Challenges in Securing Multimedia Communications

Vijay K. Gurbani

(Joint work with Alan Jeffrey, Bell Labs)

Security Technology Research Group,

Bell Laboratories/Lucent Technologies, Inc.

June 9th, 2006.

IEEE COMMUNICATIONS SOCIETY

CQR

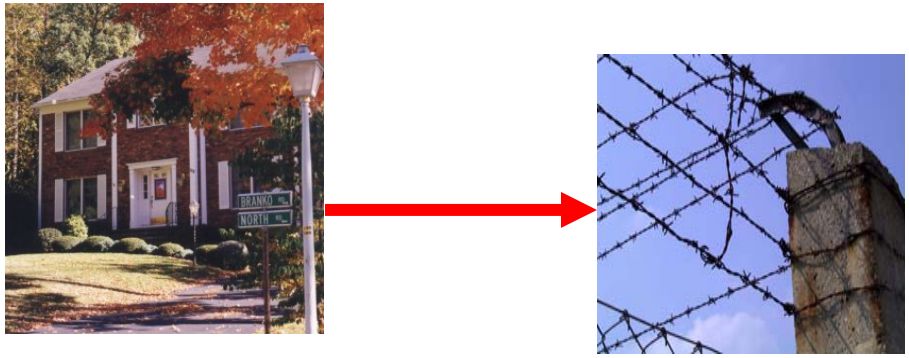
IEEE

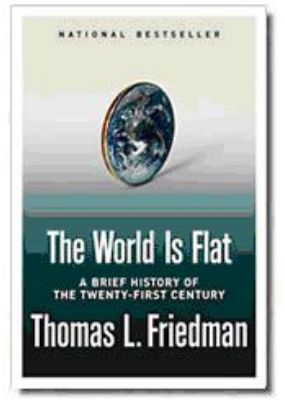
IEEE CQR 2006, London

Lucent Technologies
Bell Labs Innovations

Why are Attacks Increasing?

Explosion of IP networking: ***The world is flat***

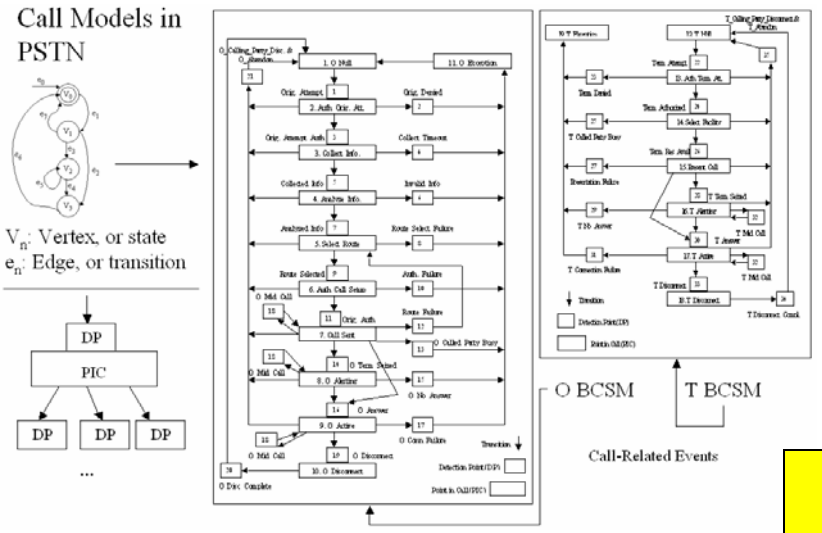


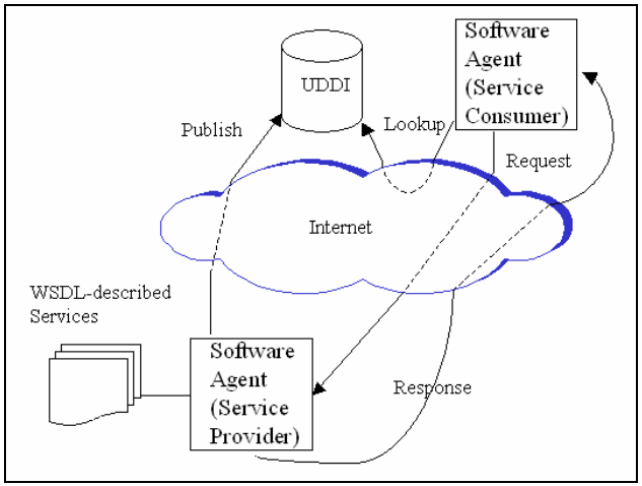


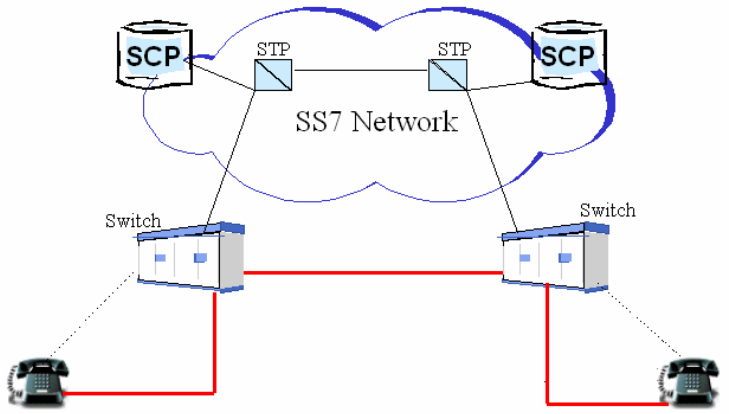
- Limited authentication/trust/encryption
- Wide variety of networked devices
- Limited security checks in software
- Limited security expertise

Why are Attacks Increasing?

Telecommunications, meet the Web!







The "Telecommunications SoA" will be characterized by an emphasis on Security:

- PSTN: Security by obscurity (how many crackers have an IP address? And how many have A- and F- links to PSTN gear?)
- Internet: no one knows you're a …
- Web services: emerging access policies, requester authentication, …

Signaling Security and SIP

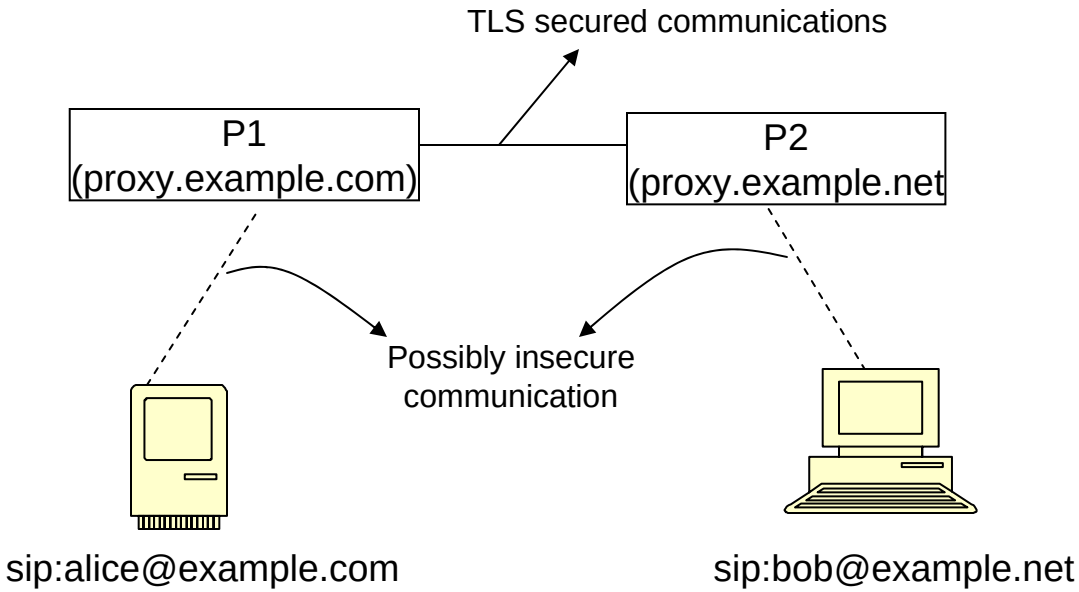
- Four ways to ensure signaling security in SIP:
  - HTTP Digest: prone to eavesdropping, replay, and MiTM attacks. Provides authentication only.
  - TLS: Hop-by-hop SIP transport security; not end-to-end! Provides confidentiality, authentication, encryption.
  - S/MIME: End-to-end signaling and body security. Provides confidentiality, authentication, encryption.
  - IPSec: Layer 3 security. Provides confidentiality and encryption.

Use of TLS in SIP references:

[1] V.K. Gurbani and Alan Jeffrey, “The Use of Transport Layer Security (TLS) in the Session Initiation Protocol,” IETF Internet-Draft, Work in Progress, February 2006, available online <http://www.ietf.org/internet-drafts/draft-gurbani-sip-tls-use-00.txt>
[2] V.K. Gurbani and Alan Jeffrey, “Domain Certificates in the Session Initiation Protocol,” IETF Internet-Draft, Work in Progress, February 2006, available online <http://www.ietf.org/internet-drafts/draft-gurbani-sip-domain-certs-00.txt>

Assumptions

Well known SIP trapezoid



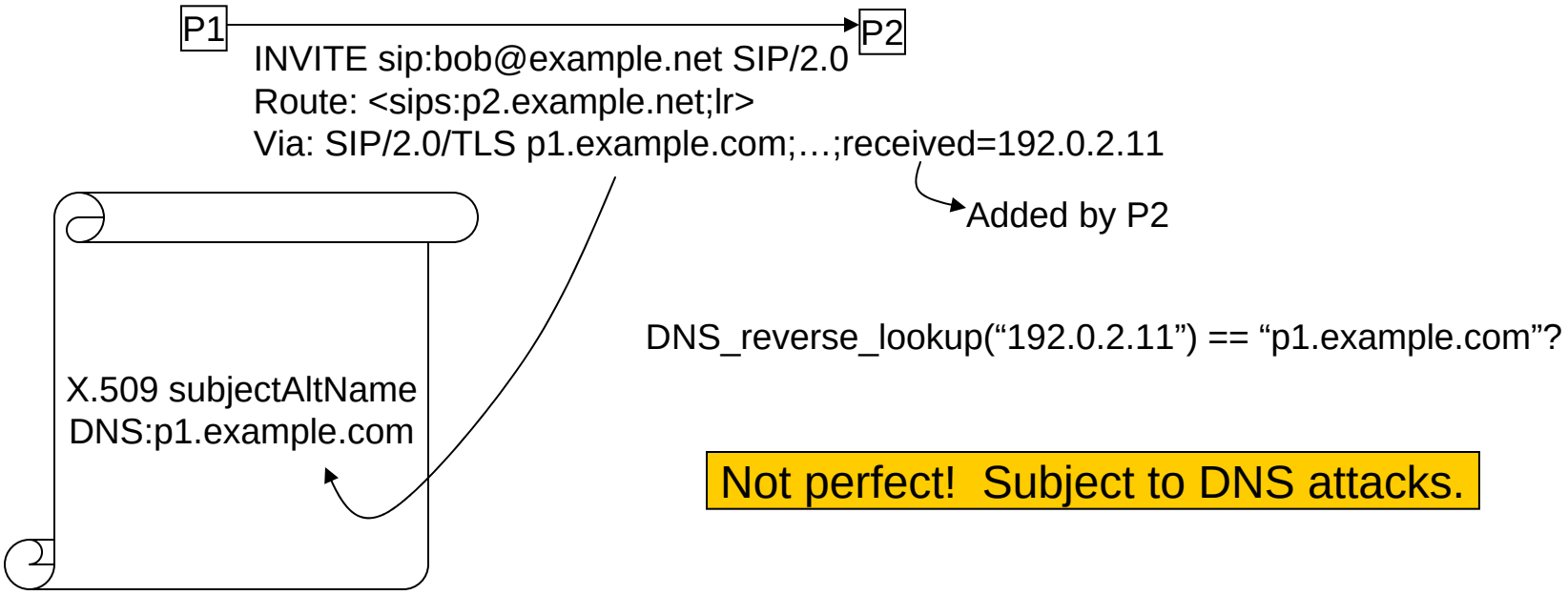
- Endpoints do not posses X.509 certificates.
- P1 and P2 support TLS and have certificates.

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?

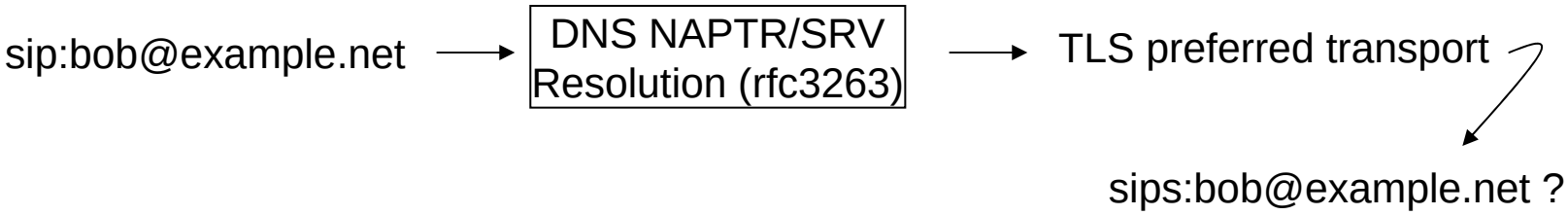
Open questions (#2)

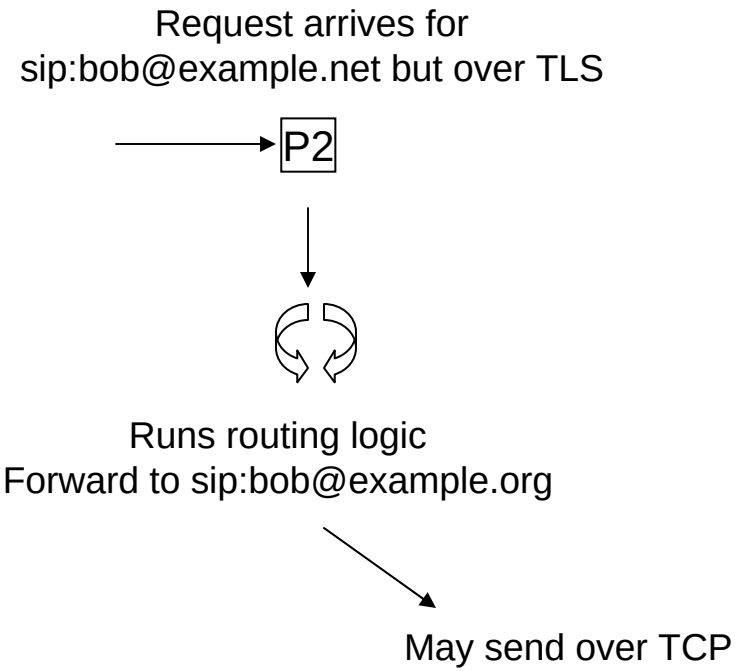
- Mutual authentication.
  - Can rfc3261 do more on mut-auth?



Open question (#3)

- URI promotion.





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

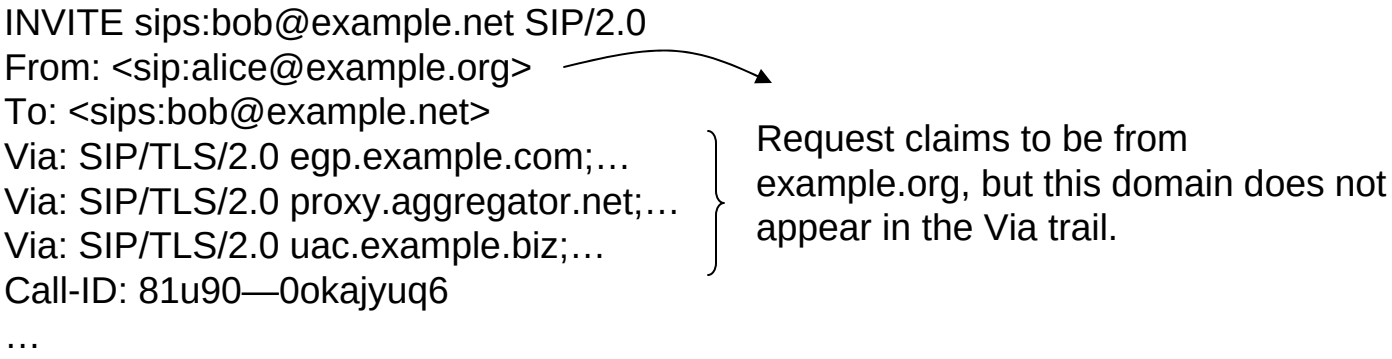
But, promotion makes the intent more explicit.

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)



Summary

- Next steps:
  - Fair amount of discussion in WG on site certificates
    - If inbound proxy presents certificate that asserts an identity of sip:example.com, then this is sufficient trust guarantee. Canonical hostname match is not required.
    - Maintain two identities in the certificate (sip:example.com and sip:p1.example.com).
  - New draft on interpreting “sips” (draft-audet-sip-sips-guidelines-00).
  - More discussion to be continued on WG mailing list.
- What does all this mean for VoIP deployments?
  - Provide a sufficient anchor of trust in the peer.
  - Lay out the rules of processing and operating assumptions to ensure minimal ambiguity during implementation.
  - Increase trust in the overall VoIP system.

Conclusion/Q&A.

Thank You!