promotion.



Request arrives for
`sip:bob@example.net` but over TLS



Runs routing logic
Forward to `sip:bob@example.org`



May send over TCP

Observations:

- If Bob's paranoid, could use `sips` for forwarding.
- `example.org` domain may have configured DNS for TLS preference.

But, promotion makes the intent more explicit.

Open question (#4)

- Site certificate.

- What does it mean when multiple servers exist for a domain:

- Each server has the same high level name (example.com) in the certificate? The receiver must trust that the peer it is talking to – p1.example.com – is represented by a certificate whose DN or subjectAltName contains “example.com”.
- Each server has its canonical name (p1.example.com, p2.example.com) in the certificate?

Open question (#5)

- Leveraging the Via trail (possible use: spit)

INVITE sips:bob@example.net SIP/2.0

From: <sip:alice@example.org>

To: <sips:bob@example.net>

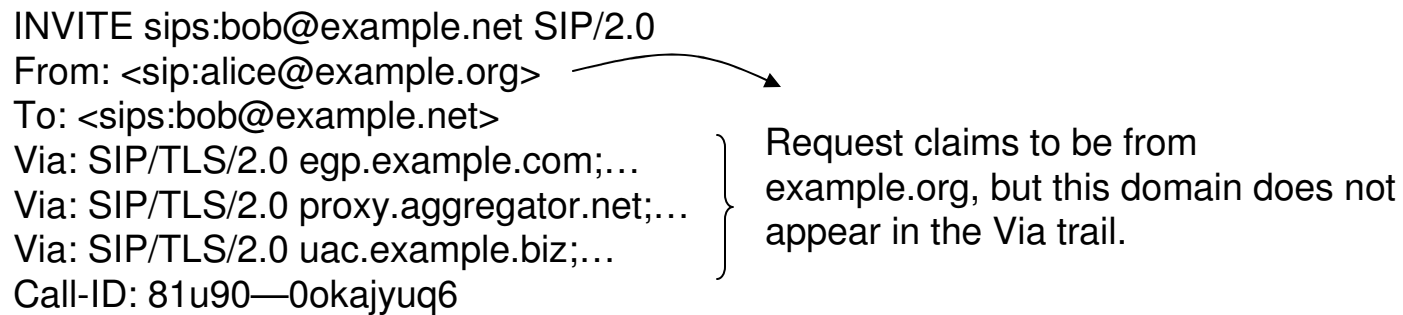
Via: SIP/TLS/2.0 egp.example.com;...

Via: SIP/TLS/2.0 proxy.aggregator.net;...

Via: SIP/TLS/2.0 uac.example.biz;...

Call-ID: 81u90—0okajyuq6

...



Request claims to be from example.org, but this domain does not appear in the Via trail.