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?

- 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

Cyberattacks continue to plague our networks

- 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
Why do Cyberattacks continue to plague Internet?

- 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

Problem II: Who generates all this traffic?

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!
Problem summary

- 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

Solution?

- 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
LOBSTER Profile

**LOBSTER: Large-Scale Monitoring of Broadband Internet Infrastructure**

- Funded by EC
- A “Specific Support Action”
- **Duration:**
  
- Successor of IST SCAMPI (R&D Project)
- SCAMPI: a SCAlable Monitoring Platform for the Internet
  
  • High-performance single node monitoring

The LOBSTER infrastructure

**LOBSTER**

- A network of passive Internet traffic monitors
- **Cooperation:**
  
  • **Exchange** information and observations
  • **Correlate** results
Dr. Panos Trimintzios, FORTH

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 (Distributed Monitoring Application Programming Interface)
  - MAPI developed within the SCAMPI project

Dr. Panos Trimintzios, FORTH
Research Infrastructures Information Event, 26-27 May, Brussels
• 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

• Accurate traffic monitoring
  – How much of your bandwidth is going to file sharing applications such as Gnutella?
  – Which application generates most of the traffic?
Potential LOBSTER applications …

- 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
  - …

Who can benefit from LOBSTER?

- 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
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

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
  – ALCATEL, France
  – Endace, UK
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

Distributed Passive Network Monitoring
the LOBSTER project

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