BRNO UNIVERSITY OF TECHNOLOGY
FACULTY OF INFORMATION TECHNOLOGY

Lawful interception in IPv6 networks

Libor Polčák and prof. Miroslav Švéda
{ipolcak,sveda}@fit.vutbr.cz
Brno University of Technology, Faculty of Information Technology, 612 66 Brno, Czech republic

Lawful Interception (LI)

Law Enforcement Agencies (LEAs) use content of network communications for investigation purposes. Courts authorise network operators to copy communications of suspects for specified time period. Data of other users are not collected.

Specified by

- ETSI standards (EU) [1]
- J-STD-025B (U.S.) [2]
- RFC 3924 - Cisco Architecture for Lawful Intercept in IP Networks

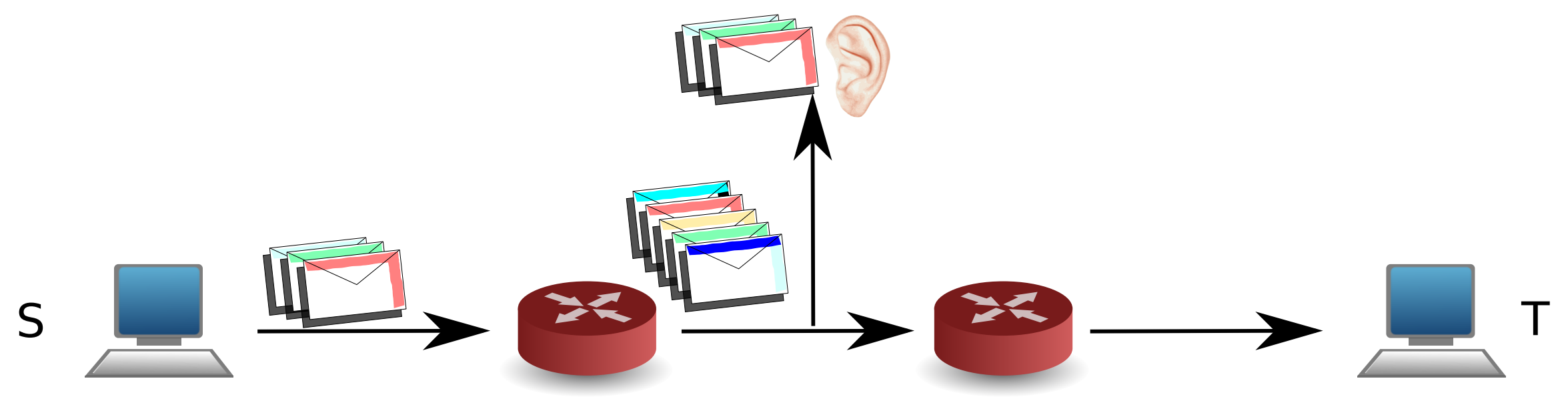


Figure 1: Schematic of Lawful Interception

Challenges in IPv6

User Identification

Different types of addresses

- Link-Local (RFC4291) 🟡
- Site Local Address (RFC4291)
- Stateless Address Autoconfiguration (SLAAC)
  - EUI-64 (RFC4862) 🟢
  - Privacy extension (RFC4941) ●
- DHCPv6 (RFC3315)

Hosts use more than one address per interface at the same time. Many of them are generated by the host itself.

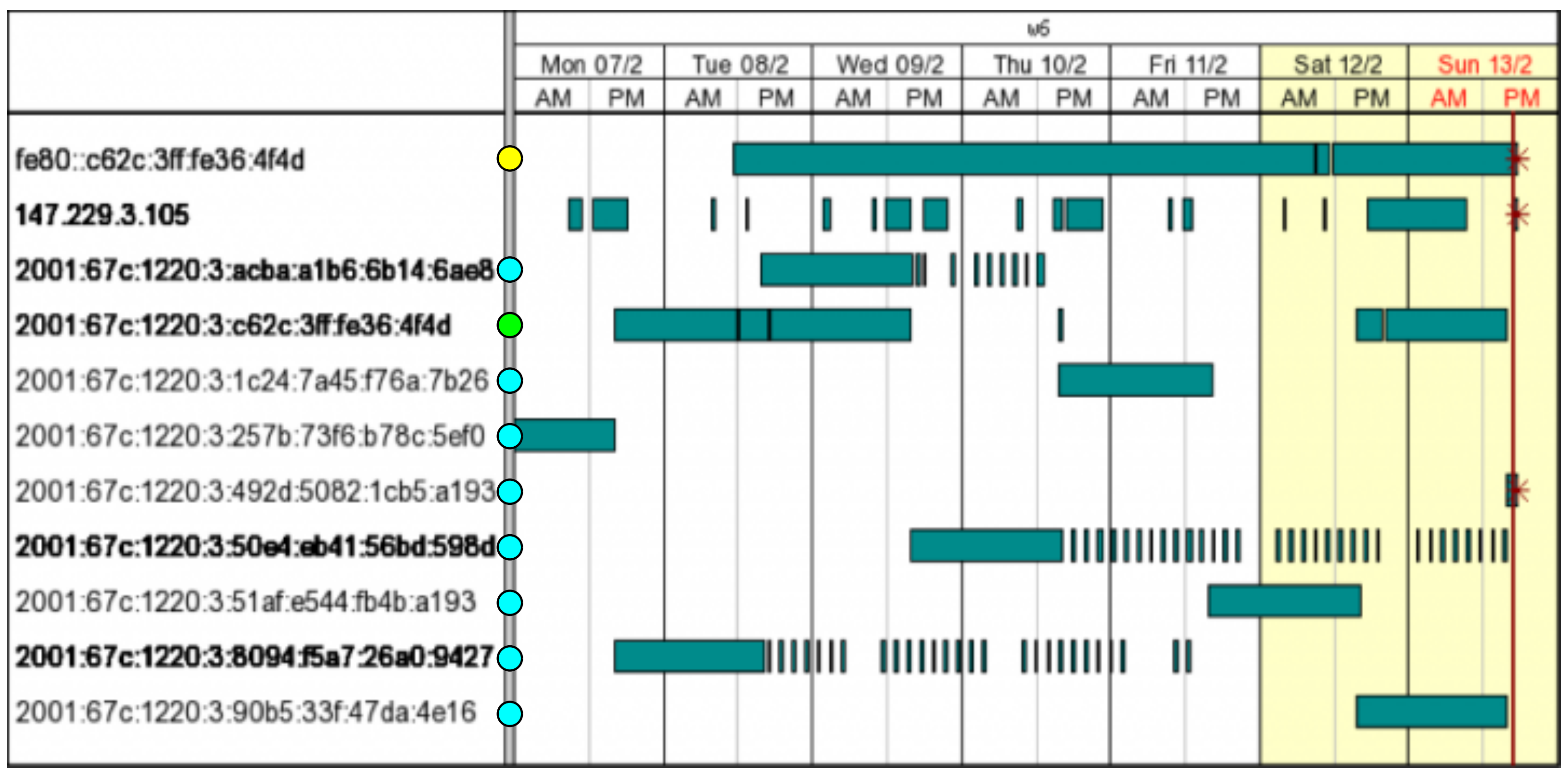


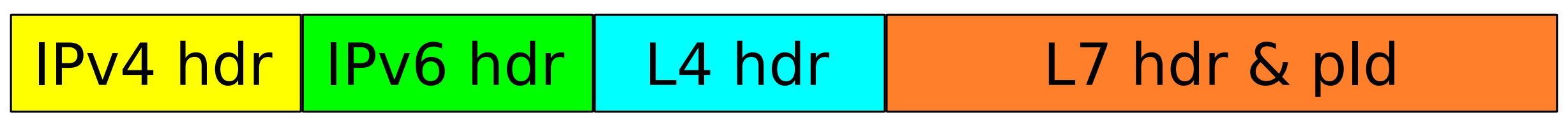
Figure 2: IP addresses used for communication by single computer during one week

Multicast Traffic

- Not covered by current LI standards [1, 2]
- Suspects may communicate using multicast
- How to identify multicast groups of a suspect?

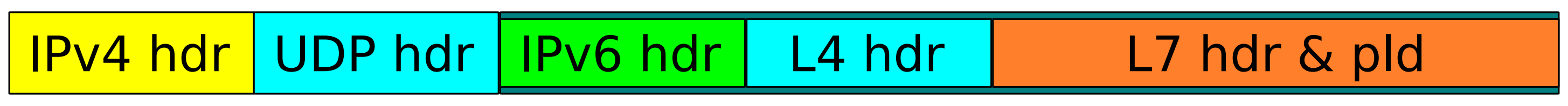
Transition mechanisms

Allows hosts without native IPv6 connectivity to communicate with IPv6 only hosts. IPv6 datagrams tunneled through network and decapsulated at the other end of the tunnel. IPv4 destination address does not identify the final destination. Moreover, these mechanisms may confuse application layer protocol detection.



IPv4 hdr | IPv6 hdr | L4 hdr | L7 hdr & pld

Figure 3: Encapsulation in 6to4 (RFC3056), 6rd (RFC5969), ISATAP (RFC5214) - IP protocol = 41



IPv4 hdr | UDP hdr | IPv6 hdr | L4 hdr | L7 hdr & pld

Figure 4: Encapsulation in Teredo (RFC4380) - arbitrary UDP port may be used

State-of-the-art

Several commercial solutions available. However, they are not ideal. Czech LEAs are interested in development of white box solution.

Some of the pitfails of current solutions:

- Limited LI support of some available solutions; for example interception performed by Cisco devices does not intercept tunneled traffic [3]
- Vendors add surveillance modes to networks devices (e.g. routers). These solutions are typically not hardware accelarated and may lower performance of such devices [3]
- Malicious users may confuse some LI systems [4]
- Dependency on administratively managed IP addresses [5]; even IPv6-surveillance-capable products do not detect all methods that allows network hosts to determine their IPv6 address [6]
- Current LI systems do not handle multicast traffic

Our contribution

Main goals

We focus on development of framework for LI in future networks. Our reasearch will answer following questions:

1) What is the state-of-the-art? The study will include comparison of different published models, their strengths and weaknesses.

2) What are the expectations from different LEAs? Do they use LI to obtain indisputable evidence? What metadata about the communication do they need? What are the applications they are interested in?

3) On which network layer intercept the data? We want to learn about suspect's activities (application layer) but we also need content of lower layers. How to utilise informations from lower layers?

4) How to deal with encapsulation and tunneling?

5) How to recognize useful data (content of the communication is needed) from unimportant data (metadata are enough; e.g. IPTV)? How to ensure privacy of innocent network users?

6) How to deploy the system in the network?

LI deployment model

The goal of the model is to help with distribution of probes in the network. There is a tradeoff between cost of devices and completness of intercepted information. For example ICMPv6 from suspect's LAN provides information about users identity and multicast group membership.

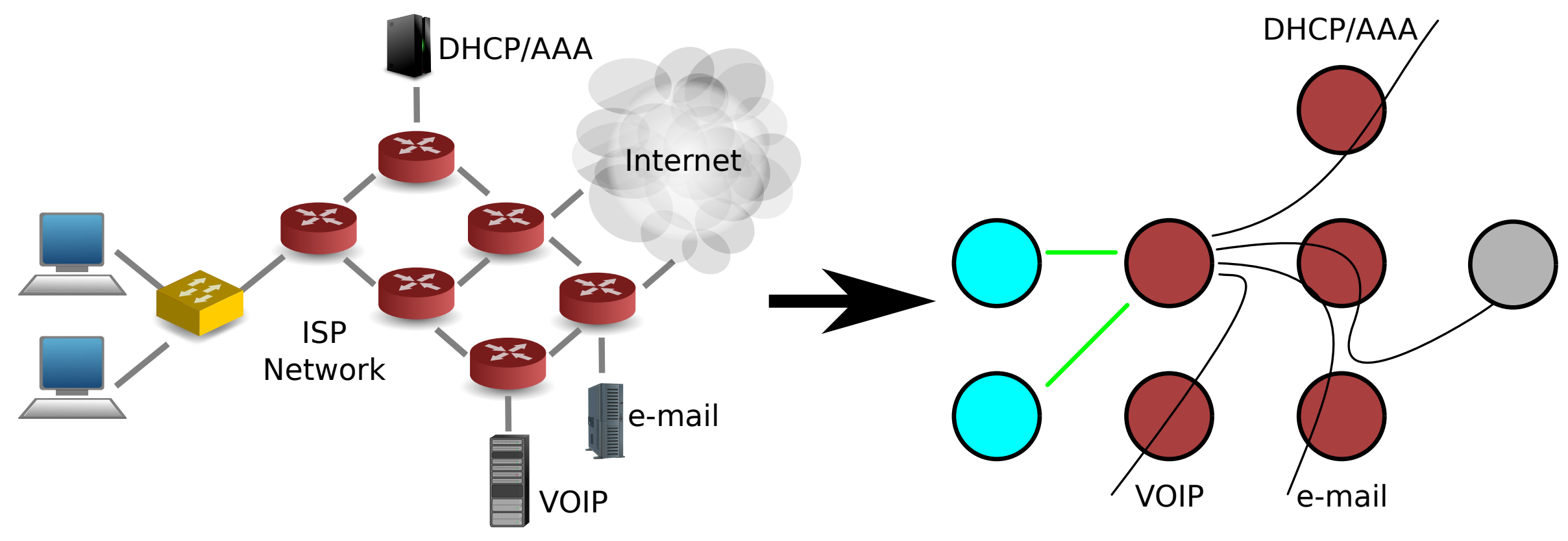


Figure 5: Physical network and abstract model

Future work

- Provide answers to research questions
- Prototype of LI system
- Hardware accelerated probes
- Protocol analysis and reconstruction

Bibliography

[1] European Telecommunications Standards Institute. ETSI TR 101 943: Telecommunications security; Lawful Interception (LI); Concepts of Interception in a generic Network Architecture.
[2] Alliance for Telecommunications Industry Solutions/Telecommunications Industry Association Joint Standard. Lawfully Authorized Electronic Surveillance. J-STD-025-B. July 2006.
[3] Cisco Systems. Cisco 7600 Lawful Intercept Configuration Guide. December 2007.
[4] Cronin, E., Sherr, M. and Blaze, M. On the (un)reliability of eavesdropping. Int. J. Secur. Network. February 2008, Sv. III, 2, pp. 103-113.
[5] Aqsacom. Lawful Interception for IP Networks - White Paper. March 2010.
[6] IP Fabrics. DeepProbe Datasheet. 2011. http://www.ipfabrics.com/pdf/DeepProbe.pdf

Acknowledgement

This work was supported by ESF project CZ.1.07/2.3.00/09.0067 "TeamIT---Building Competitive Research Teams in IT". This work is part of the project VG20102015022 supported by Ministry of the Interior of the Czech Republic and was partially supported by the research plan MSM0021630528.

european social fund in the czech republic
EUROPEAN UNION
MINISTRY OF EDUCATION, YOUTH AND SPORTS
OP Education for Competitiveness
INVESTMENTS IN EDUCATION DEVELOPMENT