

Passive Network Monitoring: the SCAMPI and LOBSTER projects



Information Society
Technologies

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

<http://www.lobster.gr>

Evangelos Markatos, Ph.D.

Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Crete, Greece



Evangelos Markatos, FORTH



Roadmap of the Talk



Information Society
Technologies

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

<http://www.lobster.gr>

- Motivation
 - What is the problem?
 - Our understanding of the Internet needs to be improved
- Solution
 - Better Internet traffic monitoring through the SCAMPI/LOBSTER
- Summary



Evangelos Markatos, FORTH



What is the problem?

- Our understanding of the Internet needs to be improved
 - For example
 - We do not know
 - which applications generate most traffic
 - We suffer
 - malicious cyberattacks such as viruses and worms, spyware, DoS/DDoS attacks
 - We witness incidents
 - of “friendly fire” - Unintentional attacks to major Internet servers
- What is going on out there?



Problem I: Security

- Our understanding of the Internet needs to be improved
 - For example
 - We suffer
 - malicious cyberattacks such as viruses and worms, spyware, dos/ddos attacks
 - We do not know
 - which applications generate most traffic
 - We witness incidents
 - of “friendly fire” - Unintentional attacks to major Internet servers
- What is going on out there?

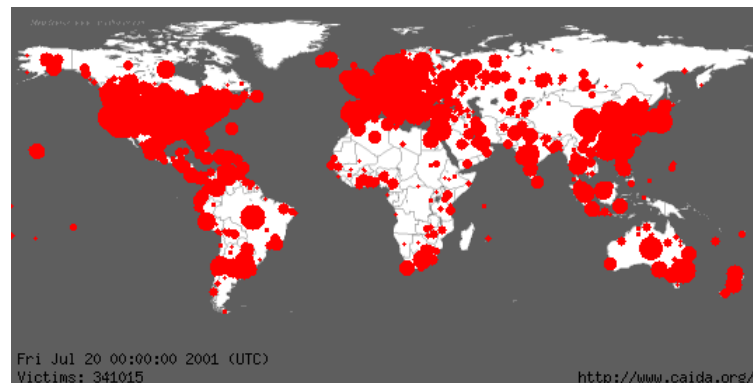


Cyberattacks continue to plague our networks

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

<http://www.lobster.gr>

- 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



Evangelos Markatos, FORTH

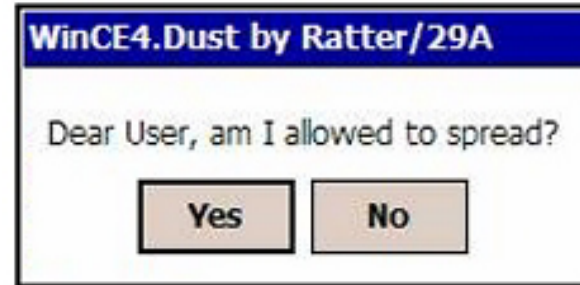


Cyberattacks in palmtops and mobile phones

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

<http://www.lobster.gr>

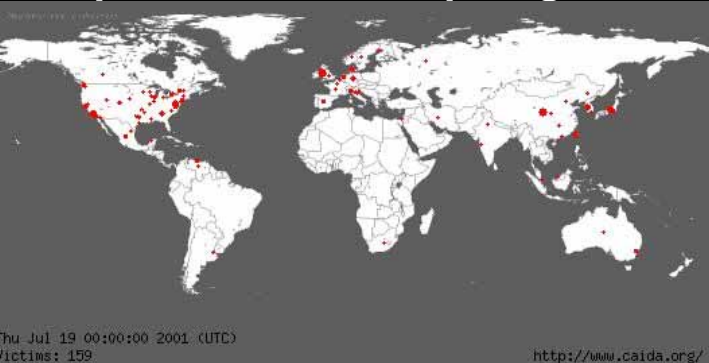
- PocketPC virus:
 - Duts
- Mobile phone virus:
 - Cabir
 - Infects the Symbian operating system



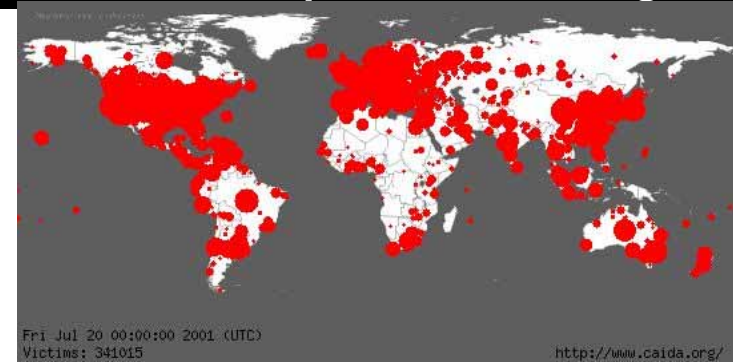
Evangelos Markatos, FORTH

Why do Cyberattacks continue to plague Internet?

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



<http://www.lobster.gr>



- Defense against worms consists of
 - **Detection** (of the worm)
 - It takes several minutes to a few hours (semi-manual)
 - **Identification** (i.e. generate an IDS signature or firewall rule)
 - It takes a few hours (manual)
 - **Deployment** of signatures to firewalls/IDSs
 - It takes minutes to hours

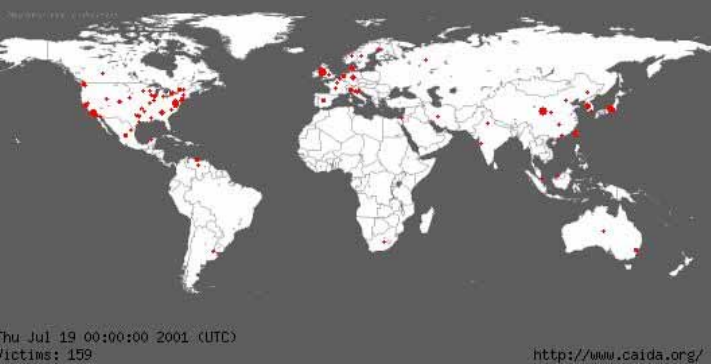


Evangelos Markatos, FORTH

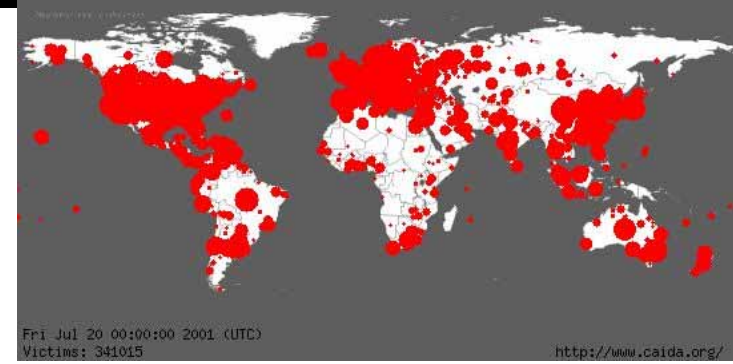


Why do Cyberattacks continue to plague Internet? II

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



<http://www.lobster.gr>



- Cyberattack Detection, identification, response/deployment
 - May take several hours
- Which implies that
 - cyberattack response is initiated
 - AFTER almost all computers have been infected
 - and AFTER the attack is practically over
 - Can we start response BEFORE all computers have been infected?

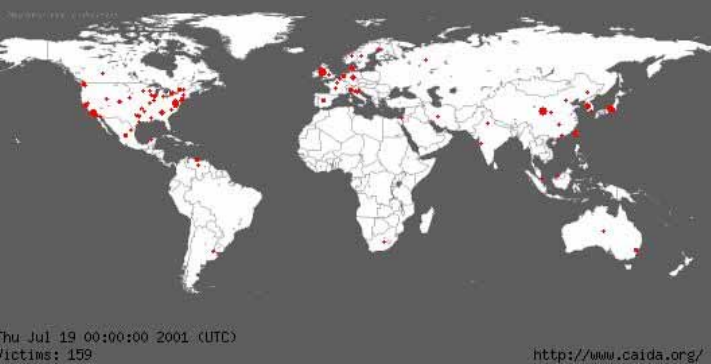


Evangelos Markatos, FORTH

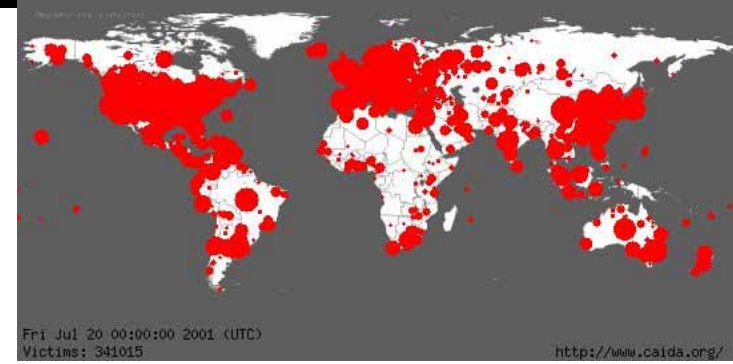


Why do Cyberattacks continue to plague Internet? III

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



<http://www.lobster.gr>



- Can we start response **BEFORE** all computers have been infected?
 - Yes! But we need:
 - Smart Internet traffic monitoring sensors
 - Capable of detecting new worms
 - Distributed infrastructure of Internet traffic sensors
 - More sensitive to attacks
 - pinpoint attacks as soon as they emerge
 - Spread information about new worms fast



Evangelos Markatos, FORTH



Problem II: traffic accounting

- Our understanding of the Internet needs to be improved
 - For example
 - We suffer
 - malicious cyberattacks such as viruses and worms, spyware, dos/ddos attacks
 - We do not know
 - which applications generate most traffic
 - We witness incidents
 - of “friendly fire” - Unintentional attacks to Root DNSs
- What is going on out there?



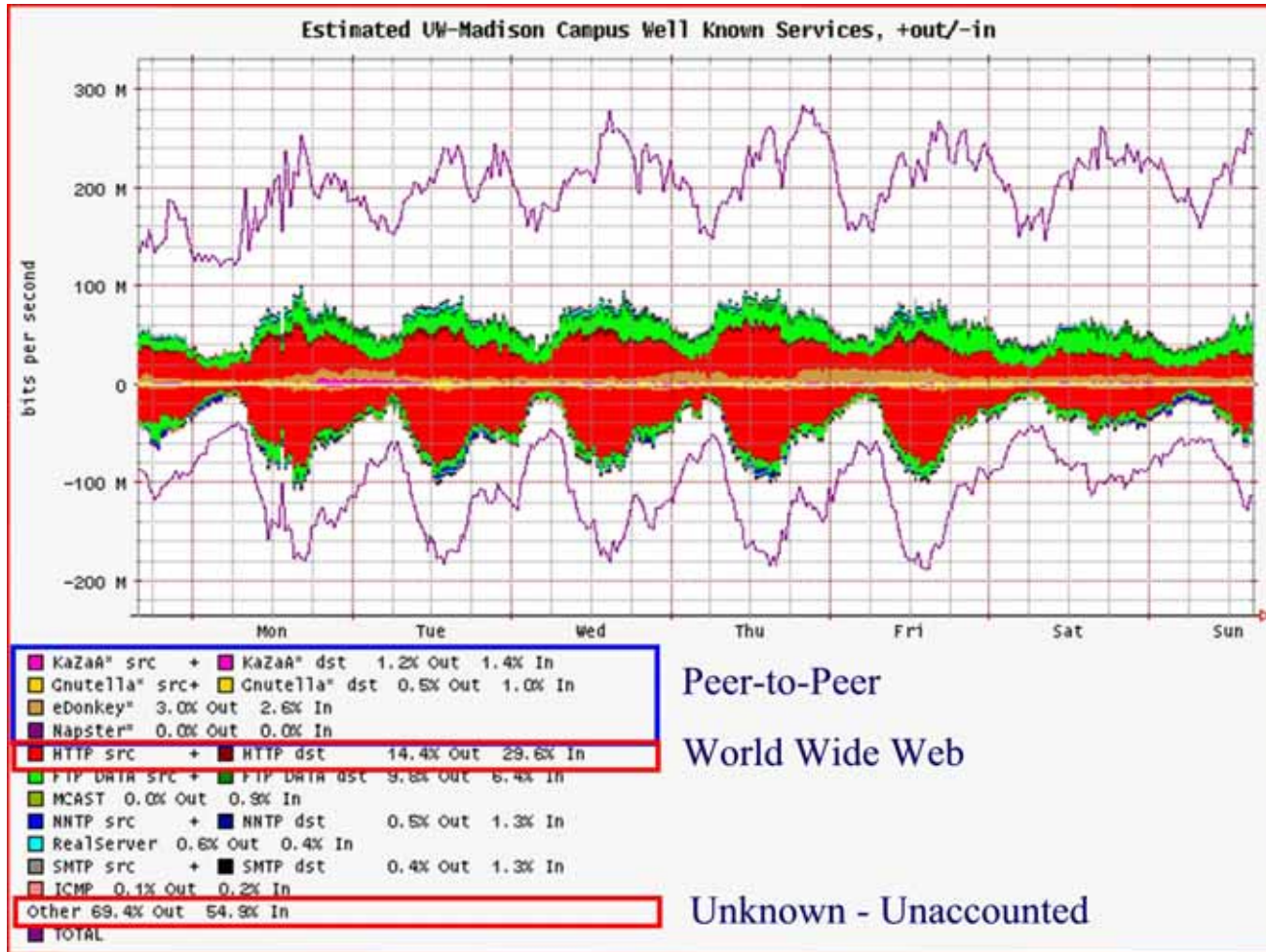
Problem II: Who generates all this traffic?



Information Society
Technologies

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

<http://www.lobster.gr>



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



Evangelos Markatos, FORTH



Problem III: “Friendly Fire”



Information Society
Technologies

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

<http://www.lobster.gr>

- Our understanding of the Internet needs to be improved
 - For example
 - We suffer
 - malicious cyberattacks such as viruses and worms, spyware, dos/ddos attacks
 - We do not know
 - which applications generate most traffic
 - We witness incidents
 - of “friendly fire” - Unintentional attacks to major Internet servers
- What is going on out there?



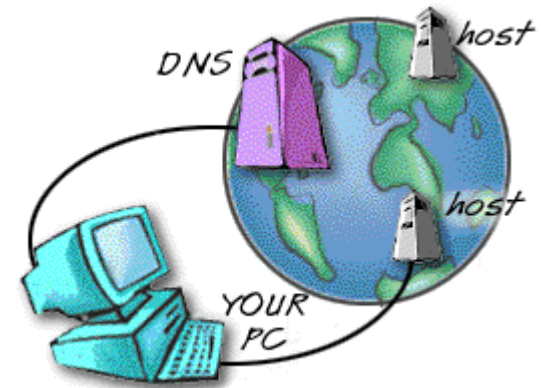
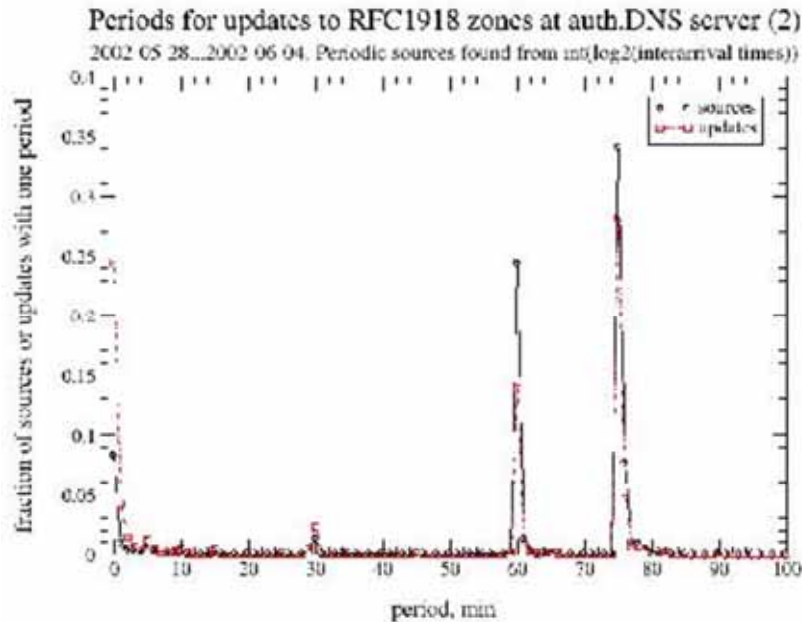
Evangelos Markatos, FORTH



“Friendly Fire” on the Internet

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

<http://www.lobster.gr>



- Win 2K and Win XP computers
 - Started updating root DNS servers
 - Created significant load to DNS
 - Not clear why...

So, what do these all mean?



Information Society
Technologies

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

<http://www.lobster.gr>

- Our understanding of the Internet
 - Needs to be improved
- The gap between
 - What we measure/understand, and
 - What is really going on out there
 - is already large,
 - and is probably getting larger



Evangelos Markatos, FORTH



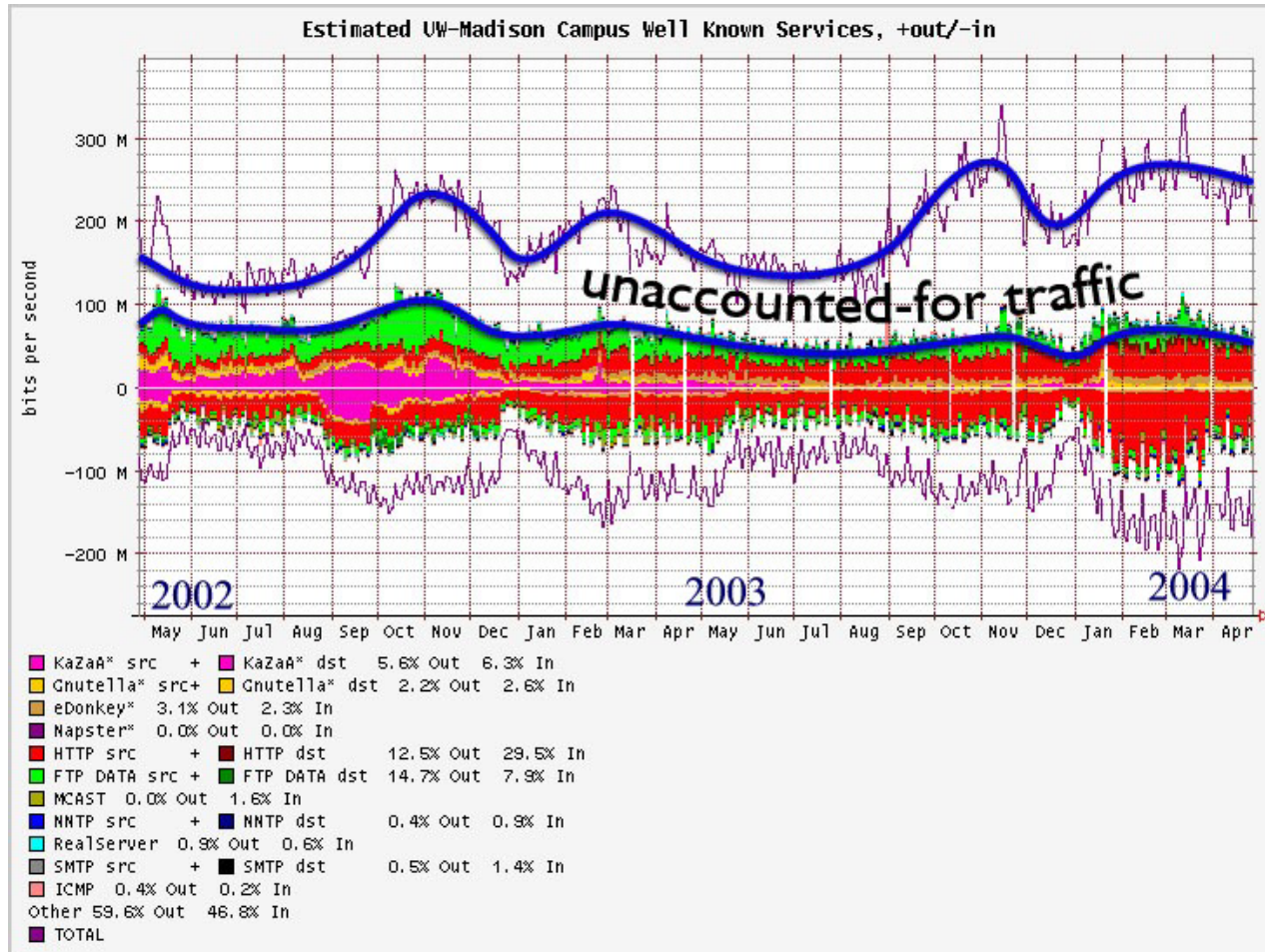
The GAP



Information Society
Technologies

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

<http://www.lobster.gr>



- The GAP continues to widen with time...

Evangelos Markatos, FORTH



Solution?

- We need better Internet traffic monitoring
 - Faster
 - i.e. to detect worms BEFORE they infect the planet
 - More accurate
 - i.e. to close the gap between what we measure and what is going on



SCAMPI and LOBSTER: two steps for better Internet Monitoring

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

<http://www.lobster.gr>

- SCAMPI: a SCAlable Monitoring Platform for the Internet
- LOBSTER: Large Scale Monitoring of Broadband Internet Infrastructure



Evangelos Markatos, FORTH



SCAMPI



- SCAMPI is an IST project
- Funded by European Commission
- Duration: 1/4/02-31/3/05



SCAMPI: What is it?

- A passive monitoring platform
- Passive means:
 - capture **all network traffic** and examine it
- How?
 - Develop a 10 Gbps FPGA-based card
 - Develop a Monitoring Application Programming Interface (MAPI)
 - Develop Monitoring Applications



SCAMPI: What is it good for?

- Security – **High-speed** Intrusion Detection:
 - Find all packets that are being sent to my network and contain the “CODE-RED” worm
 - Find all computers in my network that are infected with backdoors
- Security - DDOS attack detection
- Performance Analysis
 - What percentage of my traffic goes to KaZaA?
 - What is my network latency to <http://www.cnn.com>?



SCAMPI: What are its benefits?

- **Portability:** MAPI has been ported to
 - Commodity network interfaces
 - DAG packet capture cards
 - SCAMPI card
 - Partial implementations also exist for
 - IXP 1200 network processors



SCAMPI: What are its benefits?

- Ease of use
- MAPI provides high-level abstractions
 - **More expressive**: users can better communicate their monitoring needs to the system [NOMS 03]
 - **Faster**: MAPI can capitalize on underlying special-purpose monitoring hardware [MASCOTS 03]
- The end result:

Shorter and Faster monitoring applications



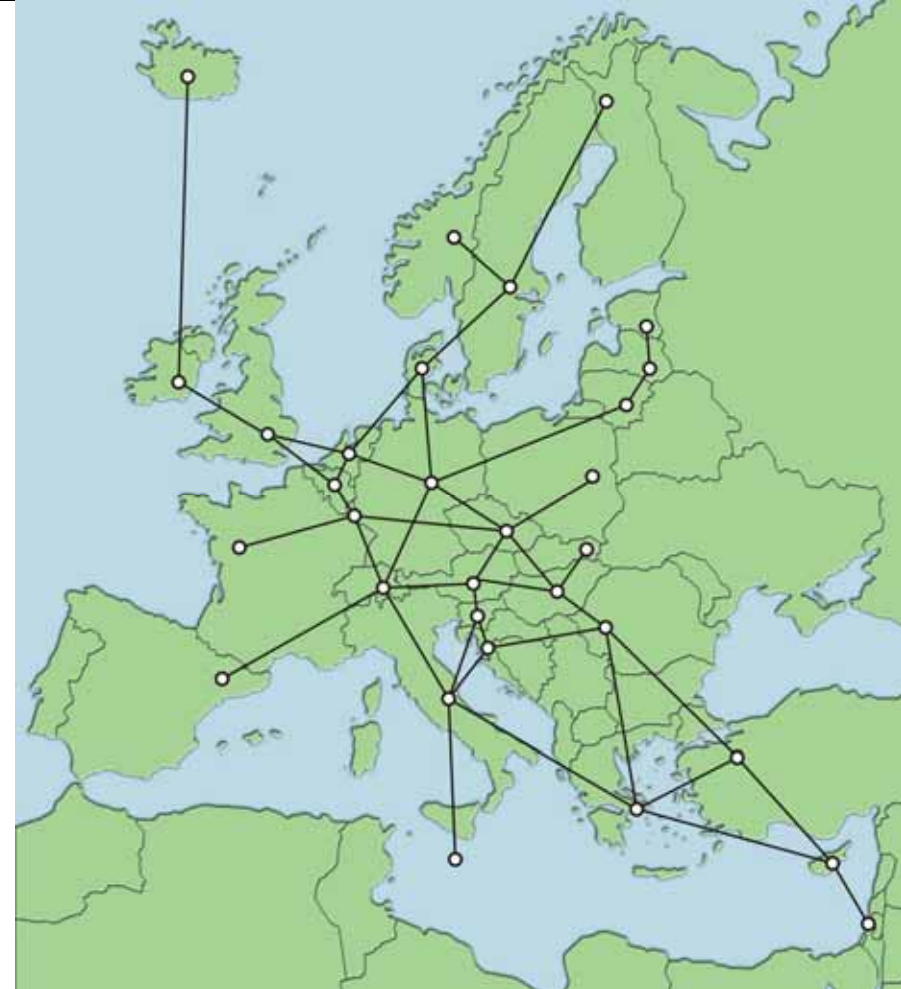
SCAMPI: What are its benefits?

- **Speed**

- FPGA-based card allows hardware implementation of important functions
 - e.g. packet filtering/pre-processing
- Novel algorithms allow faster packet processing
 - e.g. high-speed string searching [SEC03]



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



LOBSTER SSA



Information Society
Technologies

- LOBSTER is a
 - Specific Support Action
- Funded by European Commission
- Two-year project
 - Duration 1/10/05-31/12/06



Evangelos Markatos, FORTH



Challenging issues I

- Trust: cooperating sensors may not trust each other
 - Protection of private data
 - Protection of confidential data
 - Solution: anonymization
 - Outside users will be able to operate on
 - Anonymized data



Challenging issues II



Information Society
Technologies

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

<http://www.lobster.gr>

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



Evangelos Markatos, FORTH



- 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



Information Society
Technologies

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

<http://www.lobster.gr>

- Automatic Detection of New worms
- Contributes to early-warning System
 - Detect worms within minutes
 - i.e. before they manage to spread
- Facilitates early response to worms
 - Before they infect all computers



Evangelos Markatos, FORTH



- GRID Performance debugging
 - GRID-enabled applications access:
 - Remote data
 - Remote resources (e.g. sensors, instruments)
 - Remote computing power
 - How can you figure out what is the problem if the application is slow?
 - The local LAN? the WAN? The remote LAN?
 - The local computer? The remote server? A middleware server?



Who can benefit from LOBSTER?

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

<http://www.lobster.gr>

- NRNs/ISPs
 - Better Internet traffic monitoring of their networks
 - Better understanding of their interactions with other NRNs/ISPs
- Security Researchers
 - Access to anonymized data
 - Access to anonymized testbed
 - Study trends and validate theories about cybersecurity
- Network/Security Administrators
 - Access to a traffic monitoring Infrastructure
 - Access to early-warning systems
 - Access to software and tools



Evangelos Markatos, FORTH



Summary

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

<http://www.lobster.gr>

- Our understanding of the Internet
 - needs to be improved
- SCAMPI/LOBSTER will provide better monitoring
 - based on
 - A network of passive monitoring sensors, and
 - State-of-the-art passive monitoring research
 - and by providing
 - Trusted co-operation in an un-trusted world
 - Common programming platform
 - Resilience to attackers



Evangelos Markatos, FORTH



Passive Network Monitoring: the SCAMPI and LOBSTER projects



Information Society
Technologies

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

<http://www.lobster.gr>

Evangelos Markatos, Ph.D.

Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Crete, Greece



Evangelos Markatos, FORTH



LOBSTER partners



Information Society
Technologies

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

<http://www.lobster.gr>

- 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



Evangelos Markatos, FORTH



SCAMPI partners



Information Society
Technologies

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

<http://www.lobster.gr>

- Research Organizations
 - ICS-FORTH, Greece
 - University of Leiden, The Netherlands
 - Masaryk University, Czech Republic
 - IMEC, Belgium
- NRNs/ISPs, Associations
 - CESNET, Czech Republic
 - UNINETT, Norway
 - FORTHNET, Greece
 - TERENA, The Netherlands
- Industrial Partners
 - NETIKOS, Italy
 - SIEMENS, Germany
 - 4PLUS, Greece



Evangelos Markatos, FORTH

