

LOBSTER



SUMMARY

LOBSTER is a pilot European Infrastructure for accurate Internet traffic monitoring that will improve our understanding of the Internet and will contribute towards solving difficult performance and security problems. Based on appropriate abstractions and willing-full cooperation among points of presence, LOBSTER will work towards effectively monitoring the underlying network, providing early warning for security incidents, and providing accurate and meaningful measurements of performance.

WHAT IS THE PROBLEM?

As networks get faster and network-centric applications get more complex, our understanding of the Internet continues to diminish. For example:

- We do not know, which applications generate most traffic
- We suffer malicious cyber attacks like viruses and worms
- We witness incidents of “friendly fire” – unintentional attacks to Root DNS servers

In order to understand more and to be able to fight the malicious cyber attacks, the defense mechanisms have to be more intelligent and as quick as the spreading of the worms. They need:

- Smart, flexible, high-performance Internet monitoring sensors, capable of detecting new worms
- Distributed infrastructure of Internet traffic sensors which are more sensitive to attacks, can pinpoint attacks as soon as they emerge and spread information about new worms fast

DISSEMINATION

The project’s public communication strategy is through its Website, Tutorials, EC organized events, publications and presentations.

The workshops are another mechanism through which information will be transferred to the relevant target groups. The workshops will enable to build trust relations, promote European technologies, and exchange knowledge.

LOBSTER planned events:

- 1st LOBSTER Tutorial – 6 May 2005, Stockholm, Sweden
- 1st LOBSTER workshop – 7 June 2005, Poznan, Poland
- 2nd LOBSTER Tutorial – May 2006
- 2nd LOBSTER workshop – May 2006

OBJECTIVES

The main goal of LOBSTER is to deploy an advanced pilot European Internet Traffic Monitoring Infrastructure based on passive monitoring sensors at speeds starting from 2.5Gbps and possibly up to 10Gbps.

More specifically the objectives of LOBSTER are:

- To organize stakeholders in the area of advanced internet traffic monitoring
- To realize the appropriate data anonymizing tools that will prohibit unauthorized tampering with the original traffic data
- To develop novel applications enabled by the availability of the passive network traffic monitoring infrastructure (such as accurate traffic characterization applications for programs using dynamic ports, zero-day worm spread detection applications, European Internet measurement services etc.)
- To provide anonymized data traffic information on a regular basis

To provide traffic data and project results to interested network researchers, ISPs, ASPs, security analysts etc.

WHO CAN BENEFIT FROM LOBSTER?

Various user communities will benefit from the LOBSTER infrastructure, including:

- NRENs/ISPs
 - Better Internet traffic monitoring of their networks
 - Better understanding of their interactions with other NRENs/ISPs
- Security analysts and researchers
 - Access to anonymized data
 - Access to “safe” testbed to study trends and validate research results
- Network and security administrators
 - Access to a traffic monitoring infrastructure
 - Access to early warning systems
 - Access to software and tools

LOBSTER

TECHNICAL APPROACH

LOBSTER is a step towards providing an advanced pilot European passive Internet traffic monitoring infrastructure that will improve our understanding of the Internet and will contribute towards solving difficult performance and security problems. This infrastructure will empower network administrators with the appropriate abstractions and tools of network monitoring that will enable them to accurately monitor networks for performance and security.

LOBSTER is based on powerful monitoring methods collectively known as passive monitoring. Instead of collecting lousy flow-level statistics or probing through active packets, passive monitoring records all IP packets (both headers and payloads) that flow through a link. Since passive monitoring methods record complete traffic information, they are able to tackle monitoring problems more effectively and accurately than methods based on flow-level statistics or active monitoring.

However, passive monitoring methods require a more advanced monitoring infrastructure because they place a significant burden on the computation, storage, and communication resources of the monitoring system. For example, monitoring a 10Gbps link, may generate more than four terabytes of monitoring data per hour, or close to a petabyte of data per week. Transferring, storing, and accessing such amounts of data is a significant challenge for ordinary systems.

Within LOBSTER it is planned to use the experience gained in the SCAMPI IST project (<http://www.ist-scampi.org/>), which designed and implemented a passive network monitoring system for speeds up to 10 Gbps. Central to the SCAMPI system is the SCAMPI monitoring adapter, equipped with powerful FPGAs that implement most kinds of monitoring functions, such as filtering, hashing, sampling, string searching, header matching, etc. In addition to the adapter, the SCAMPI monitoring system provides an expressive monitoring application programming interface (MAPI) that enables applications to express their monitoring needs to a fine detail. The ENDACE produced DAG cards will be used as well.

LOBSTER INFRASTRUCTURE

The LOBSTER infrastructure will be a distributed system of passive network monitoring sensors. It will focus on cooperation:

- Sharing raw and pre-processed data
- Correlating results

Initially three sites will be connected: UNINETT, CESNET, FORTHnet. The participation model to the infrastructure will be open, similar to the PlanetLab.

LOBSTER ENGINEERING CHALLENGES

LOBSTER project will have to address different challenges.

- Trust: cooperation sensors may not trust each other
 - Easily configurable privacy and anonymization policies
 - Distinction between user groups, e.g., internal and external
 - Audit trail for accountability
- Security: prevent attackers from gaining access to private and confidential data
 - Strong authentication framework
 - Tamper-proof hardware- and software-level anonymization
- Easy of use: need a common programming environment
 - Use DiMAPI (Distributed Monitoring Application Programming Interface)

EXPECTED IMPACT

Besides monitoring the performance and quality-of-service of the Internet, LOBSTER will: a) help to accurately characterise and classify Internet traffic even from applications that use dynamic ports, e.g., peer-to-peer traffic, and b) create a platform that has unprecedented potential for the detection and analysis of cyber attacks. By monitoring the European ISP and NRN networks for signs of large-scale attacks, including worms, viruses, and (Distributed) Denial-of-Service attacks, LOBSTER may function as an early warning system to the European community. Cyber attacks can be detected, localised, and traced by for example Computer Incident Response Teams, security administrators, and Law Enforcement Agencies. The privacy of Internet-users will be fully maintained in this process, because the LOBSTER platform uses anonymous network statistics.

LOBSTER will also contribute towards consolidating the scientific community in the area of network monitoring, by bringing together the engineering and the research communities in this area. A unique European Infrastructure on advanced network traffic monitoring may serve as a center of reference for researchers all over Europe.

Project name:
LOBSTER

Contract no.:
IST-004336

Project type:
SSA

Start date:
1/10/2004

Duration:
27 months

Total budget:
2050403.63 €

Funding from the EC:
1625072.08 €

Total effort in person-month:
183

Web site:
www.ist-lobster.org

Contact details:
Mr.Evangelos Markatos
Foundation for Research
and Technology Hellas
(FORTH)
Science and Technology
Park of Crete
711 10 Heraklion
Greece
info@ist-lobster.org

Project participants:
FORTH-ICS GR
VU NL
CESNET CZ
UNINETT NO
ENDACE UK
Alcatel FR
FORTHnet GR
TNO NL
TERENA NL

Key words:
Advanced pilot Internet
Traffic Monitoring
Infrastructure,
Passive network
monitoring

Collaboration with other
EC funded projects:
GN2, SCAMPI, MOME,
NoAH