



# Simple Peer-to-Peer SIP Privacy

Joakim Koskela  
MobiSec 2009

# Introduction

- Privacy in computer networks important
  - *What* are we protecting, and from *Who*?
- Centralized systems require us to trust the service provider
  - Content can be encrypted, but everything else is exposed
  - Usually not a concern for end-users
- In P2P networks, the peers are the service provider
  - We should re-evaluate our relationship with the services
- What are the privacy concerns in P2P systems?
- How can these be solved and how does it affect the usability?

# P2P Communication Systems

- A peer network is used to collectively provide the service
  - Connection set-up and presence
  - Distributed database for storing connectivity information, presence
- Peer network accessed through a DHT-like interface
  - Simple key-based put/get interface
  - Keys well-known (e.g., hash of the user's name)
- Strong (public-key based) identities
- IETF P2PSIP fits into this model
  - Problem discussed in draft, but not addressed

# Problem description

- To be reached, we need to place our connectivity information into the peer network
  - Exposes our status and location
- To be able to reach someone, we need to retrieve that person's information
  - Reveals call intent
- We might trust Skype, but certainly not everyone in a peer network
  - Abroad – Good time to break into your home!
  - Blackmail!
- How do we guarantee privacy in fully distributed communications systems?

# Privacy model

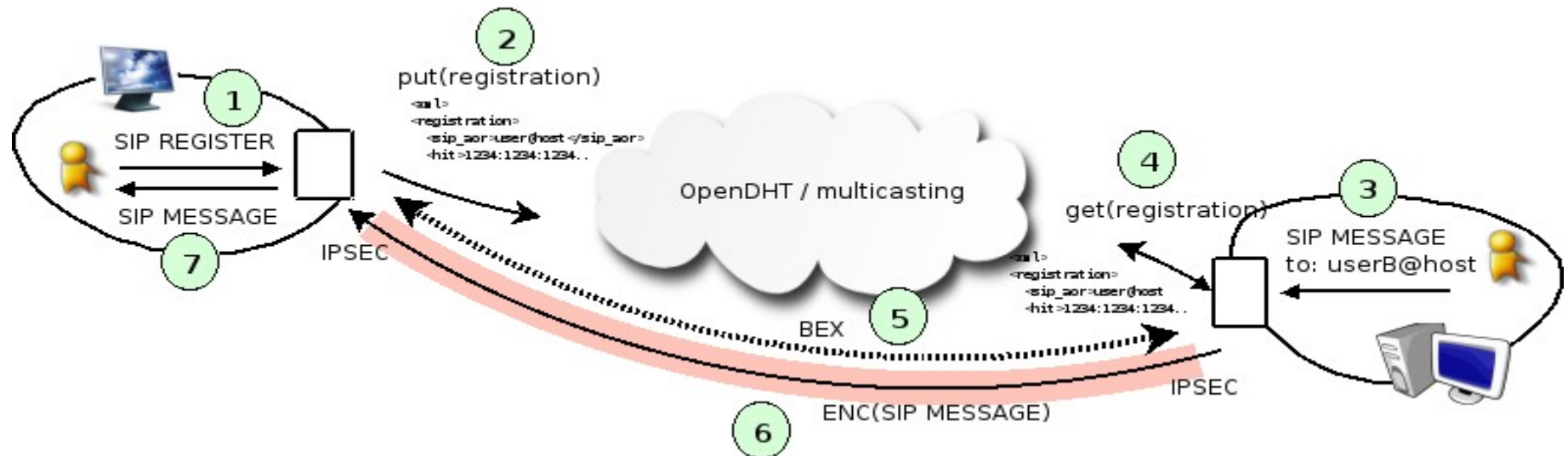
- **Step 1:** Encrypt the connectivity information
  - Using intended recipient's public key or common key shared with a group
  - Bystanders can not determine what the packet contains
  - Still reveals that *something* is taking place
- **Step 2:** Obfuscate the storage keys
  - Using an automatically re-negotiated shared secret
  - Bystanders can not determine *who* published the packet, *what* it contains or for *whom* it is intended
    - .. or if it even contains valid data!

# Challenges

- Packets need to be published once for each friend
  - Overloading the network with data
  - Overloading the client with public-key operations
- Bootstrapping problem
- The effect on usability
  - The model affects who we are able to contact
    - Users online might seen offline
  - How do we present this to the user? How should it be controlled?
- Not to limit who is able to contact you, but hide who *does*

# Implementation

- Linux-based local SIP proxy
  - Compatible with SIP-based VoIP/IM clients
  - Nokia N810 Internet Tablet
- Client-Server (CS) signaling converted into P2P operations
  - Multicast, OpenDHT / OpenLookup used for lookup
- Connectivity information published in XML-formatted *registration packages*



# Implementation

- Privacy enhancements controller through a presence-like *privacy mode* setting
  - The use of *open* and *secret* lookup keys
- Three modes:
  - **Open**
    - Registration packages published using both keys
    - Lookup only with open key
  - **Relaxed**
    - Lookup with secret (if possible), otherwise using open key (but not as fallback!)
  - **Paranoid**
    - Uses only the secret keys
- Introduces restrictions even though we have a shared secret
  - **Open** to **Paranoid** not possible

# Traffic trace

Time	Source	Target	Data
..			
157	10.0.0.64	(all)	Lookup(vd4o2lZJ/yAVY9+pgU+Fz9Uh+PA=)
157	10.0.0.48	10.0.0.64	Registration package for Carol (1527 bytes)
157	10.0.0.64	10.0.0.48	HIP BEX (HIT1 to HIT2)
162	10.0.0.64	10.0.0.48	Small burst of ESP
162	10.0.0.48	10.0.0.64	Small burst of ESP
165	10.0.0.64	10.0.0.48	Small burst of ESP
165	10.0.0.48	10.0.0.64	Small burst of ESP

Hash	SIP AOR	IP address
I6XlisZMhWcf07gdVni4HdGZLbA=	alice@p2psip.hiit.fi	10.0.0.64
uD0I1fxZGRC4ghvHrbGSx+Ia6xM=	bob@p2psip.hiit.fi	10.0.0.68
vd4o2lZJ/yAVY9+pgU+Fz9Uh+PA=	carol@p2psip.hiit.fi	10.0.0.48
/+aYyc+gJMwccgRoV3QoBcdyGfk=	dave@p2psip.hiit.fi	10.0.0.54

Time	Source	Target	Data
..			
122	10.0.0.18	(all)	Lookup(2qjJ8rllbzgk5QivRZ8PfZ4XSB0=)
124	10.0.0.12	10.0.0.18	Encrypted data (2796 bytes)
124	10.0.0.18	10.0.0.12	HIP BEX (HIT5 to HIT6)
130	10.0.0.18	10.0.0.12	Continuous flow of ESP
131	10.0.0.12	10.0.0.18	Continuous flow of ESP

# Conclusions

- We need to re-evaluate privacy in P2P-provided services
  - We cannot trust the service provider anymore
  - This affects the usability
- We have experimented with a simple, straight-forward mode
  - Easily adaptable to other systems
  - Concentrates on application-level data
  - Introduces *privacy modes* for controlling the behavior
- Users are still vulnerable to other means of analysis
  - Source-address hiding
  - Traffic patterns



# Thank you

Questions & comments?

For more information:

[joakim.koskela@hiit.fi](mailto:joakim.koskela@hiit.fi)  
<http://www.trustinet.net>  
<http://www.infracore.net>