HIP-based Peer-to-Peer SIP

Joakim Koskela
24 July 2007
Introduction

• Part of the HIIT TrustInet project
  – Building a better, more trustworthy, internet
  – This prototype used to study trust and reputation schemes in P2P
    • SPAM / SPIT prevention in P2PSIP

• Peer-to-Peer Session Initiation Protocol (P2PSIP)
  – Used to negotiate how connections are established
    • VoIP, Video calls, screen sharing, white boarding, IM, file transfers etc..
  – DHT replaces centralized registrar servers

• Challenges and open questions in this distributed model
  – NAT traversal
  – New security model
  – Peer / Client separation and protocol

• HIP provides tools for these
System overview

- DHT built on connections on top of HIP
- Data connections also on HIP
- Peers provide the needed services
  - RVS and relay for NAT traversal
  - Multiple RVS registrations
Application overview

- Software consists of HIPL stack, P2PSIP proxy and SIP application
  - Existing SIP applications can be used unmodified
- Each peer may offer additional services advertised in the overlay
  - Both SIP (e.g. voicemail) and HIP (RVS and relays)
- P2PSIP proxy handles authentication and identity management transparently
  - Based on signed certificates
Implementation notes

• Nokia Internet tablet (N800) target platform
  – HIPL stack and SIP applications available
• P2PSIP proxy lightweight & efficient, few dependencies
  – osip2, libxml2, glib, openssl
• Currently status
  – Basic SIP functionality works from application's point-of-view
    • Registration, finding users
    • IM, VOIP and video calls
    • 'Good enough' SIP support
  – The P2PSIP proxy provides a mediaprox
    • Connections should be formed directly between HITs
  – No modification needed to applications
    • Tested with applications such as Ekiga, Gaim, MiniSIP
  – OpenDHT used for storage
  – Native HIP not utilized yet
    • No NAT traversal
Open issues

• Client / Peer protocol
  – Currently a very simple binary format on TCP

• DHT algorithm and overlay structure
  – Multiple simultaneous overlays
    • ISP account 'always on'
    • Work-related only when in office WLAN
    • Ad-hoc

• Improved NAT traversal needed from HIP

• Incentive to offer services
  – Might be solvable using the reputation schemes?

• Can HIP be used for more?
  – Joining networks
  – Locating services
Summary

• A prototype for conducting research on
  – Trust and reputation systems for fighting SPIT in P2P environments
  – Tool to get more real-life experience of using HIP
  – Tool to study P2PSIP

• HIP used for
  – NAT traversal
  – Authentication, security
  – Mobility

• Sets new requirements for HIP
  – Improved NAT traversal