With the internet a crucial tool in international business, the monitoring of internet traffic takes on increasing importance. In this exclusive article **Evangelos Markatos** analyses the work of the LOBSTER project in developing advanced pilot European Internet Traffic Monitoring Infrastracture

# Monitoring traffic to protect internet users

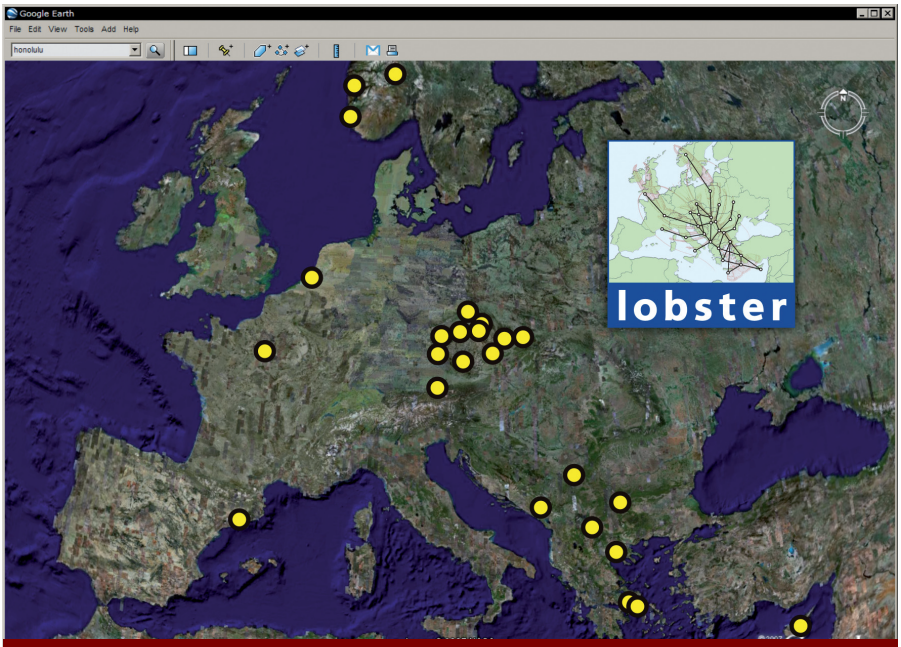
**Over the last few years,** the European Commission has been encouraging innovative Research and Development on experimental networking testbeds, work which has involved several member states. The LOBSTER project (Large-Scale Monitoring of Broadband Internet Infrastructure) has made a bold contribution towards this effort, with the objective of rolling out innovative instrumentation and monitoring tools on advanced computer networks across Europe. Such tools are essential if we are to offer network operators and researchers a global view of network activity, something notoriously hard for local monitors and laboratory testbeds to achieve.

Based on passive monitoring, LOBSTER infrastructure is the only project of its kind in Europe. In fact, it is one of only a few examples of such an infrastructure across the world. Despite, or perhaps because of its relative youth, great importance is attached to its development. Indeed, the scale of its deployment gives some idea as to how central it is to future planning. At the time of writing, the LOBSTER infrastructure is operational in 50 locations across 10 countries. It monitors networks with a cumulative capacity in excess of 25 Gigabits per second. The testbed is being used actively for tasks such as traffic characterisation, quality-of-service measurements, network attack detection, and real-time tracking of cyberattack trends. In all these focus areas, LOBSTER facilitates the live testing and evaluation of innovative techniques that have never before been tested on such a grand scale. To provide a case in point, the NEMU innovative cyber-attack detection technique developed by FORTH, LOBSTER's coordinator), has already been deployed in LOBSTER. The technique captured its first zero-day polymorphic exploit in March 2007, and so far has intercepted more than 600,000 attacks.

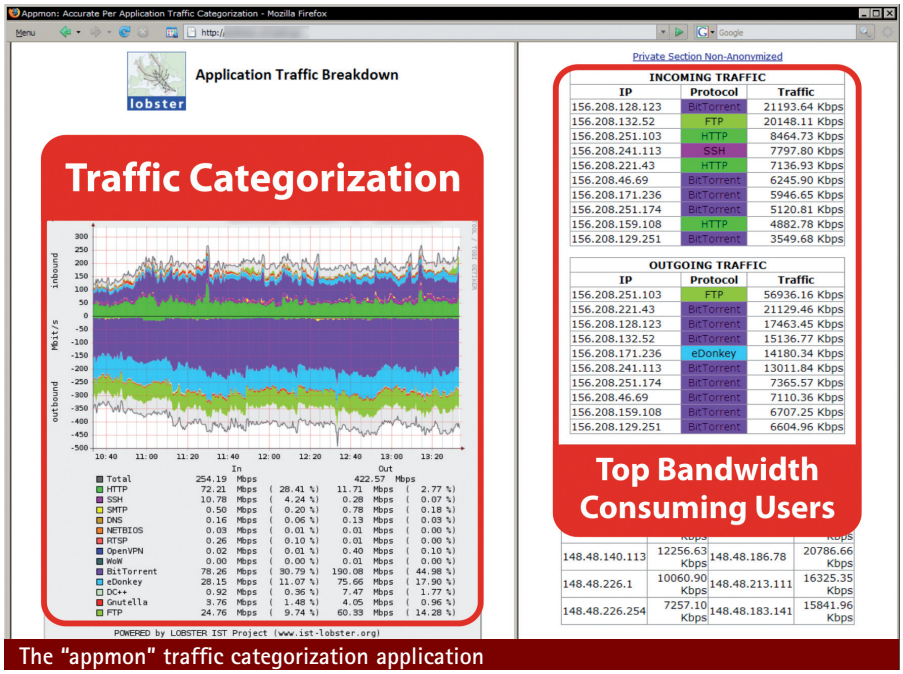
## Successes of the LOBSTER project

LOBSTER is a clear example of the "can do" mentality of European entrepreneurs, and is an excellent showcase for European talent. The technology used within LOBSTER is for the most part derived from an earlier FP5-IST project, called SCAMPI (www.ist-scampi.org), which developed flexible, high-performance monitoring tools, and helped build up European expertise in this focus area. The technology developed in SCAMPI was not simply documented then shelved, but was actually put in real use in a new testbed effort, with new industry partners and operator involvement, particularly from National Research and Education Networks (NReNs) from member states, thanks to the dissemination efforts of TERENA, the Trans-European Research and Education Networking Association, project coordinator of SCAMPI, and leader of the LOBSTER dissemination effort.

If their work is to survive the test of time, one key challenge LOBSTER face is how to develop instrumentation that is cost-effective, yet sufficiently general-purpose. This has to be done against a backdrop of uncertainty as to what the testbed participants might want to monitor or measure in the future. LOBSTER has so far succeeded in this aim, they have responded to the changing environment and new,



The geographic location of the deployed LOBSTER sensors in Europe



The "appmon" traffic categorization application

more security-oriented tasks are now the focus of attention (along with Symantec, the global leader in information security and availability). These tasks are now more important than the performance and QoS measurement tools that it was originally envisioned would form the largest part of LOBSTERs work.

LOBSTER have paid particular attention to the question of privacy. During the design phase, LOBSTER was enriched with a flexible API and ways to specify privacy policies per site, as well as quantitative studies of how much privacy might be lost if LOBSTER data was in the hands of an adversary.

To evade detection, skillful cyber-attackers have recently started to camouflage their attacks by blending them with ordinary traffic. LOBSTER has deployed novel applications which identify sophisticated camouflaged attacks, also known as polymorphic attacks. During its deployment, LOBSTER has managed to detect hundreds of thousands of such attacks. The information gained during these operations has led to the pinpointing of both the sources of the attacks and the vulnerabilities of the attack victims.

## What does the future hold for LOBSTER?

Several major European leaders have recognised the benefits of passive network monitoring in general and thus have expressed their interest in collaboration, particularly with LOBSTER. Indeed, SEEREN, the Research Internet provider in the SouthEast of Europe, has already signed an MoU with LOBSTER and installed LOBSTER sensors monitoring traffic in Serbia, Montenegro and the FYR of Macedonia. In the same spirit, several members of Geant, the most advanced network in Europe, have also installed LOBSTER sensors monitoring the performance and security of their networks around the clock.

With more than 600,000 network attacks having been captured and more than 50 sensors in high-speed networks installed, the LOBSTER project was successfully completed at the end of June 2007. However, the completion of the project has not led to any complacency amongst the LOBSTER support team, and the LOBSTER community retains an innovative, vibrant spirit. They have ambitious plans to maximise the impact of LOBSTER technology: after successful initial tests, LOBSTER will be deployed in Lithuania, Poland, Switzerland, and Bulgaria, monitoring network connections whose cumulative capacity exceeds 30 Gbps, within Geant.

The importance of the internet to modern society cannot be overstated. It is a forum in which people can learn, exchange information, gather knowledge and conduct business. And yet with this multiplicity of functions comes an element of risk, a risk which can be alleviated by co-operation with our European partners. By capitalising on human potential and exploiting technology developed in Framework Programs, Europe can build world-leading testbeds which will provide a lasting framework for internet security. ★

## At a glance

### About LOBSTER

As networks get faster and network-centric applications get more complex, our understanding of the internet continues to diminish. New aspects of internet behaviour emerge that are either unknown or poorly understood. Denial-of-service attacks, malicious self-replicating programmes (worms) and viruses plague the internet. All of these factors point to a need for better internet traffic monitoring, one of the main aims of the LOBSTER project.

### Partners:

- Foundation for Research and Technology Hellas (FORTH)
- Alcatel-Lucent
- Czech National Research and Education Network (CESNET)
- Hellenic Telecommunications and Telematics Application Company S.A (FORTHnet)
- Symantec
- TNO Telecom
- Trans-European Research and Education Networking Association (TERENA)
- Uninett A/S
- Vrije Universiteit Amsterdam (VU)

### Contact details:

info@ist-lobster.org
www.ist-lobster.org

Evangelos Markatos

Head of the Distributed Computing Systems Lab, ICS-FORTH
Professor of Computer Science, University of Crete