



Information Society
Technologies

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

<http://www.lobster.gr>

Network Monitoring for Performance and Security

The SCAMPI and LOBSTER projects

Kostas Anagnostakis

Institute of Computer Science (ICS)

Foundation for Research and Technology – Hellas (FORTH)

Crete, Greece



Kostas Anagnostakis, FORTH



Talk Roadmap

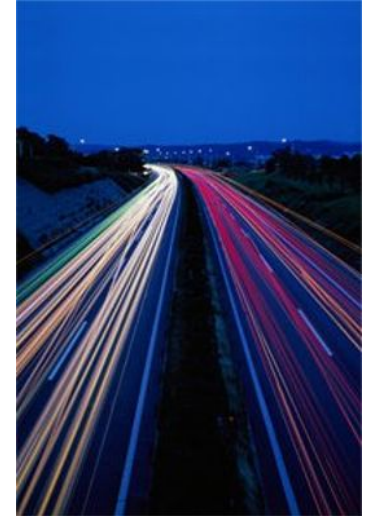


Information Society
Technologies

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

<http://www.lobster.gr>

- Motivation
 - Understanding the Internet
 - Performance, diagnosis and security
- EC-funded work on net. monitoring
 - R&D: SCAMPI (2001-2004)
 - Pilot Infrastructure: LOBSTER (2005-2007)



Kostas Anagnostakis, FORTH



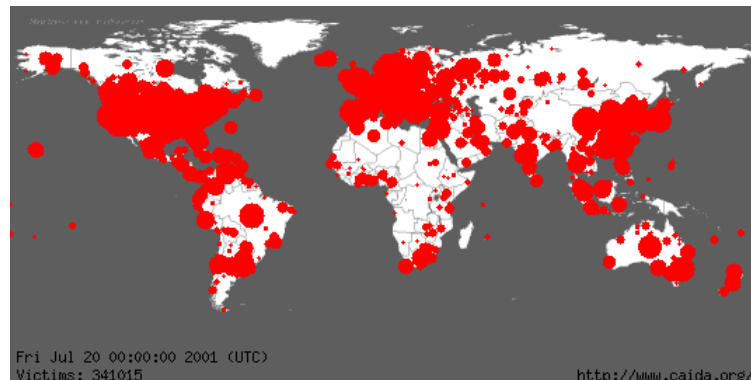
What is the problem?

- 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
 - “Friendly fire”: unintentional attacks to major Internet services



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

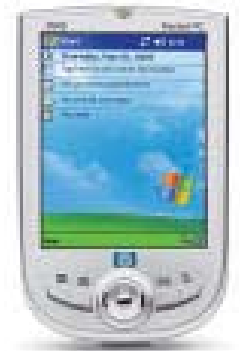
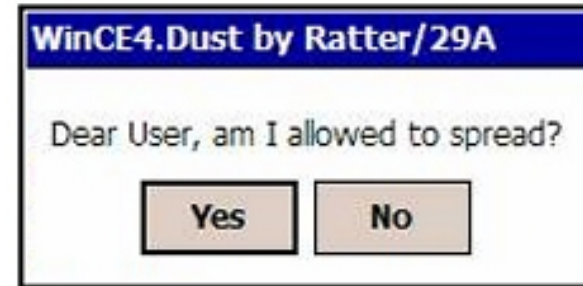


Kostas Anagnostakis, FORTH



Cyberattacks in palmtops and mobile phones

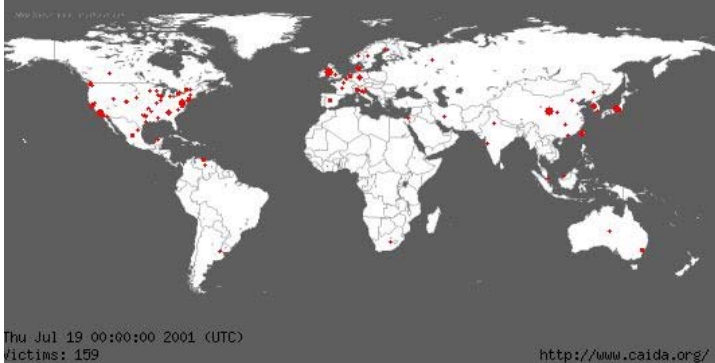
- PocketPC virus:
 - Duts
- Mobile phone virus:
 - Cabir
 - Infects the Symbian operating system



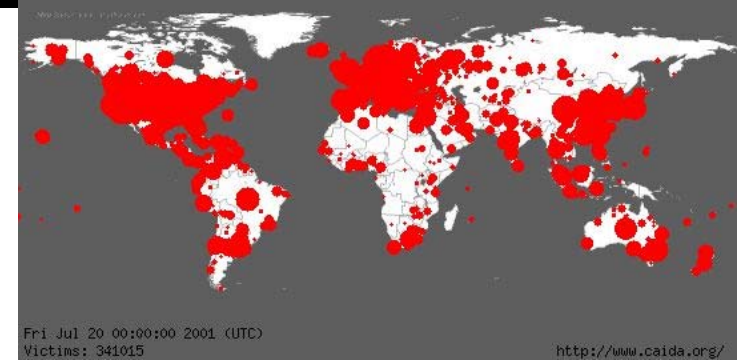
Why do Cyberattacks continue to plague Internet?



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



<http://www.lobster.gr>



- Defense against worms:
 - **Detection:**
 - minutes to hours (semi-manual)
 - **Identification** (i.e., generate an IDS signature or firewall rule)
 - Hours (manual)
 - **Deployment** of signatures to firewalls/IDSs, and patching
 - Minutes to hours



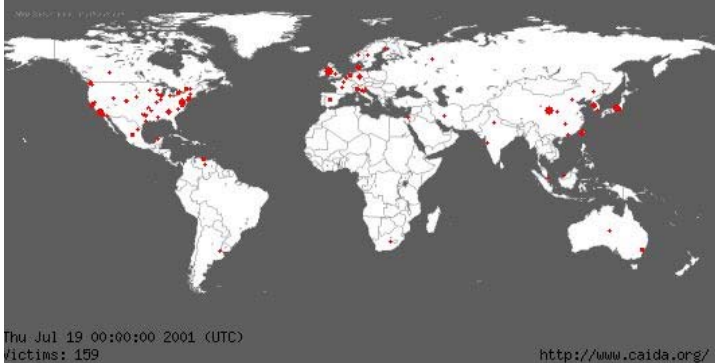
Kostas Anagnostakis, FORTH



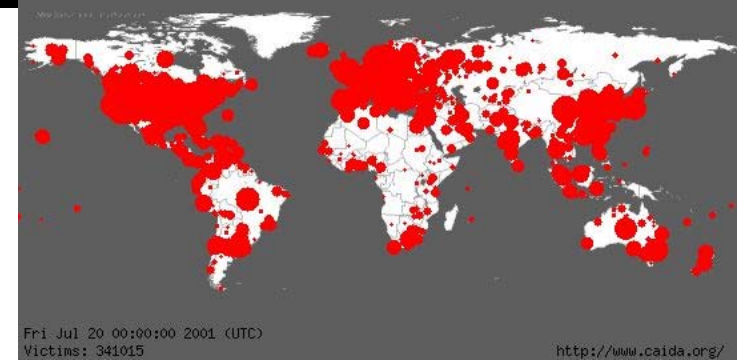
Why do Cyberattacks continue to plague Internet? II



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



<http://www.lobster.gr>



- 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?



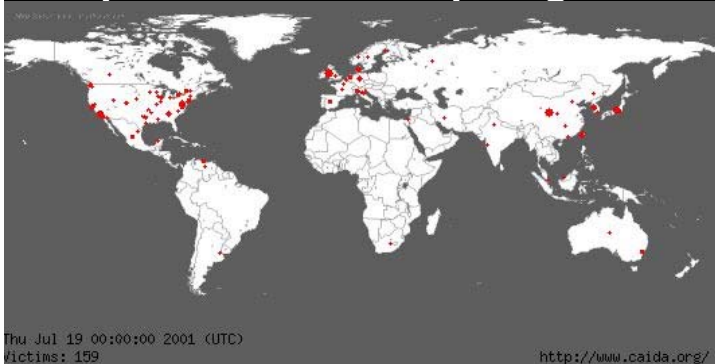
Kostas Anagnostakis, FORTH



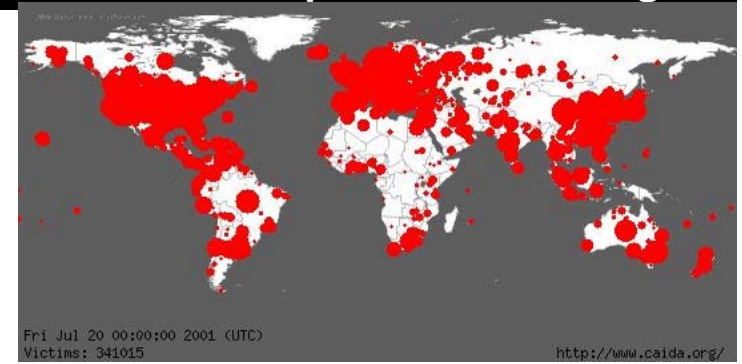
Why do Cyberattacks continue to plague Internet? III



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



<http://www.lobster.gr>



- Can we respond **before** the damage is done?
- Yes! But we need:
 - Smart, flexible, high-performance Internet 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



Kostas Anagnostakis, FORTH



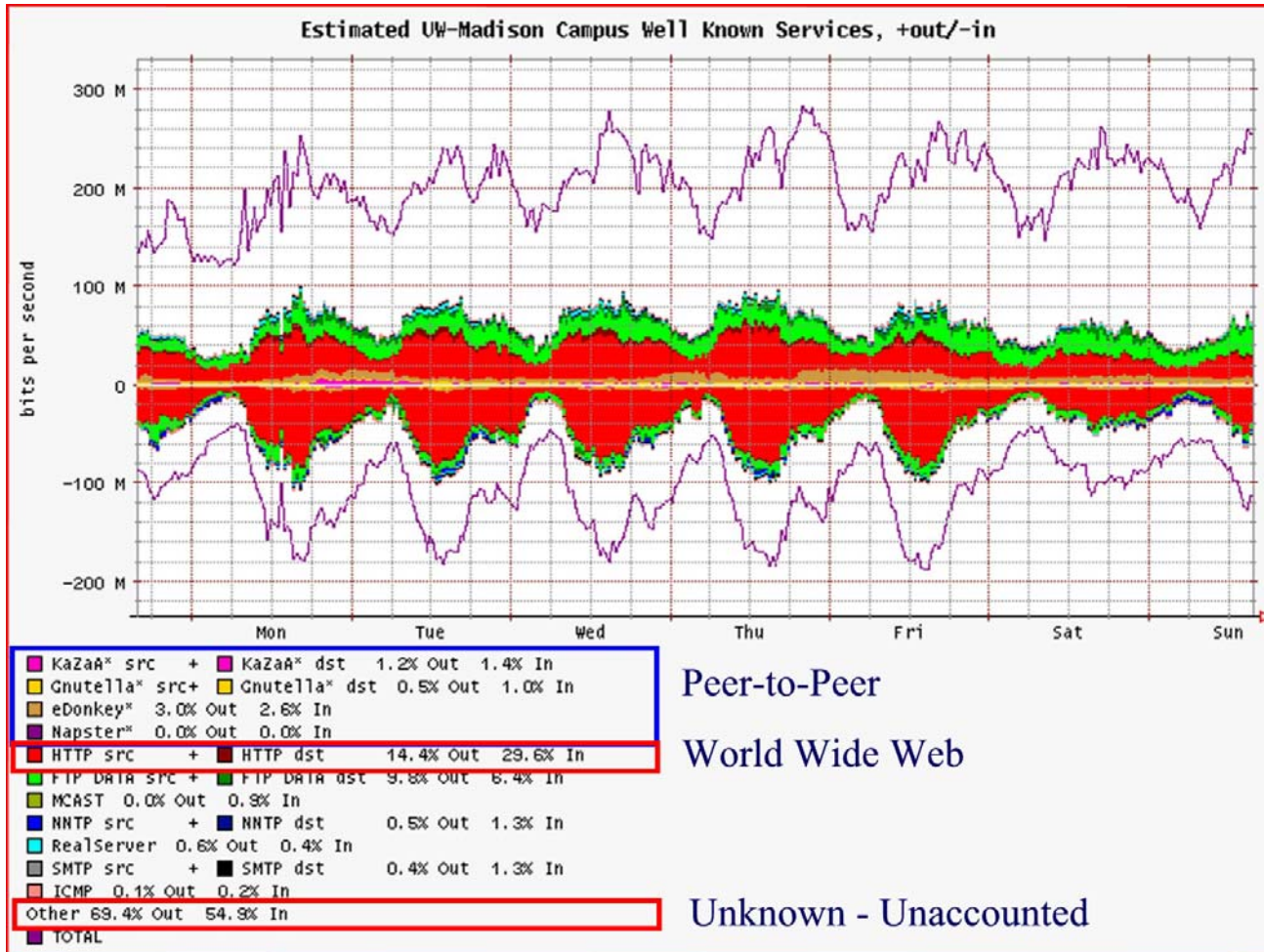
Problem II: Who generates all this traffic?



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



Kostas Anagnostakis, FORTH



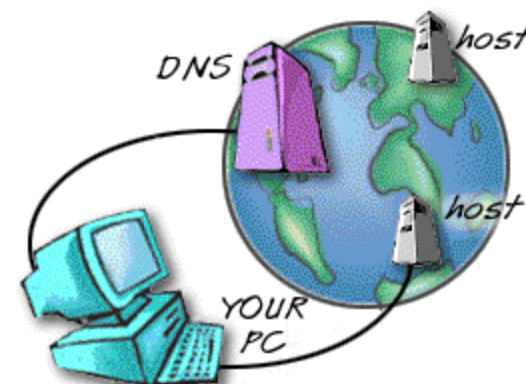
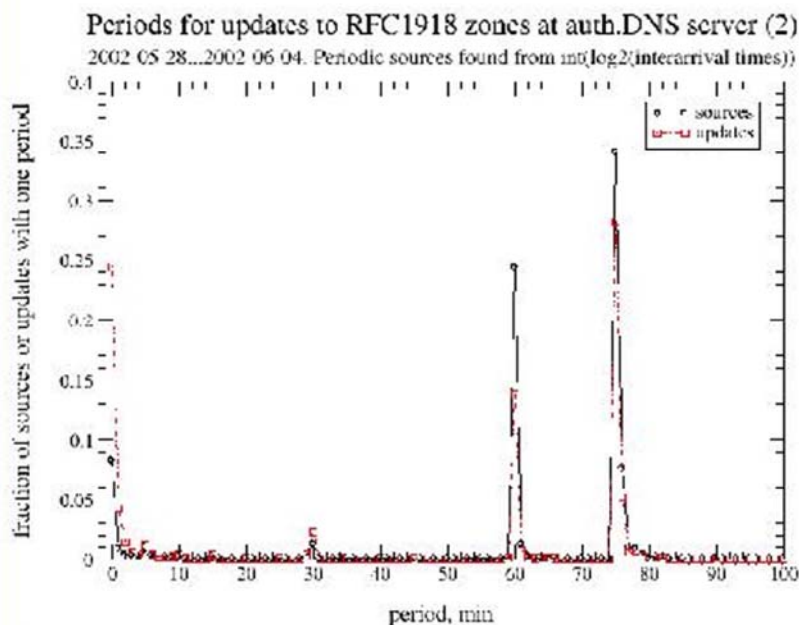
“Friendly Fire” on the Internet



Information Society
Technologies

<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...



Kostas Anagnostakis, FORTH



Problem summary



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 can measure and what we need to measure is large and getting larger



Kostas Anagnostakis, FORTH



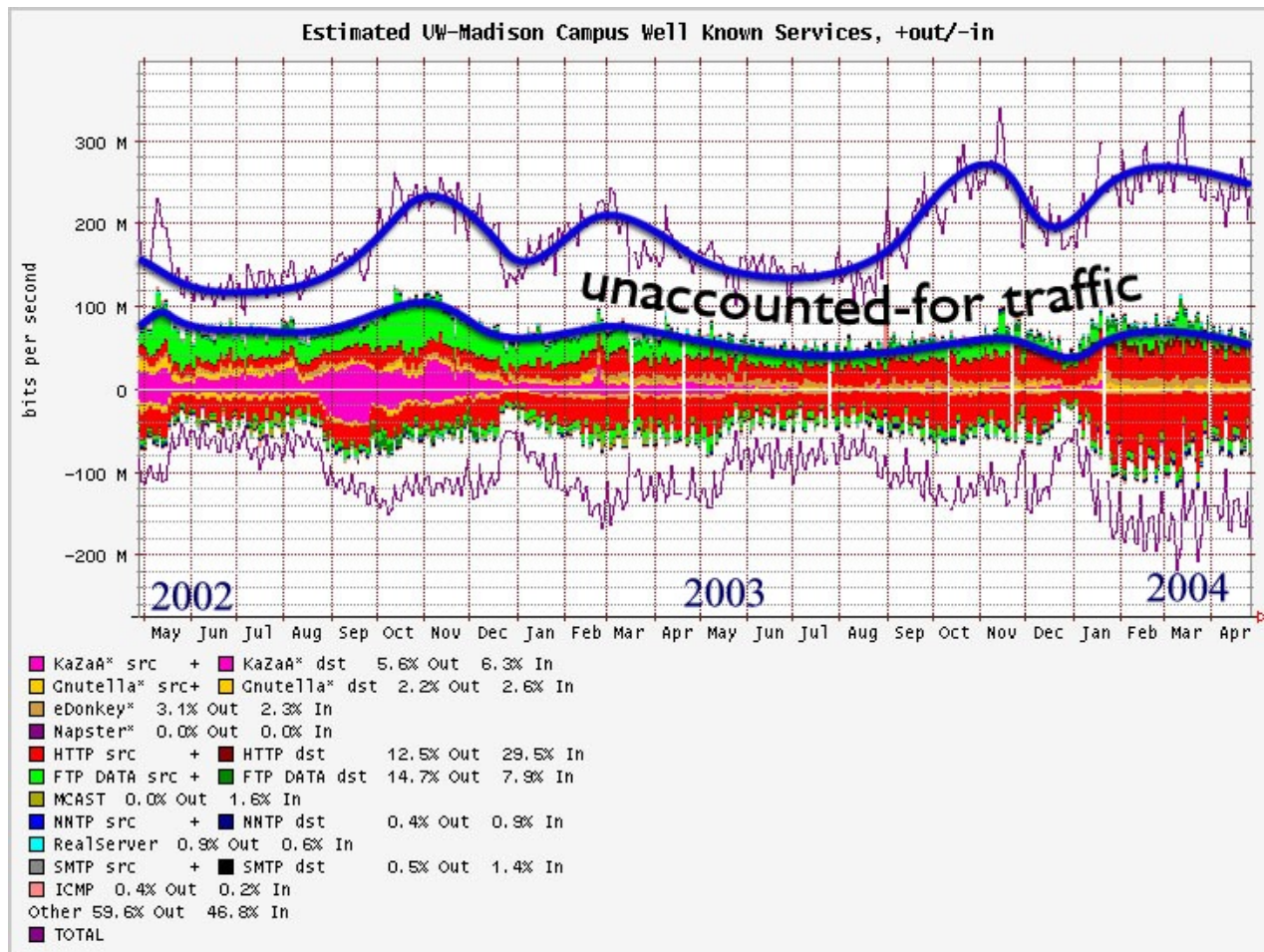
Unaccounted traffic is increasing



Information Society
Technologies

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

<http://www.lobster.gr>



- The gap continues to widen with time...



Kostas Anagnostakis, FORTH



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



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



Kostas Anagnostakis, FORTH



SCAMPI



Information Society
Technologies

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

<http://www.lobster.gr>



Information Society
Technologies

- SCAMPI profile:
 - IST R&D project
 - Funded by European Commission
 - Duration: 1/4/02-31/3/05



Kostas Anagnostakis, FORTH



SCAMPI: Goals



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

<http://www.lobster.gr>

- Develop a passive monitoring platform
 - capture **all network traffic** and examine it
- Technology:
 - Develop a 10 Gbps FPGA-based card
 - Develop a Monitoring Application Programming Interface (MAPI)
 - Develop efficient monitoring applications



Kostas Anagnostakis, FORTH



SCAMPI: Achievements



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

<http://www.lobster.gr>

- 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>?



Kostas Anagnostakis, FORTH



SCAMPI: Achievements II



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

<http://www.lobster.gr>

- **Portability:** MAPI has been ported to
 - Commodity network interfaces
 - Endace DAG packet capture cards
 - SCAMPI 10 Gbit/s card
 - Partial implementations also exist for Intel IXP network processors



Kostas Anagnostakis, FORTH



SCAMPI: Achievements III

- MAPI provides high-level abstractions
 - **Ease of use**
 - **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:
 - Improved network monitoring capability**



SCAMPI: Achievements IV



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

<http://www.lobster.gr>

- **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]



Kostas Anagnostakis, FORTH



The LOBSTER infrastructure

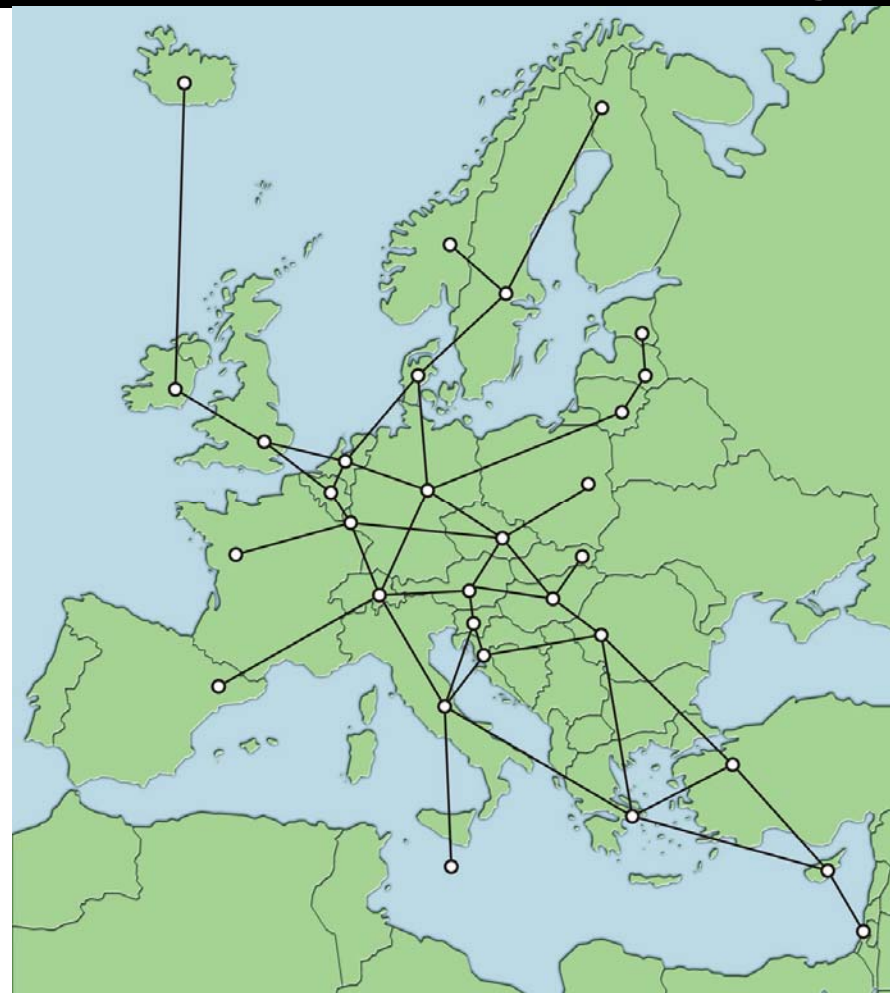


Information Society
Technologies

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

<http://www.lobster.gr>

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



Kostas Anagnostakis, FORTH



LOBSTER SSA



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

<http://www.lobster.gr>



Information Society
Technologies

- LOBSTER profile:
 - A “Specific Support Action”
 - Funded by European Commission
 - Two-year project: 1/1/05-31/12/06



Kostas Anagnostakis, FORTH



Challenging issues I

- 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 on **anonymized data** only



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



Kostas Anagnostakis, FORTH



Challenging issues III



Information Society
Technologies

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

<http://www.lobster.gr>

- 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



Kostas Anagnostakis, FORTH



- 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



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

<http://www.lobster.gr>

- Automatic detection of new worms
 - Detect worms within minutes
- Early-warning
 - Alert administrators+users about potential attacks
- Timely response to worms
 - Generate attack signature



Kostas Anagnostakis, FORTH



Potential LOBSTER applications: GRIDs



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

<http://www.lobster.gr>

- GRID Performance debugging
 - GRID-enabled applications highly dependent on network characteristics
 - Remote data access
 - Remote resource access (e.g. sensors, instruments)
 - Remote computing power
 - How can we perform complete diagnosis when applications are not working as expected?
 - The local LAN? the WAN? The remote LAN?
 - The local computer? The remote server? A middleware server?



Kostas Anagnostakis, FORTH



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 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



Kostas Anagnostakis, FORTH



Summary

- Our understanding of the Internet needs to be improved
- SCAMPI/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



Passive Network Monitoring: the SCAMPI and LOBSTER projects



Information Society
Technologies

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

<http://www.lobster.gr>

Kostas Anagnostakis

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



Kostas Anagnostakis, 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



Kostas Anagnostakis, 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



Kostas Anagnostakis, FORTH

