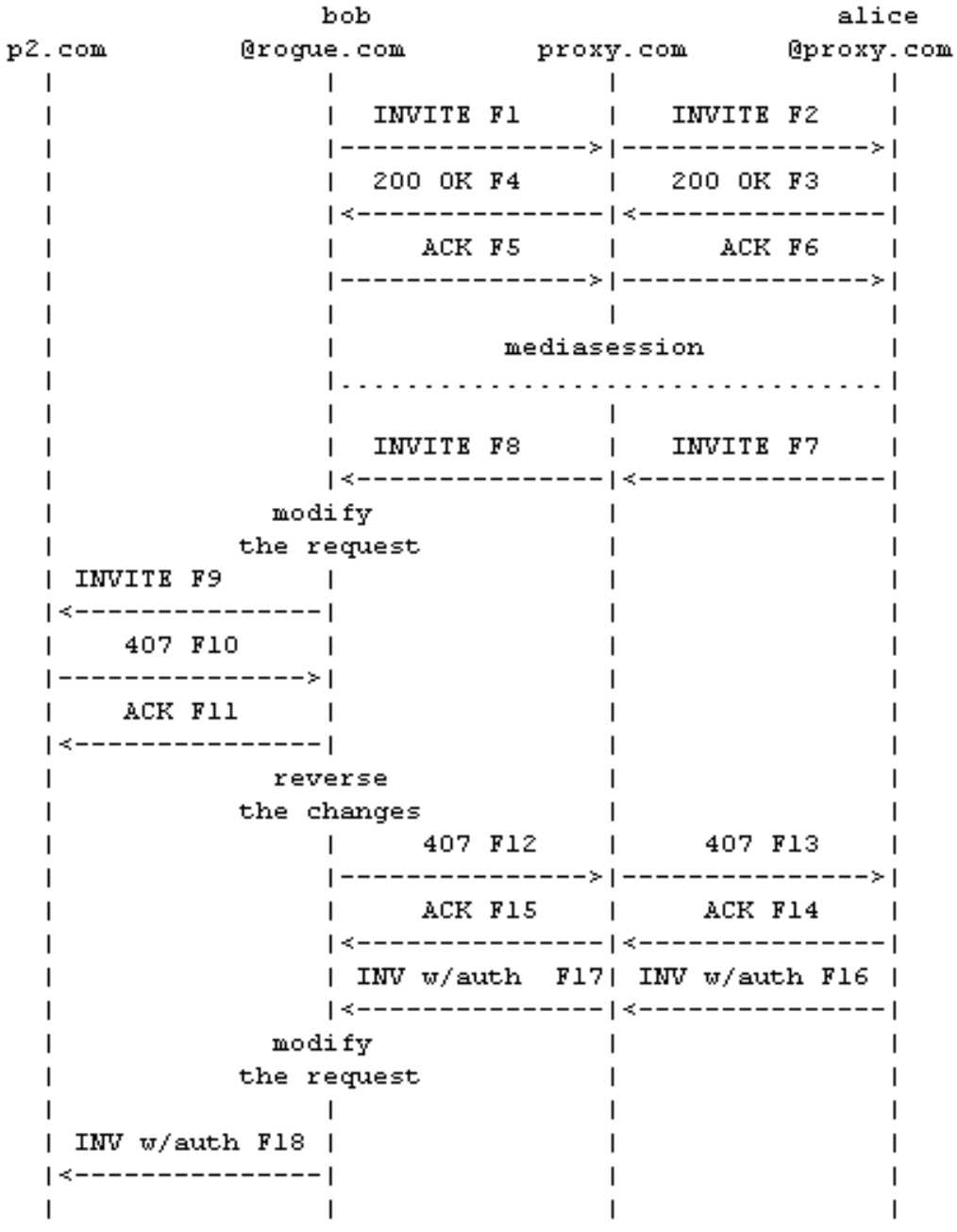
draft-state-sip-relay-attack-00

74th IETF San Francisco

Radu State radu.state@uni.lu
Raphael Coeffic rco@iptel.org


bob
alice
p2.com
@rogue.com
proxy.com
@proxy.com
INVITE F1
INVITE F2
200 OK F4
200 OK F3
ACK F5
ACK F6
mediasession
INVITE F8
INVITE F7
modify
the request
INVITE F9
407 F10
ACK F11
reverse
the changes
407 F12
407 F13
ACK F15
ACK F14
INV w/auth F17
INV w/auth F16
modify
the request
INV w/auth F18

Purpose and scope

- This draft focuses on documenting an attack, which has been tested and does work against several commercial providers.

- What is the purpose of the document?
  - Make SIP providers aware of the risks.

Next steps?

- Proposed steps:
  - Remove section 4 (i.e. “Possible Mitigations“).
  - Update the document with the comments from the mailing list which are focused the problem statement.

- Do we want to acknowledge the attack by publishing it?