

LOBSTER

Large-Scale Monitoring of Broadband Internet Infrastructure

Baiba Kaškina
TERENA

Evangelos Markatos & Panos Trimintzios, Arne Øslebø

markatos@ics.forth.gr

ptrim@ics.forth.gr

arneos@uninett.no

FORTH

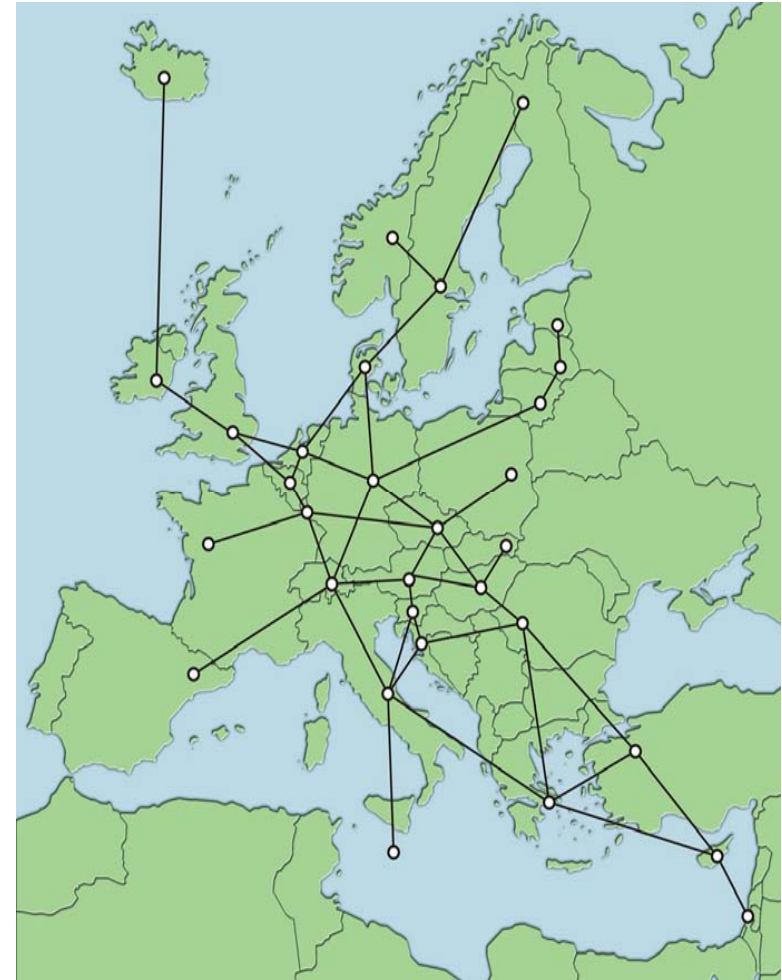
UNINETT

TF-CSIRT

27-28 January 2005, London

LOBSTER overview

- Specific Support Action project
 - Start: 1 October 2004
 - Finish: 31 December 2006
- 9 partners
 - ALCATEL, CESNET, ENDACE, FORTH, FORTHNET, VRIJE, TERENA, TNO, UNINETT
- Main goal:
 - To develop an advanced European infrastructure for passive network traffic monitoring.



Motivation

- Improve our understanding of the traffic on the Internet
 - Which applications generate the most traffic?
- QoS
 - Packet loss, packet reordering, one way delays,
- Security
 - “Friendly fire”
 - Viruses and worms

Well known worms

- Summer 2001: CODE RED worm
 - Infected 350,000 computers in 24 hours
- January 2003: Sapphire/Slammer worm
 - Infected 75,000 computers in 30 minutes
- March 2004: Witty worm
 - Infected 20,000 computers in 60 minutes

Technical challenges

- Network speed
 - Passive monitoring on slow networks is easy
 - Passive monitoring on high speed networks is HARD
 - 10GB/s
 - 1250MB/s
 - Worst case: ~24Mpps
 - Normal network: 1-1.5Mpps
- Need specialized hardware:
 - SCAMPI adapter, DAG cards etc.

Technical challenges(2)

- Distributed access to monitoring probes
 - DMAPI
- Anonymization
 - In hardware and/or software
 - SiSaL: Scripting Sanitization Language

LOBSTER focuses

- An advanced infrastructure for passive monitoring
- Common programming environment – DMAPI
- Anonymization
- Applications
 - Contribution to the early warning system
 - Network monitoring applications

Timeline

- Early 2005
 - Questionare
 - Requirements
- 2005
 - Design
 - Development of basic components
- Late 2005
 - First deployment phase
- 2006
 - Development of applications
 - Second deployment phase

Relation with TF-CSIRT & GN2 JRA2

- Questionnaire (February – March)
 - Requirement collection
 - Information about the organisation
 - Passive monitoring issues
 - Interest in collaboration with LOBSTER
 - Acceptable Use Policy
 - Policy issues
 - Anonymizatiois issues

Relation with TF-CSIRT & GN2 JRA2

- **Next LOBSTER meeting** – 21-22 March, Amsterdam (TERENA's office)– interested?– Join!
- LOBSTER people are available to follow GN2 JRA2 activities
- Website: www.ist-lobster.org
- News, announcement list - <http://www.ist-lobster.org/announcements/>
- Joining the infrastructure – end of 2005

More information

- <http://www.ist-lobster.org>
- info@ist-lobster.org
- Evangelos Markatos: markatos@ics.forth.gr
- Arne Øslebø: arneos@uninett.no
- Baiba Kaškina: baiba@terena.nl