Empowered by Innovation NEC

Lawful Interception in P2P-based VoIP Systems

Jan Seedorf
(jan.seedorf_at_nw.neclab.eu)
NEC Laboratories Europe
Heidelberg, Germany

IPTCOMM 2008
Heidelberg, Germany

Outline

1. Introduction to Lawful Interception in VoIP Systems
2. VoIP Signalling without Servers: P2P-SIP
3. Technical Implications of the P2P Paradigm for Lawful Interception of VoIP
4. Possible Solutions
5. Conclusion

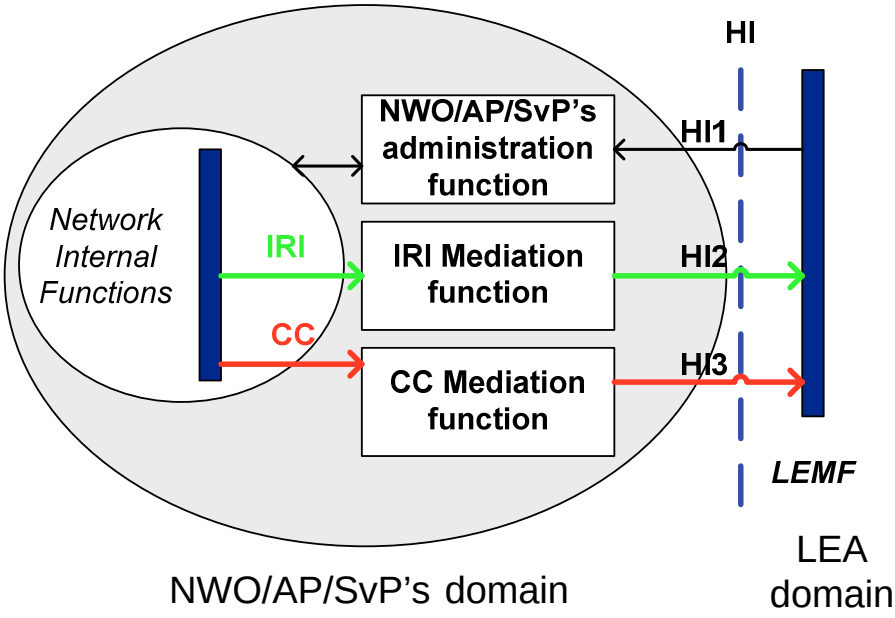
Empowered by Innovation NEC

Introduction: Lawful Interception in VoIP Systems

Lawful Interception

- Lawful Interception
  - authorised wiretapping of communications carried out by law enforcement organisations
- Some Terminology
  - LEA: Law Enforcement Agency
  - IRI: Intercept Related Information
    signalling data identifying the communication
    E.g., source identity, destination identity, call duration, …
  - CC: Content of Communication
    actual payload being transmitted
    For VoIP: audio content of the call, i.e., RTP-packets

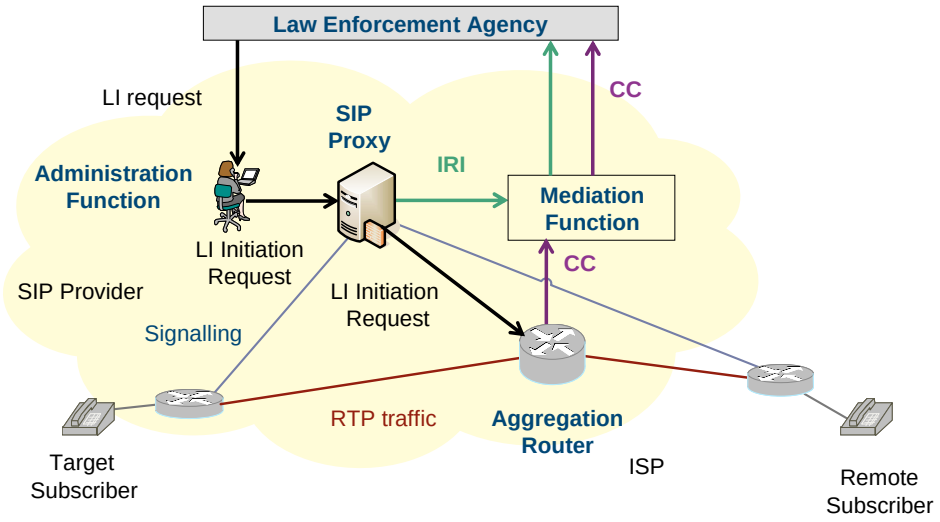
ETSI Reference Model for Lawful Interception



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

Example of LI in Client-Server SIP



Empowered by Innovation NEC

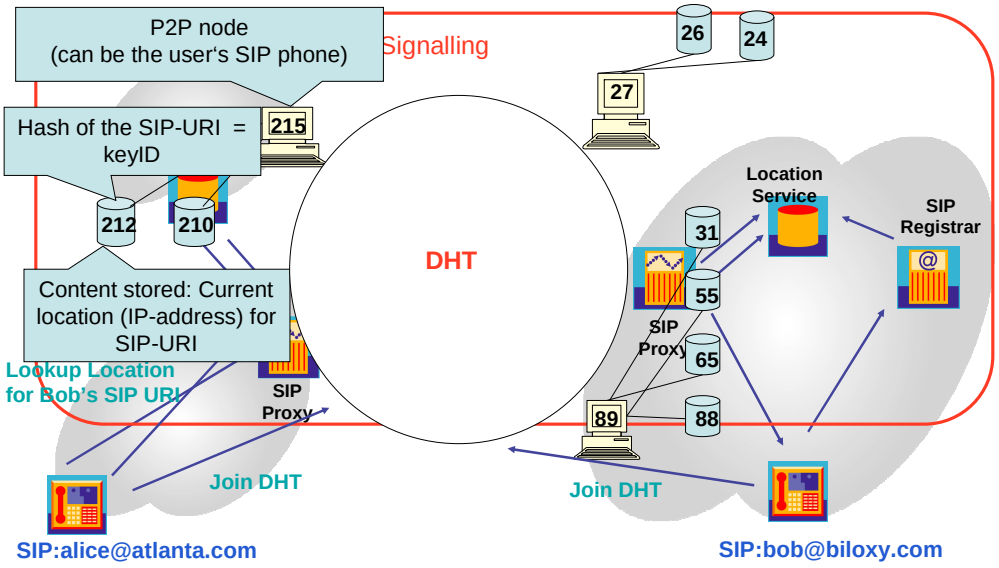
VoIP Signalling without Servers: P2P-SIP

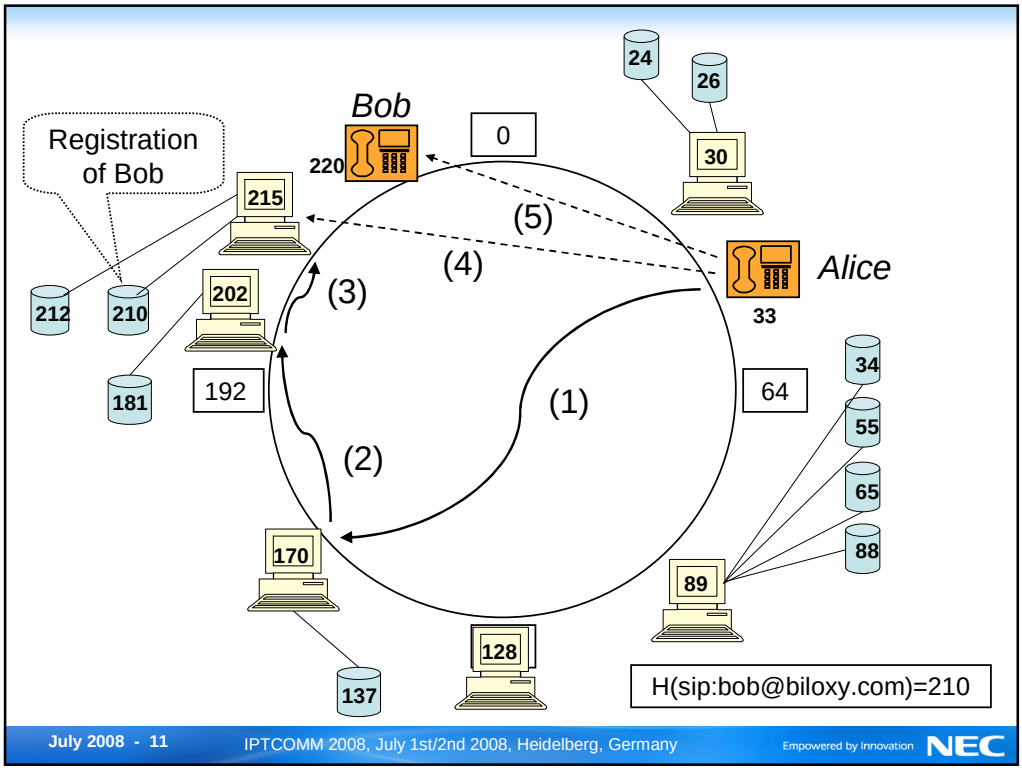
What is P2P-SIP?

- 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 central server but instead distributedly in a highly dynamic P2P network at participating nodes

Arbitrary clients / terminals are storing SIP-registrations

P2P-SIP: Basic Overview





What will a P2P-based VoIP Service Architecture look like?

- P2PSIP is an official IETF working group*
  - 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

* more info:

http://www.ietf.org/html.charters/p2psip-charter.html
http://www.p2psip.org/

Technical Implications of the P2P Paradigm for Lawful Interception of VoIP

Challenges for Lawful Interception in P2PSIP Systems

- P2P implies a significant paradigm shift for VoIP signalling
  - no centralised components on the signalling path
  - network is highly dynamic and there are no static routing paths between entities

  LI methods used in Client-Server systems are not applicable
- Similarities with Client-Server SIP
  - signalling and media take different routes in the network
  - the media path cannot be determined prior to a call

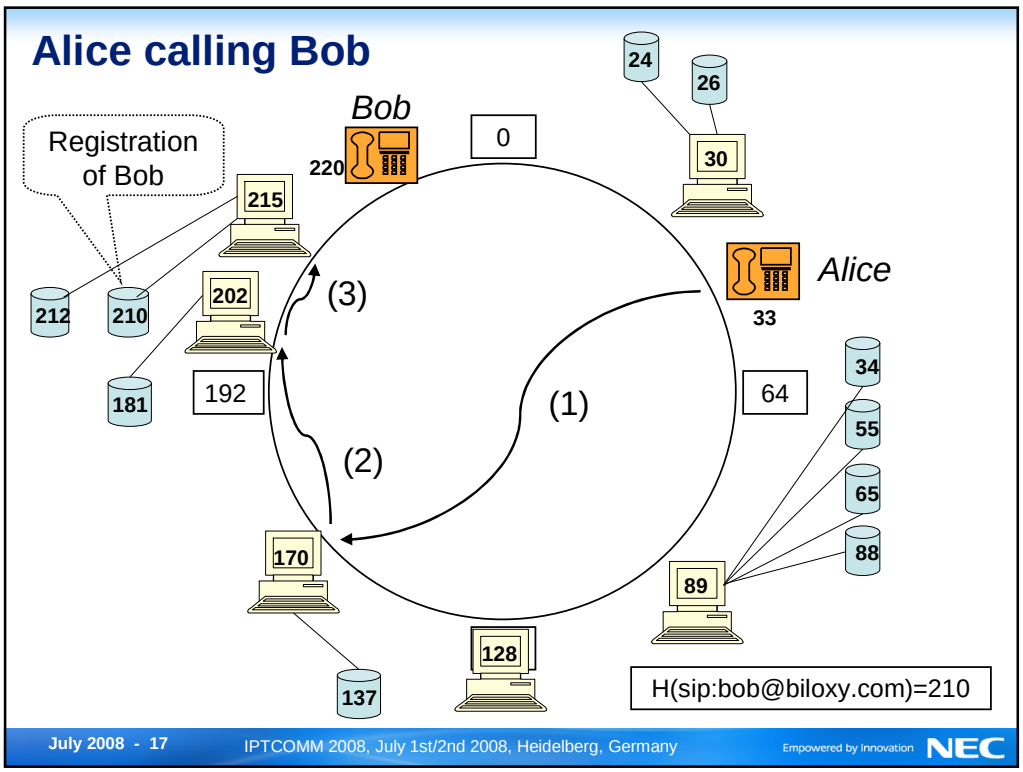
This analysis focuses on the signalling differences in P2PSIP (compared to client-server SIP) and the consequences for Lawful Interception

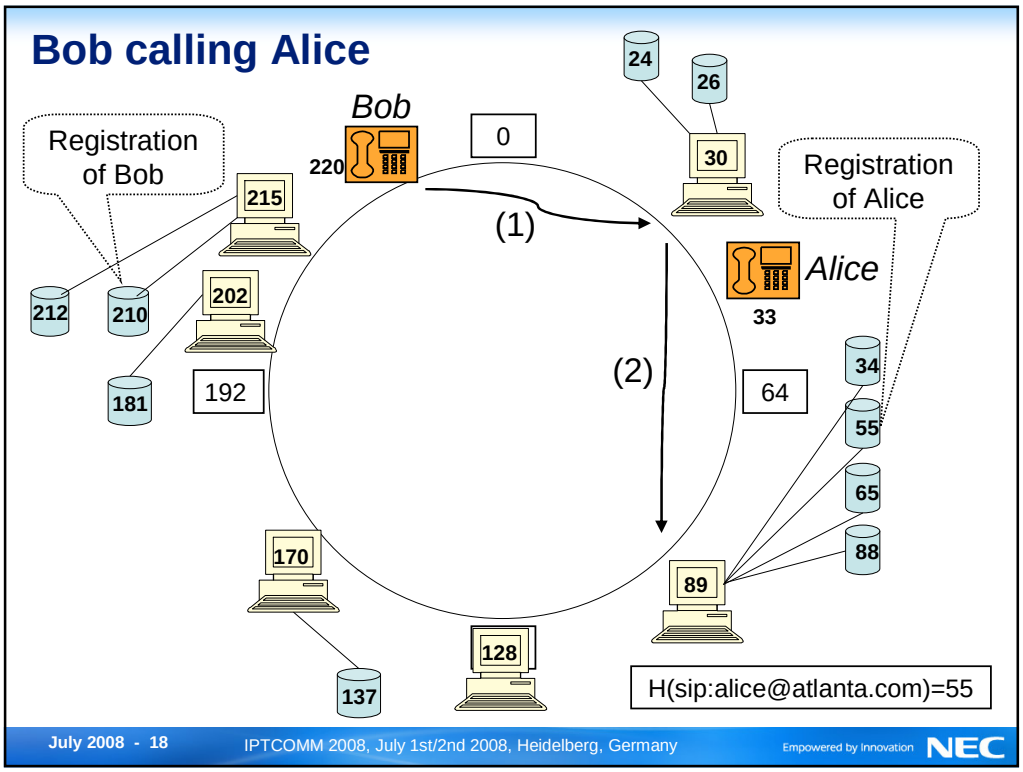
Lack of a Central Entity

- No server involved in call-setup
  - Not possible to determine prior to a call which nodes will be on the signalling path for outgoing calls
  - No single interception point for a specific target
- No VoIP Service Provider to receive interception requests from LEA
  - ETSI reference model assumes an operator (e.g., Network Operator, Access Provider, VoIP Provider)
    - in order for the LEA to trigger Lawful Interception for a specic target identity through the administration function
    - With legal agreements between LEA and operator
  - P2PSIP: LEA has no legal agreement with nodes involved in routing signalling messages through the network

P2P-Routing

- P2P-routing is very different from Client-Server routing
  - Unique routing path with respect to signalling messages ***for every call***
- Inbound and outbound signalling messages take different paths
  - last signalling hop of an incoming call is usually different than the first signalling hop of an outgoing call (for a specific target identity)
- Different outgoing signalling node for different callee
  - SIP-URI of the callee determines the first signalling hop


Alice calling Bob
Bob
220
0
Registration of Bob
215
212
210
202
181
192
(3)
(2)
(1)
24
26
30
Alice
33
64
34
55
65
88
89
170
137
128
H(sip:bob@biloxy.com)=210
July 2008 - 17
IPTCOMM 2008, July 1st/2nd 2008, Heidelberg, Germany
Empowered by Innovation
NEC

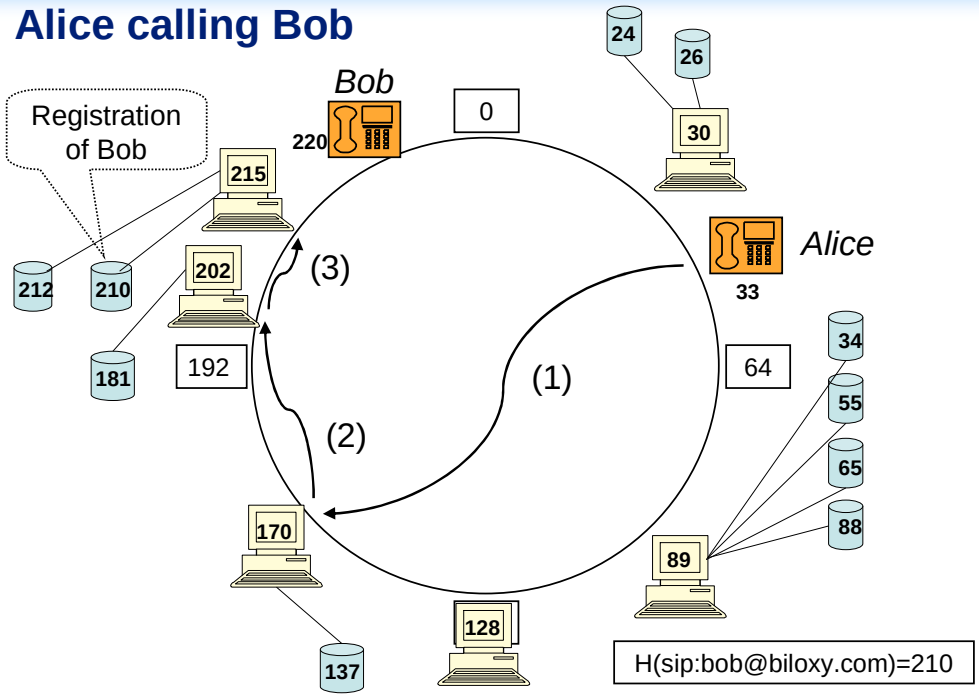

Bob calling Alice
Bob
220
0
Registration of Bob
215
212
210
202
181
192
(1)
(2)
24
26
30
Registration of Alice
Alice
33
64
34
55
65
88
89
170
137
128
H(sip:alice@atlanta.com)=55
July 2008 - 18
IPTCOMM 2008, July 1st/2nd 2008, Heidelberg, Germany
Empowered by Innovation
NEC

Dynamic Nature of P2P Systems

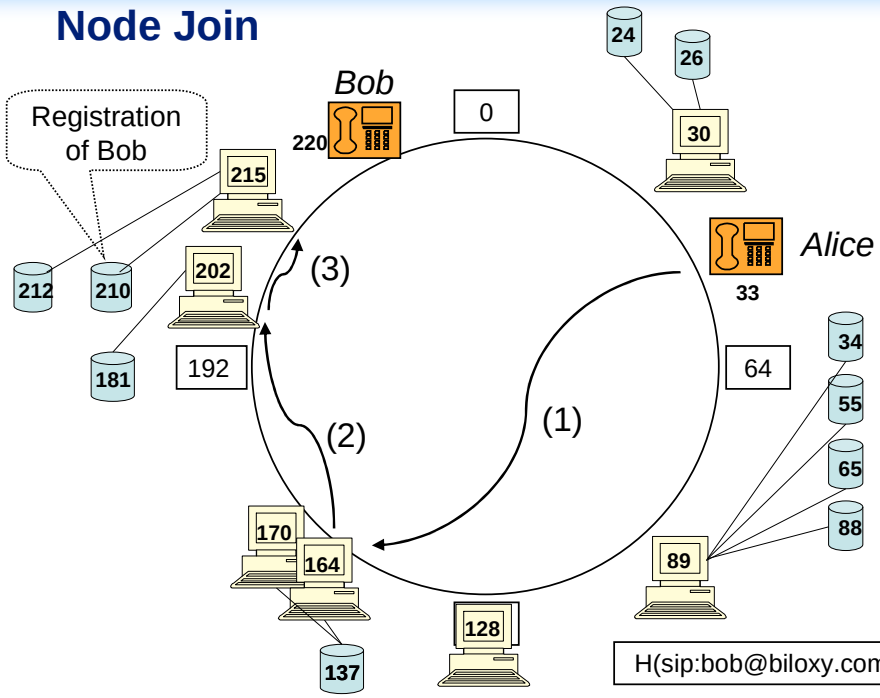
- P2P systems are highly dynamic
  - network membership and routing paths change constantly
- Nodes join and leave frequently
  - the signalling routing path between a specific caller and a specific callee cannot be determined prior to call-setup time because it changes frequently over time
  - Responsibility for user registrations changes over time

Any LI attempt must derive the **first signalling hop** for an outgoing call attempt of a target identity **in real-time**

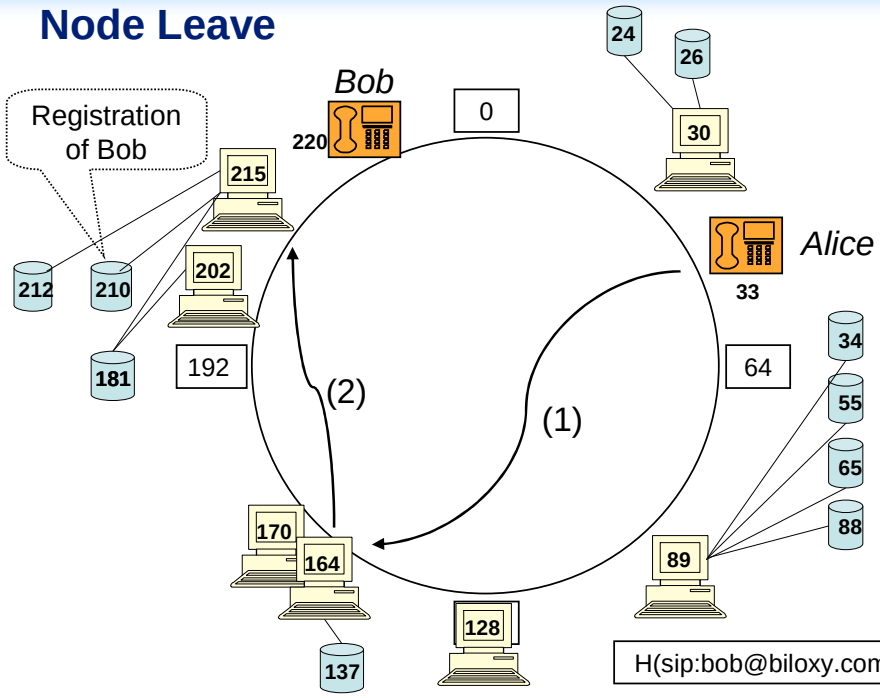
Alice calling Bob



Node Join



Node Leave



Trustworthiness of P2P Nodes

- User registrations are stored distributedly at all participating nodes in the network
  - Nodes can be compromised or act intentionally maliciously
  - Chosen-location attacks

    Attackers can try to join the DHT at a specific location in order to intercept all traffic for a specific target identity

  Integrity of user registrations stored in the network cannot be guaranteed
- Difficult to authenticate user registrations
  - No trust relationship or shared secret between nodes

User registrations stored in a P2PSIP network can be forged, possibly misleading Lawful Interception operations

Possible Solutions

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 feasable 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/

Intercepting at IP-Layer

- 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

    Send out target SIP-URI to all access providers?

    How to correlate dynamically in real-time the triggering of CC interception between different providers?

    Authentication and Authorization issues
  - 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

Conclusion

- P2P paradigm imposes new challenges to Lawful Interception
  - Future VoIP service architectures may lack central servers
  - Without a central component where (at least) signalling traverses, Lawful Interception gets technically complex
- Possible Solutions
  - Footprint in devices
  - Correlated interception at IP-layer
  - Infiltrating P2P Network
- Status Quo
  - All potential solutions have drawbacks
  - Concrete properties of P2P-based VoIP service architectures are not predictable yet (but will affect LI solution space)

  Further research necessary

Empowered by Innovation

NEC

Contact Details:
Jan Seedorf, Research Scientist (jan.seedorf_at_nw.neclab.eu)
NEC Laboratories Europe (NLE), Network Division
NEC Europe Ltd., Heidelberg, Germany