

INFORMATION SOCIETY TECHNOLOGIES (IST) PROGRAMME



*Large Scale Monitoring of BroadBand Internet Infrastructure
Contract No. 004336*

Deliverable D4.2a: First LOBSTER Workshop Proceedings and Summary

Abstract: This document is a report on the first LOBSTER workshop which was held on 7 June 2005 in conjunction with the TERENA Networking Conference in Poznan, Poland.

Contractual Date of Delivery	30 June 2005
Actual Date of Delivery	30 June 2005
Deliverable Security Class	PU
Editor	Baiba Kaskina
Contributors	Baiba Kaskina, Evangelos Markatos, Rutger Coolen

The LOBSTER Consortium consists of:

FORTH-ICS	Coordinator	Greece
VU	Partner	Netherlands
CESNET	Partner	Czech Republic
UNINETT	Partner	Norway
ENDACE	Partner	United Kingdom
Alcatel	Partner	France
FORTHnet	Partner	Greece
TNO	Partner	Netherlands
TERENA	Partner	Netherlands



Table of Contents

1. Introduction	3
2. First session: Network Monitoring for the NREN community, the LOBSTER contribution	3
2.1. Large-Scale Infrastructure for Passive Monitoring	4
2.2. LOBSTER use cases for NREN's	4
2.3. GN2 JRA1 monitoring approach and relation with LOBSTER	4
3. Second session: Technological advances in Network Monitoring	5
3.1. Full Packet Passive Monitoring Sensors: Hardware and Software Challenges	5
3.2. Fairly Fast Packet Filtering	6
3.3. Latest Developments in DAG Data Capture Technology	6
4. LOBSTER workshop evaluation	6
Annex 1 – Slides of the presentations	7



1. Introduction

The first LOBSTER workshop was held on 7 June 2005 in conjunction with the TERENA Networking Conference in Poznan, Poland.

The workshop was divided into two sessions. The first session of the workshop was devoted to the LOBSTER project overview and issues interesting for the NRENs. The second session was outlining technological advances in the network monitoring.

The target of the workshop was to present recent results and ongoing efforts from the research community in the area of passive network traffic monitoring with full packet inspection. The workshop addressed both hardware and software challenges related to individual passive traffic sensors as well as large-scale passive monitoring infrastructures, including monitoring applications. The workshop showed the added value of passive network monitoring to network administrators and practitioners, while it was interesting for researchers since it presented the research issues still open in this area. Another objective of the workshop was to disseminate the LOBSTER project to the NREN community. Because LOBSTER is a Specific Support Action it is important that this community knows about the potential added-value the LOBSTER project brings them.

The LOBSTER workshop was run as two parallel sessions of the conference from 11:00 to 15:30. The first session attracted about 60 participants and the second one about 40.

The full proceedings of the LOBSTER workshop can be found on the LOBSTER website at:

<http://www.ist-lobster.org/events/tnc-2005/>

The slides of all the presentations are attached in the Annex 1.

2. First session: Network Monitoring for the NREN community, the LOBSTER contribution

The LOBSTER project aims at realizing a pilot infrastructure for passive network monitoring primarily with and for the NREN community. In this session an overview of the LOBSTER project was presented and the benefits it wants to achieve for the NREN user community. In particular several use cases of the LOBSTER infrastructure were presented. LOBSTER invited people from NRENs to join this session and discuss these use cases. The input from the discussion will be used to improve the design of LOBSTER. Finally in this session the monitoring efforts and related issues in the GN2 project Joint Research Activities were presented and the relation with LOBSTER was discussed.

Presentations were as follows:



- Large-Scale Infrastructure for Passive Monitoring - *by Evangelos Markatos, FORTH*
- LOBSTER use cases for NREN's - *by Rutger Coolen, TNO Telecom*
- GN2 JRA1 monitoring approach and relation with LOBSTER - *by Nicolas Simar, DANTE*

The first session of the LOBSTER workshop was chaired by Baiba Kaskina from TERENA.

2.1. Large-Scale Infrastructure for Passive Monitoring

Evangelos Markatos, FORTH

Accurate network monitoring systems give rise to a wide variety of new applications including provision of early warning for the detection of Internet worms as soon as they start to spread, detection of Distributed-Denial-of-Service attacks, accurate traffic characterization even for applications that use dynamically generated ports such as peer-to-peer systems, and accurate traffic weather service for GRID-enabled applications. The LOBSTER project is working towards designing and deploying an advanced European Infrastructure for accurate Internet traffic monitoring.

This presentation gave an overview on the LOBSTER goals, motivation, described why accurate traffic monitoring is hard and how LOBSTER would contribute towards improving the situation.

Questions raised afterwards were about dynamic port and port 80 traffic handling, possibilities and limitations of hardware, as well as motivation-related issues.

2.2. LOBSTER use cases for NREN's

Rutger Coolen, TNO Telecom

A number of use cases of the LOBSTER infrastructure were presented to show how the LOBSTER monitoring infrastructure can be useful for the NREN community. These cases were open for the discussion to gather participants' input for the design of LOBSTER.

Tackling of the following problems were discussed – encrypted traffic, dynamic ports, and backdoors. Furthermore, the risks associated with automated response to security incidents were discussed. The audience suggested to consider shaping as a measure for potentially suspicious traffic instead of fully denying access. Participants thought that it would be great to involve the universities in the LOBSTER infrastructure, but that might be financially too hard for them. The features of the LOBSTER infrastructure were compared with Netflow and RIPE distributed sensor network. Also, the benefits of honey pots to the detection of worms were discussed.

2.3. GN2 JRA1 monitoring approach and relation with LOBSTER

Nicolas Simar, DANTE



This presentation provided an overview of specific GN2 work which could be of direct interest for the LOBSTER project.

Nicolas Simar gave an overview on the Service Activity (SA) 3 – End-to-End Services, Joint Research Activity (JRA) 1 – Performance Measurement and Management, JRA 2 – Security, as well as other JRAs. He focused on the passive network monitoring issues and presented proposed passive network monitoring applications for GN2. The potential collaboration with the LOBSTER project was mentioned.

3. Second session: Technological advances in Network Monitoring

This session addressed the research and development advances in passive network monitoring. The LOBSTER technical infrastructure consists of monitoring hardware cards, a distributed application programming interface, an anonymization language and demonstration applications. The focus in this session was to present some of the highlights in the state-of-the-art monitoring technology.

Presentations were as follows:

- Full Packet Passive Monitoring Sensors: Hardware and Software Challenges - *by Vladimir Smotlacha, CESNET*
- Fairly Fast Packet Filtering - *by Willem de Bruijn, VUA*
- Latest Developments in DAG Data Capture Technology - *by James Spooner, ENDACE*

The second session of the workshop was chaired by Rutger Coolen from TNO Telecom.

3.1. Full Packet Passive Monitoring Sensors: Hardware and Software Challenges *Vladimir Smotlacha, CESNET*

Packet inspection is an important task of the high speed passive monitoring. Real-time processing of the full line traffic is computationally difficult problem and requires an effective combination of software and specialized hardware.

In his presentation Vladimir Smotlacha spoke about high speed network monitoring issues, flow and packet based monitoring, software optimization, monitoring API, software – hardware co-design and intelligent hardware adapters, i.e. COMBO cards. He described adapters functionality and various different units. At the end of the presentation open problems were stated. Questions after the presentation were about the accuracy of the time-stamp unit and flow cooking.



3.2. Fairly Fast Packet Filtering

Willem de Bruijn, VUA

FFPF is a network monitoring framework designed for three things: speed (handling high link rates), scalability (ability to handle multiple applications) and flexibility. Multiple applications that need to access overlapping sets of packets may share their packet buffers, thus avoiding a packet copy to each individual application that needs it. In addition, context switching and copies across the kernel boundary are minimised by handling most processing in the kernel or on the network card and by memory mapping all buffers to user space, respectively.

Willem de Bruijn spoke about the challenges of passive network monitoring, design and implementation of FFPF, as well as demonstrated use cases of it.

3.3. Latest Developments in DAG Data Capture Technology

James Spooner, ENDACE

With the bleak outlook on the future of Moores law, and the trailing off of ever-increasing processor speeds, network bandwidth is opening the gap on the computer trying to monitor and analyse it.

James Spooner talked about existing and new strategies being planned in order to address this gap, including hardware offload, distributed systems and dedicated processors for network analysis and capture.

4. LOBSTER workshop evaluation

During the TNC all the participants were asked to fill the evaluation forms. The results about the LOBSTER workshop were assessed, the overall rating was good – average 3.8 points from 5 possible. Each speaker was evaluated separately as well. The best and the most interesting presentation in the first session according to the evaluation forms was Evangelos Markatos presentation “Large-Scale Infrastructure for Passive Monitoring”. The second session the most interesting presentation was James Spooner presentation “Latest Developments in DAG Data Capture Technology”.



Annex 1 – Slides of the presentations

The slides of all the presentations are attached:

- Large-Scale Infrastructure for Passive Monitoring - *by Evangelos Markatos, FORTH* - 6 pages (lobster-1.pdf)
- LOBSTER use cases for NREN's - *by Rutger Coolen, TNO Telecom* – 4 pages (lobster-2.pdf)
- GN2 JRA1 monitoring approach and relation with LOBSTER - *by Nicolas Simar, DANTE* – 5 pages (lobster-3.pdf)
- Full Packet Passive Monitoring Sensors: Hardware and Software Challenges - *by Vladimir Smotlacha, CESNET* – 3 pages (lobster-4.pdf)
- Fairly Fast Packet Filtering - *by Willem de Bruijn, VUA* – 3 pages (lobster-5.pdf)
- Latest Developments in DAG Data Capture Technology - *by James Spooner, ENDACE* - 4 pages (lobster-6.pdf)