

LOBSTER: Large-Scale Monitoring of Broadband Internet Infrastructures

An FP6 IST Research Infrastructures project

Presentation by
Dr. Panos Trimintzios
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Crete, Greece



Talk Roadmap

- Motivation
 - Understanding the Internet
 - Performance, diagnosis and security
- Pilot Infrastructure: LOBSTER
 - Challenges
 - Potential Applications



What is the problem?



<http://www.ist-lobster.org>

- Poor network monitoring capabilities
 - We suffer malicious cyberattacks such as viruses and worms, spyware, DoS/DDoS
 - We do not know which applications are running on our networks



Dr. Panos Trimintzios, FORTH

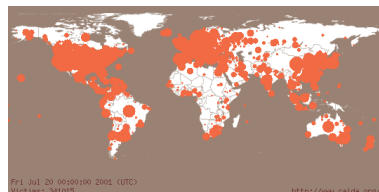
Research Infrastructures Information Event, 26-27 May, Brussels

Cyberattacks continue to plague our networks



<http://www.ist-lobster.org>

- Famous worm outbreaks:
 - 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



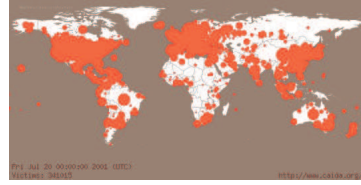
Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Why do Cyberattacks continue to plague Internet?



<http://www.ist-lobster.org>



- Attack detection, identification, and response/deployment takes hours
- Usually too late, when almost all computers have already been infected
- Can we respond faster to reduce the damage? How?
 - Smart, flexible, high-performance Internet monitoring sensors
 - Capable of detecting new worms
 - Distributed infrastructure of Internet traffic sensors
 - More sensitive to attacks, quick response



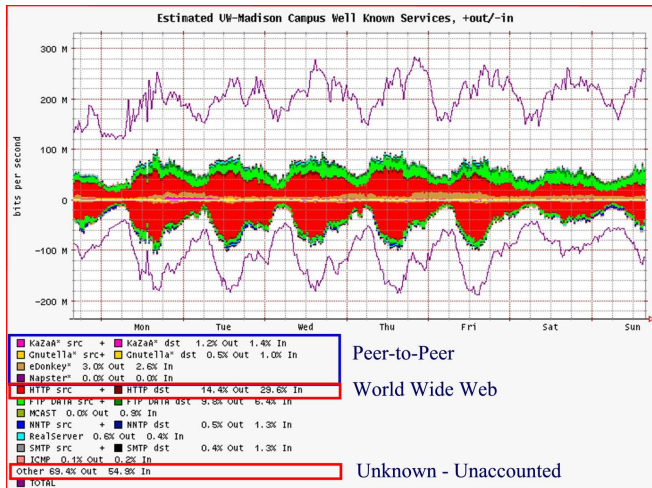
Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Problem II: Who generates all this traffic?



<http://www.ist-lobster.org>



69% of the traffic is unaccounted-for

- Maybe belongs to p2p applications that use dynamic ports
- Maybe belongs to media applications
- The bottom line is:
 - We don't know!



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Problem summary



<http://www.ist-lobster.org>

- Our understanding of the Internet needs to be improved
- The gap between what we **can** measure and what we **need** to measure is large and getting larger



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Solution?



<http://www.ist-lobster.org>

- We need better network monitoring:
 - **Faster**: detect worms *before* they infect the planet
 - **More accurate**: close the gap between what we know and what is really going on



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

LOBSTER Profile



<http://www.ist-lobster.org>

LOBSTER: Large-Scale Monitoring of Broadband Internet Infrastructure

- Funded by EC
- A “Specific Support Action”
- Duration:
Oct 2004 – Dec 2006
- Successor of IST SCAMPI (R&D Project)
- SCAMPI: a SCALable Monitoring Platform for the Internet
 - High-performance single node monitoring



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

The LOBSTER infrastructure



<http://www.ist-lobster.org>

- LOBSTER
 - A network of passive Internet traffic monitors
 - Cooperation:
 - **Exchange** information and observations
 - **Correlate** results



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Challenging Issues I: TRUST



<http://www.ist-lobster.org>

- Trust: cooperating sensors may not trust each other
 - Need to **protect private** and **confidential** information
- Achieved through multi-level **anonymization** techniques
 - Limited access to internal users
 - Outside users will be able to operate only on **anonymized data**
- Control of the above through **Administratively Configurable Policies**



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Challenging Issues II: Common Access



<http://www.ist-lobster.org>

- Need a **Common Programming Environment**
 - Use DiMAPI (**D**istributed **M**onitoring **A**pplication **P**rogramming **I**nterface)
 - MAPI developed within the SCAMPI project



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Challenging Issues III: PROTECTION



<http://www.ist-lobster.org>

- Resilience to attackers:
What if intruders penetrate LOBSTER?

- Can they have access to private/confidential data?
- NO!
 - Hardware anonymization
 - The level of anonymization can be tuned by system administrators



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Potential LOBSTER applications ...



<http://www.ist-lobster.org>

- Accurate traffic monitoring
 - How much of your bandwidth is going to file sharing applications such as Gnutella?
 - Which application generates most of the traffic?



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Potential LOBSTER applications ...



<http://www.ist-lobster.org>

- **Early-warning systems**
 - Automatic detection of new worms
 - Detect worms within minutes
 - Early-warning
 - Alert administrators+users about potential attacks
 - Timely response to worms
 - Generate attack signature
- **Other applications**
 - Grid performance debugging
 - ...



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Who can benefit from LOBSTER?



<http://www.ist-lobster.org>

- **NRNs/ISPs**
 - Better Internet traffic monitoring of their networks
 - Better understanding of their interactions with other NRNs/ISPs
- **Security analysis researchers**
 - Access to anonymized data
 - Access to anonymized testbed
 - 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



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Summary



<http://www.ist-lobster.org>

- Our understanding of the Internet needs to be improved
- LOBSTER will provide better network monitoring through
 - High-end passive monitoring systems
 - A distributed infrastructure of monitoring systems
 - Trusted cooperation in an untrusted world
 - Common programming platform
 - Infrastructure resilience against attacks



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

LOBSTER partners



<http://www.ist-lobster.org>

- Research Organizations
 - ICS-FORTH, Greece
 - Vrije University, The Netherlands
 - TNO Telecom, The Netherlands
- NRNs/ISPs, Associations
 - CESNET, Czech Republic
 - UNINETT, Norway
 - FORTHNET, Greece
 - TERENA, The Netherlands
- Industrial Partners
 - ALCA TEL, France
 - Endace, UK



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Extending the LOBSTER Infrastructure



<http://www.ist-lobster.org>

- You are welcome to join our infrastructure after Dec 2005!
 - Install one or more monitoring sensors within your network



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels

Distributed Passive Network Monitoring the LOBSTER project



<http://www.ist-lobster.org>

<http://www.ist-lobster.org>

Panos Trimintzios

(ptrim@ics.forth.gr)

Institute of Computer Science (ICS)

Foundation for Research and Technology – Hellas (FORTH)

Crete, Greece



Dr. Panos Trimintzios, FORTH

Research Infrastructures Information Event, 26-27 May, Brussels