Lawful Interception of VoIP in Highly Decentralised Systems

Jan Seedorf
(jan.seedorf_at_nw.neclab.eu)
NEC Laboratories Europe
Heidelberg, Germany
Intention of the talk

• Give a technical overview on VoIP signalling without central components (P2PSIP) and current standardisation of P2PSIP in IETF

• Identify the implications on Lawful Interception of such a serverless / highly decentralised signalling approach

• Discuss possible solutions with respect to future standardisation
Outline

• Introduction: Lawful Interception of VoIP
• VoIP Signalling without Servers: P2P-SIP
• Technical Implications of P2P Paradigm for Lawful Interception of VoIP
• Possible Solutions and Standardisation Efforts
• Conclusion
Introduction

Lawful Interception of VoIP
Lawful Interception

- **Lawful Interception**
  - authorised wiretapping of communications carried out by law enforcement organisations

- **Some Terminology**
  - LEA: Law Enforcement Agency
  - IRI: Intercept Related Information
  - CC: Content of Communication

- **Standardisation**
  - Handover Interfaces standardised by ETSI/TC LI
    - H1 – administrative information
    - H2 – Delivery of IRI
    - H3 – Delivery of CC
  - For more info see presentations on Lawful Interception from 1\textsuperscript{st} & 2\textsuperscript{nd} ETSI security workshop
ETSI Reference Model for Lawful Interception

Network Internal Functions

Intercept related information (IRI)

Content of communication (CC)

IRI mediation function

CC mediation function

NWO/AP/SvP's domain

LEA domain

LI handover interface HI

ETSI TR 102 528
Challenges for Lawful Interception of VoIP

• Different Types of VoIP Service Architectures
  • Service Provider, Access Provider and Network Operator can be different entities
  • Signalling (IRI) and media (CC) can take different routes
    ➢ With a session border controller, signalling and media are fully controlled by the VoIP service provider
    ➢ With a regular SIP proxy media packets do not necessarily traverse the server of the VoIP service provider
    ➢ Standard IETF SIP allows signalling to go directly between terminals once the `SIP-Invite` has reached the callee

• Consequences
  ➔ IRI and CC may be delivered by different entities
  ➔ Node (and entity) for intercepting the CC have to be determined in real-time from the IRI
ETSI Reference Model for LI in IP networks

LI Administration Function (AF)

Intercept Related Information Internal Interception Function (IRI-IIF)

Content of Communication Internal Interception Function (CC-IIF)

CSP DOMAIN

Lawful Interception Mediation Function (MF)

LEA

LEA Administration Function

Law Enforcement Monitoring Facility (LEMF)

ETSI TR 102 528
VoIP Signalling without Servers: P2P-SIP
P2P-SIP: how does it work technically?

• What is P2P-SIP?
  • Using a peer-to-peer network as a substrate for SIP user registration and location lookup

• SIP registrations are not stored on a server but instead distributed in a P2P network at participating nodes
  • A scenario where we do not have any trust at all in the registrar, because
    ➢ arbitrary clients/terminals are storing registrations
    ➢ Responsibility among nodes for registrations changes frequently

=> no pre-established trust between SIP-registrar and LEA possible
P2P-SIP: Basic Overview

P2P node (can be the user’s SIP phone)

Hash of the SIP-URI = keyID

Content stored: Current location (IP-address) for SIP-URI

Lookup Location for Bob’s SIP URI

Join DHT

SIP:alice@atlanta.com

SIP:bob@biloxy.com
P2P-SIP: Registration and Location

1. Bob's node joins the DHT
2. Alice's node joins the DHT
3. Bob registers his URI with the DHT
4. Alice wants to call Bob
5. DHT delivers the node (+IP-address) responsible for Bob's URI to Alice (node 215)
6. Alice contacts node 215 to get Bob's IP-address (without using the overlay)
7. Alice and Bob negotiate parameters and set up their session directly (without using the overlay)
P2PSIP: IETF Standardisation

• P2PSIP is an official IETF working group:
  • “The Peer-to-Peer (P2P) Session Initiation Protocol working group (P2PSIP WG) is chartered to develop protocols and mechanisms for the use of the Session Initiation Protocol (SIP) in settings where the service of establishing and managing sessions is principally handled by a collection of intelligent endpoints, rather than centralized servers as in SIP as currently deployed.” (http://www.ietf.org/html.charters/p2psip-charter.html)

• More info: http://www.p2psip.org/
P2PSIP: IETF work (only 2007)

- L. Ch. Li, Y. Wang, Different types of nodes in P2PSIP (November 2007) draft-li-p2psip-node-types-00 (txt)
- C. Jennings, B. Loweank, E. Rescorla, J. Rosenberg, REsource LOcation And Discovery (RELOAD) (November 2007) draft-bryan-p2psip-reload-02 (txt) (html)
- E. Marocco, E. Iovov, XPP Extensions for Implementing a Passive P2PSIP Overlay Network based on the CAN Distributed Hash Table (November 2007) draft-marocco-p2psip-xpp-can-01 (txt)
- L. Li, Ch. Zhang, Y. Wang, Y. Ji, A SIP-based P2PSIP Client Protocol (November 2007) draft-li-p2psip-client-protocol-00 (txt)
- E. Cooper, A. Johnston, P. Matthews, An ID/Locator Architecture for P2PSIP (November 2007) draft-matthews-p2psip-id-loc-00 (txt)
- I. Baumgart, Peer-to-Peer Name Service (P2PNS) (November 2007) draft-baumgart-p2psip-p2pns-00 (txt)
- XingFeng Jiang, HelWen Zheng, Service Extensible P2P Peer Protocol (November 2007) draft-jiang-p2psip-sep-00 (txt)
- Hwen Zheng, Xingfeng Jiang, P2PSIP Client Protocol (October 2007) draft-zheng-p2psip-client-protocol-00 (txt)
- S. Cirani, L. Velti, A Kademia-based DHT for Resource Lookup in P2PSIP (October 2007) draft-cirani-p2psip-dsisp-dhtkademia-00 (txt)
- G. Garcia, P2PSIP bootstrapping using DNS-SD (October 2007) draft-garcia-p2psip-dns-SD-bootstrapping-00 (txt)
- M. Matuszewski, J.-E. Ekberg, and P. Laitinen, Security requirements in P2PSIP (July 2007) draft-matuszewski-p2psip-security-requirements-01 (txt)
- D. Bryan, E. Shim, and B. Lowekamp, Use Cases for Peer-to-Peer Session Initiation Protocol (July 2007) draft-bryan-p2psip-usecases-00 (txt) (html)
- C. Jennings, J. Rosenberg, and E. Rescorla, Address Settlement by Peer to Peer (July 2007) draft-jennings-p2psip-asp-00 (txt) (html)
- D. Bryan, S. Baset, M. Matuszewski, and H. Sinnreich, P2PSIP Protocol Framework and Requirements (June 2007) draft-bryan-p2psip-requirements-00 (txt)
- E. Cooper, A. Johnston, and P. Matthews, A Distributed Transport Function in P2PSIP using HIP for Multi-Hop Overlay Routing (June 2007) draft-matthews-p2psip-hip-hop-00 (txt) (html)
- E. Marocco and D. Bryan, Interworking between P2PSIP Overlays and Conventional SIP Networks (March 2007) draft-matthews-p2psip-interwork-01 (txt) (html)
- D. Bryan, B. Lowekamp, and C. Jennings, dSIP: A P2P Approach to SIP Registration and Resource Location (February 2007) draft-bryan-p2psip-dsisp-00 (txt) (html)
- C. Jennings, Security Mechanisms for Peer to Peer SIP (February 2007) draft-jennings-p2psip-security-00 (txt)
- XingFeng Jiang, The requirement of P2PSIP Peer protocol (February 2007) draft-jiang-p2psip-peer-protocol-00 (txt)
- E. Cooper, A. Johnston, and P. Matthews, Bootstrap Mechanisms for P2PSIP (February 2007) draft-matthews-p2psip-bootstrap-mechanisms-00 (txt) (html)
- J. Hautakorpi and G. Camarillo, The Peer Protocol for P2PSIP Networks (February 2007) draft-hautakorpi-p2psip-peer-protocol-00 (txt)
IETF P2PSIP WG: Status Quo

- Many open issues
  - Architecture not clearly defined yet
  - Nat traversal / Routing
  - Security / Replication of SIP registrations

- What seems to be clear...
  - Signalling (after locating the callee through the overlay) and Call Content (RTP) can go directly peer-to-peer
  - Central Enrollment Server, but only for node-ID assignment
    - To protect against virtual node-IDs (so-called Sybil-attacks) and chosen location attacks
    - Central authority is not on every signalling path
    - Specifically, the enrollment server is not involved during call setup
Technical Implications of P2P Paradigm for Lawful Interception of VoIP
Challenges for LI imposed by P2P paradigm

• No server involved in call-setup
  • No central component on the signalling path
  • No static relationship between target identity and first application-layer signalling hop

• Routing of signalling messages
  • Incoming and outgoing calls take different routes
  • The outgoing signalling “proxy” is different for every callee
Challenges for LI imposed by P2P paradigm

• Distributed Hash Table is highly dynamic
  • The node responsible for storing the location of a SIP-URI changes frequently
  • Overlay links in participating nodes change frequently
  → For the same callee the first signalling hop may be different with every call

• Mobility
  • User mobility already a problem in server-based SIP signalling
  • Increased problem in P2PSIP because also mobility on signalling layer
Challenges for LI imposed by P2P paradigm

• Service Provider may not be involved in signalling
  • Operator role in P2PSIP deployment not defined yet
  • Service provided may only cover enrollment (node-ID assignment)
  • Registrations of users (identity/location bindings) are possibly stored at end-users’ terminals
  • Signalling will not traverse proxies once a session has been set up
    ➢ After call-setup, all signalling can go directly peer-to-peer
Possible Solutions and Standardisation Efforts
Footprint in Terminals

• Suggested solution by some government agencies for Lawful Interception of VoIP / IP traffic in general

• Advantages
  • VoIP signalling and media are correlated in terminals
    ➢ No need to trigger media interception from signalling interception
  • Mobility is not a problem if interception function is embedded in the terminal
  • Would also help against encryption done in terminals

• Problems with P2PSIP:
  • May be a feasible solution for hardphones but hard to enforce for open source softphones
  • With open standards, anybody can write software
Footprint in Devices

- Currently heavily discussed in Germany
- [http://www.bundestrojaner.net/](http://www.bundestrojaner.net/)

“Install the Bundestrojan now and get a one-year subscription of free telephone surveillance”
Intercepting all IP traffic

• Intercept all IP packets at access network and filter SIP messages containing the target URI

• Problems
  • User mobility
    ➢ the IP-address (and thus the access network) of the target may not be known prior to a call
    ➢ How to correlate dynamically in real-time the triggering of CC interception?
  • Encryption controlled by end-devices
    ➢ If users have a pre-shared key and encryption is end-to-end, CC cannot be retrieved
Infiltrating P2P network

• Intentionally place nodes controlled by the LEA in the P2P network
  • Log lookup requests and registration update messages
  • Perform location lookup on target identity frequently

• Approach pursued by the music industry to find illegal sharing of content in file-sharing P2P networks
  • Goal for music industry is simpler: find somebody who shares music illegally
  • Goal for Lawful Interception: find a specific user
  • P2PSIP will be designed to make chosen-location attacks hard
    ➢ For LI this would be exactly the goal: try to place a node at a specific location in the P2P network
Conclusion
Conclusions

• Future VoIP service architectures may lack central servers
  • P2PSIP is currently standardised by the IETF

• P2P paradigm imposes new challenges to Lawful Interception
  • Without a central component where (at least) signalling traverses, Lawful Interception gets technically complex
  • Difficult to map ETSI reference model to P2P model

• Possible Solutions (that would need to be standardised) are
  • Footprint in devices
  • Interception at access network of target and dynamic triggering of CC interception