

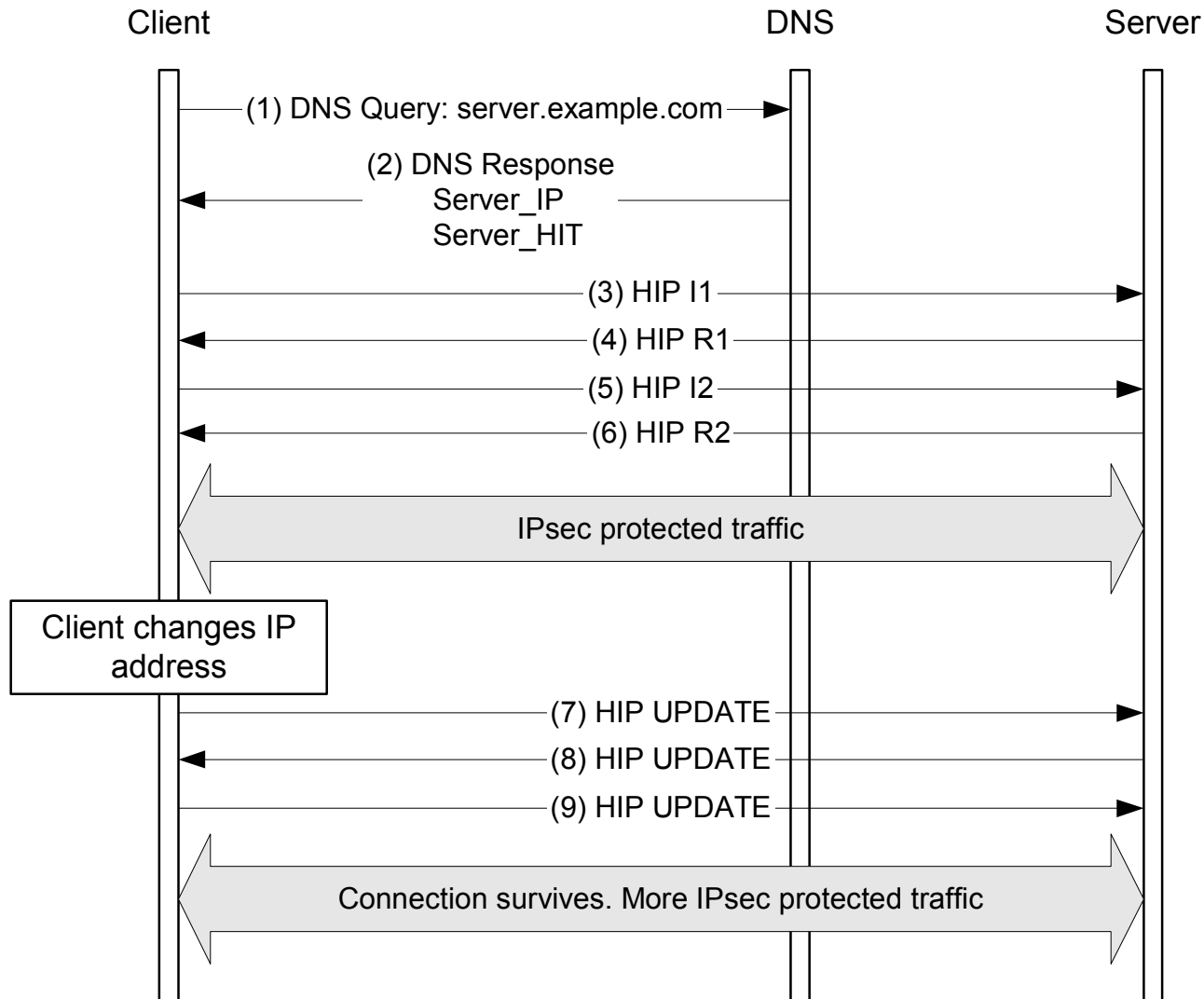
# Using SIP as a Rendezvous Mechanism for HIP End-points

Gonzalo.Camarillo@ericsson.com

# Contacting a HIP host

- An endpoint contacting a HIP host needs:
  - HIT
  - IP address to send the initial I1 packet
- This information is obtained in different ways depending on the service
  - HTTP, SMTP, telnet, ...
    - Resolving an FQDN using the DNS
  - VoIP, video conferencing, messaging, fax over IP, ...
    - Using SIP

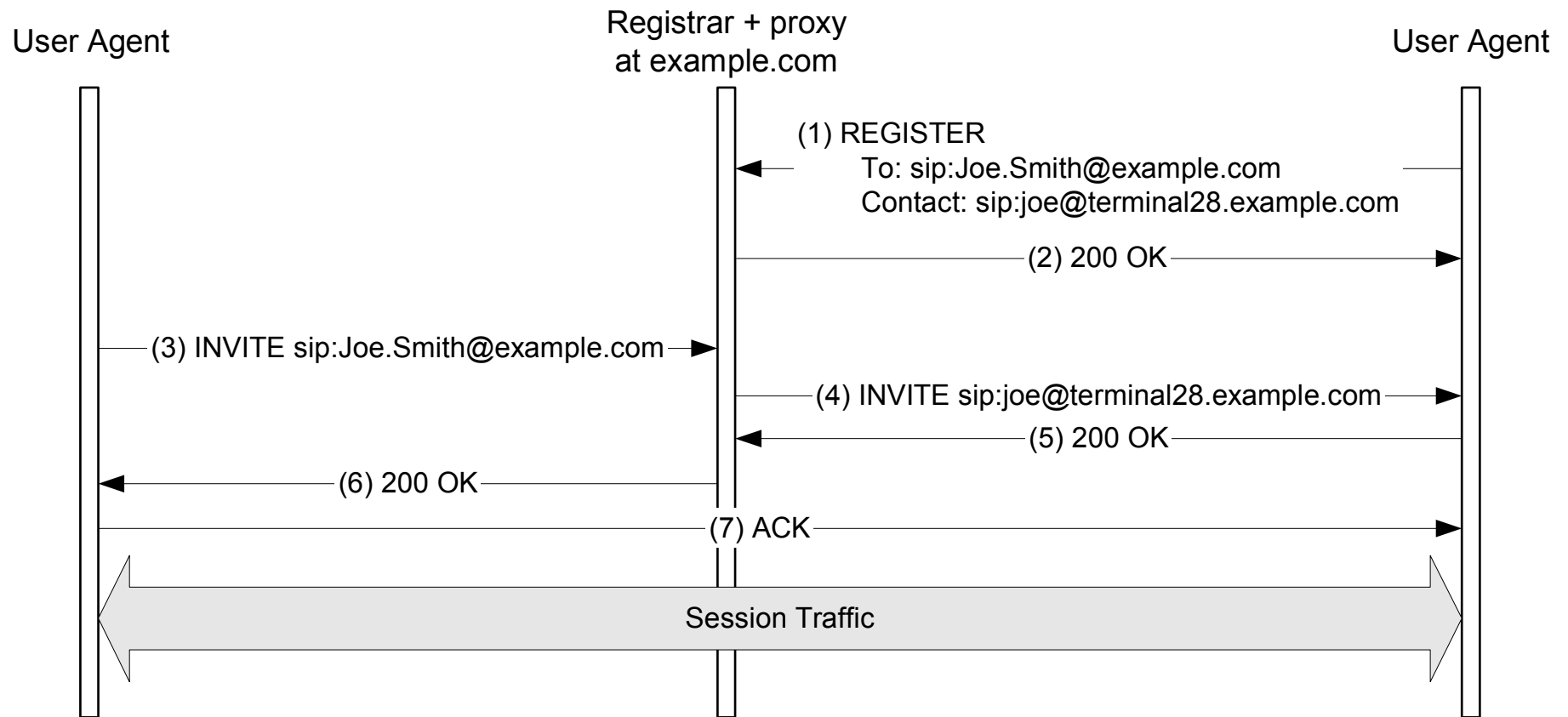
# DNS Extensions for HIP



# Establishing a Session with SIP

- A session description contains the information needed to establish the session
  - E.g., IP addresses, ports, transports, codecs, ...
- SIP delivers a session description at the user's current location
  - Carried using MIME (i.e., as an email attachment)
- Two-way offer/answer exchange
  - Rules about how to generate an answer given a particular offer
- Three-way handshake
  - INVITE – 200 (OK) – ACK

# SIP Message Flow



# Using SIP as a Rendezvous Mechanism for HIP

- Include the HIT of the host in the session description
  - In addition to the IP address and all the other parameters
- HIP handles
  - Media encryption
  - Multihoming
  - Device mobility (both for SIP and for media traffic)
- SIP handles user mobility
  - Different devices
  - It uses the Replaces mechanism

# Security in RTP Sessions

- HIP implies using of IPsec
  - Overhead
  - Disallows using header compression
- SRTP
  - Does not add a header or a trailer (depending on the mode of operation)
  - Does not encrypt the RTP headers
- If HIP did not imply using IPsec, it could be used as a mobility and multihoming solution for RTP sessions

# DoS Prevention

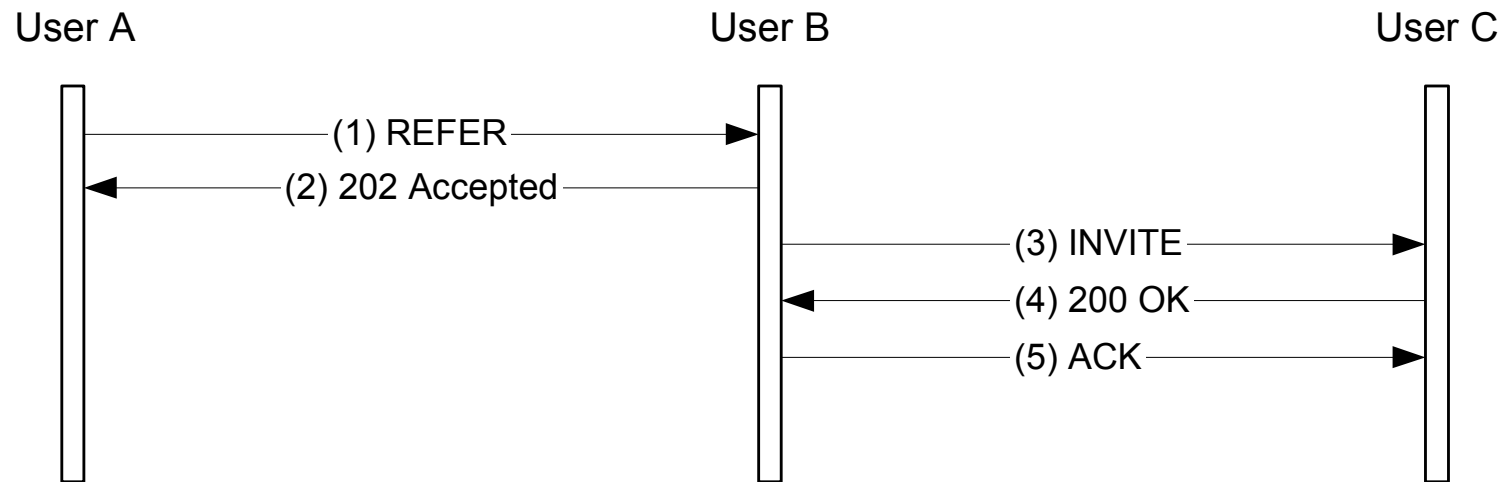
- Attacker places the victim's IP address in an offer
- Answerer sends traffic to the victim
  - Bombing attack
- The use of HIP prevents this attack
  - HIP base exchange takes place before media is transferred
  - Alternative mechanisms: ICE or DCCP

# Leap of Faith

- Both HIP and SIP use the leap of faith
  - Assume that the first time a connection is established the endpoints were not under attack
  - SIP uses self-signed certificates and S/MIME
- Proposal
  - Use self-signed certificates at the SIP level
  - Associate a user with a public key
  - The user's private key is used to sign
    - Session descriptions that contain HITs
    - Host certificates to be used in HIP

# Referrals

- SIP handles referrals to SIP URIs
  - Offer/answer is used to obtain the HIT of the new host



- Native HIP referrals outside the scope of this paper
  - Referrals to a HIT

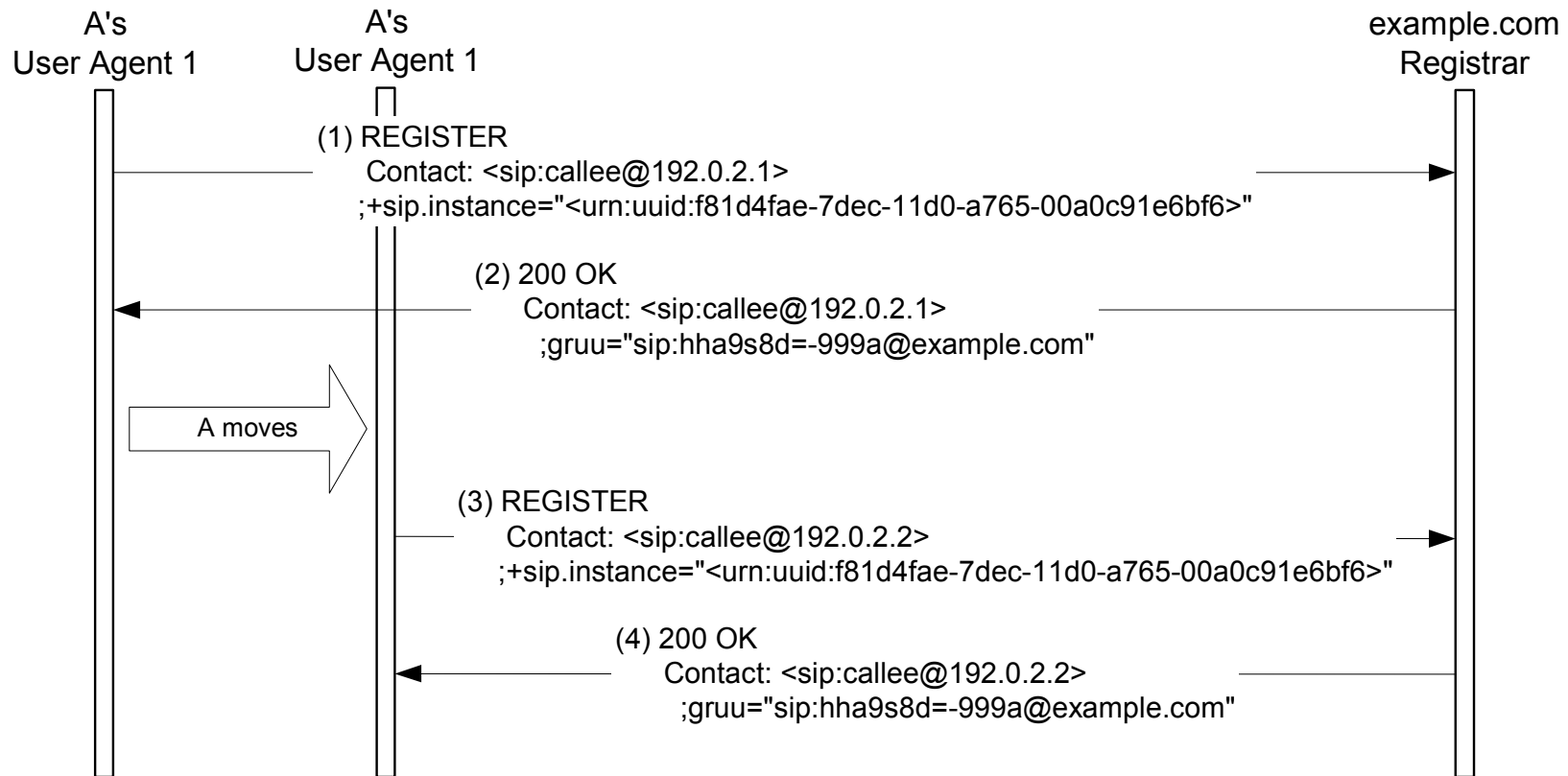
# Using HIP to Carry SIP Traffic

- Hop-by-hop security
  - TLS was chosen (instead of IPsec) because the application is aware of it
  - HIP could be used as an application level hook to use IPsec between SIP entities
    - I.e., a connection to a HIT is protected using IPsec

# GRUUs and Instance Identifiers (1)

- GRUU (Globally Routable UA URI)
  - URI that always route to a particular UA instance (e.g., to my mobile phone)
  - Instance identifiers help registrars keep track of individual UAs over registrations

# GRUU and Instance Identifiers (2)



# GRUU and Instance Identifiers (3)

- Use HITs as instance identifiers
  - Works well for hardware-based UAs
  - Does not work well for
    - Software-based UAs that may run in different hosts
    - Different software-based clients running on the same host
- HIP could be used by proxies to authenticate UASs before sending them a request
  - No need to maintain a TLS connection up all the time
  - UASs do not usually have server certificates

# Conclusions

- SIP can be used as a rendezvous mechanism between HIP hosts
  - Adding HITs to existing session description formats such as SDP is trivial
- Sessions established with SIP can benefit from HIP's mobility, multihoming, and security support
  - IPsec in HIP could be optional, though
- HIP can be used to provide hop-by-hop IPsec-based security for SIP nodes
- HITs can be used as UA instance identifiers
  - UAS authentication for incoming requests