

A map of Europe with a network of nodes and lines overlaid, representing broadband internet infrastructure. The nodes are small circles connected by thin lines, forming a complex web across the continent. The map is light green and blue, with the network lines in a darker green.

LOBSTER:
Large Scale Monitoring of
Broadband Internet Infrastructure

Evangelos Markatos

markatos@ics.forth.gr

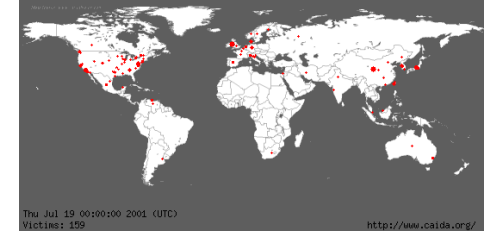
<http://www.ics.forth.gr/~markatos>

Institute of Computer Science (ICS)

**Foundation for Research and Technology – Hellas
(FORTH)**



Roadmap of the Talk



ICS-FORTH

- **Motivation**

- What is the problem?
- Our understanding of the Internet continues to fade away

- **Solution**

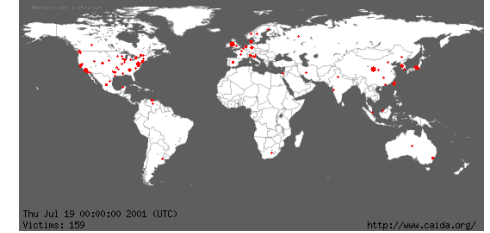
- The LOBSTER approach and infrastructure

- **How can you participate?**





What is the problem?



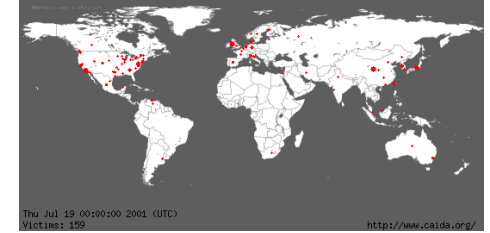
ICS-FORTH

- **Our understanding of the Internet continues to fade away**
 - For example
 - ✓ We do not know
 - which applications generate most traffic
 - ✓ We suffer
 - malicious cyberattacks such as viruses and worms
 - ✓ We witness incidents
 - of “friendly fire” - Unintentional attacks to Root DNSs
- **What is going on down there?**

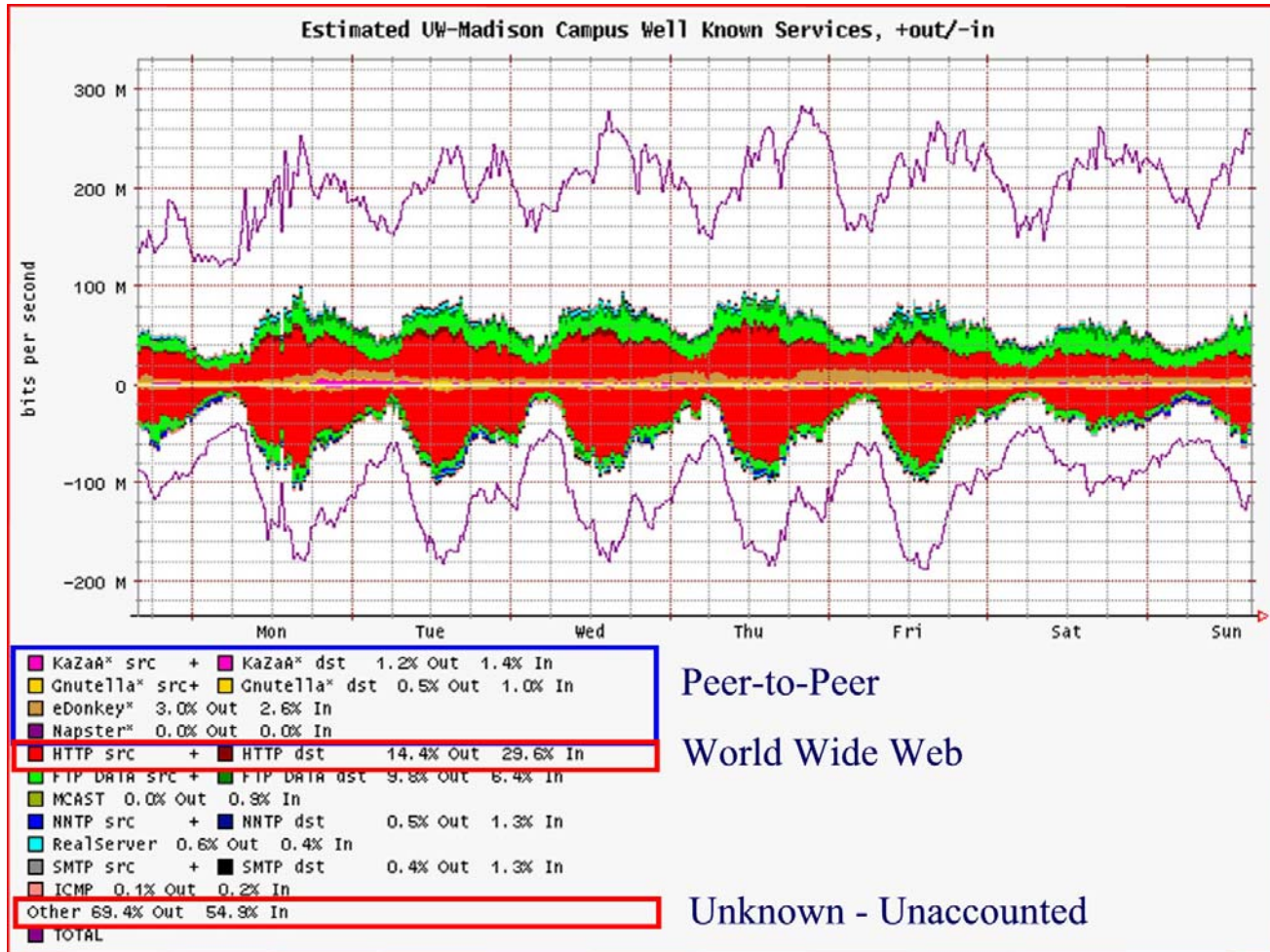




Who generates all this traffic?



ICS-FORTH

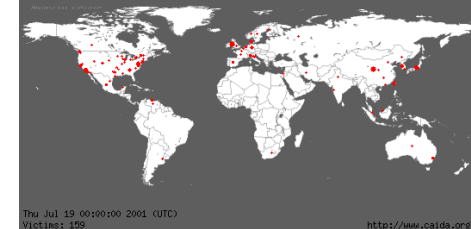


69% of the traffic is unaccounted-for

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



Cyberattacks continue to plague our networks



ICS-FORTH

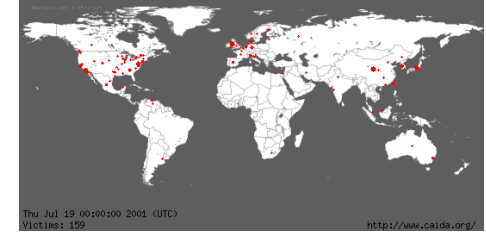
- **Summer 2001: CODE RED worm**
 - 350,000 nodes in 24 hours
- **January 2003: Sapphire/Slammer worm**
 - 75,000 nodes in 30 minutes
- **March 2004: Witty Worm**
 - 20,000 nodes in 60 minutes



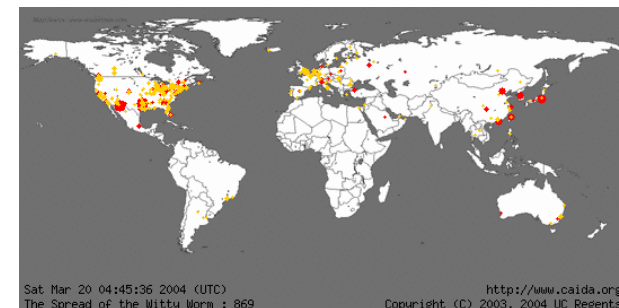
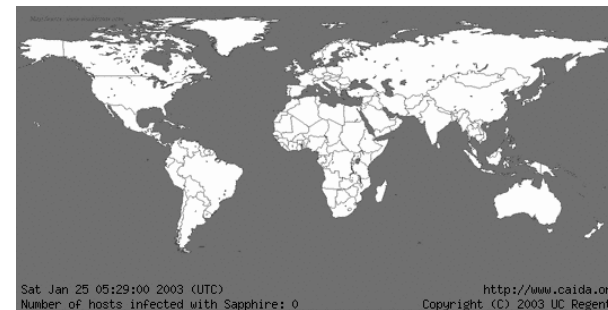
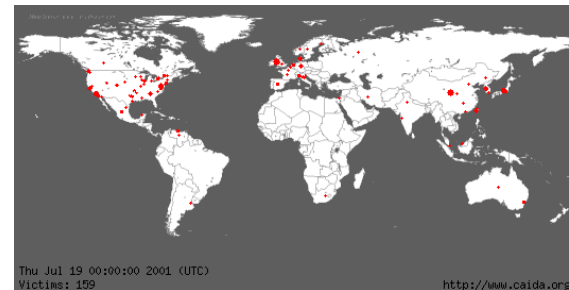


Worms so far

ICS-FORTH

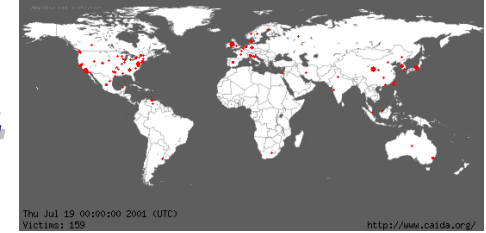


- **Summer 2001:
CODE RED
worm**
- **January 2003:
Sapphire/Slam
mer worm**
- **March 2004:
Witty Worm**

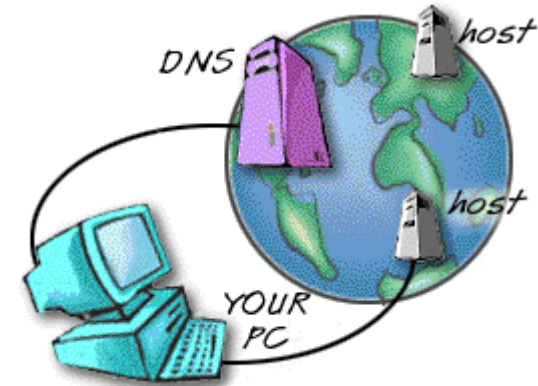
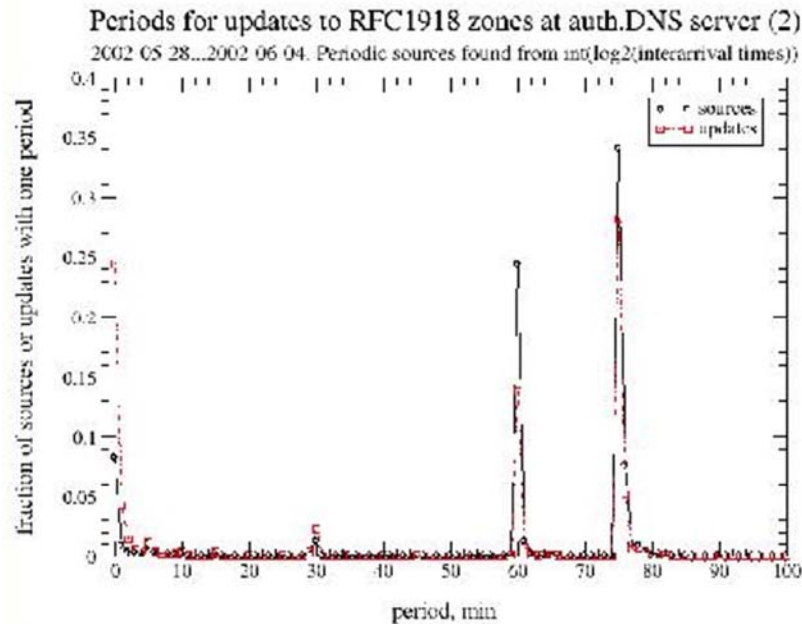




Friendly Fire on the Internet



ICS-FORTH

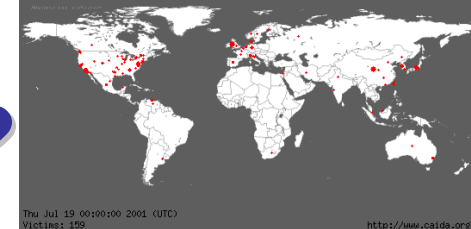


- **Win 2K and Win XP**

- Started updating root DNS servers
- Created significant load to DNS
- Not clear why...



So, what do these all mean?

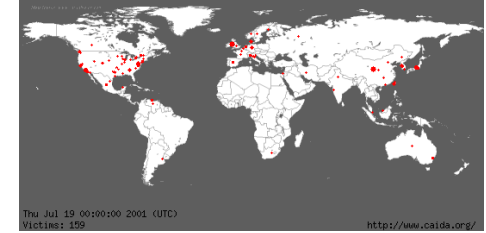


ICS-FORTH

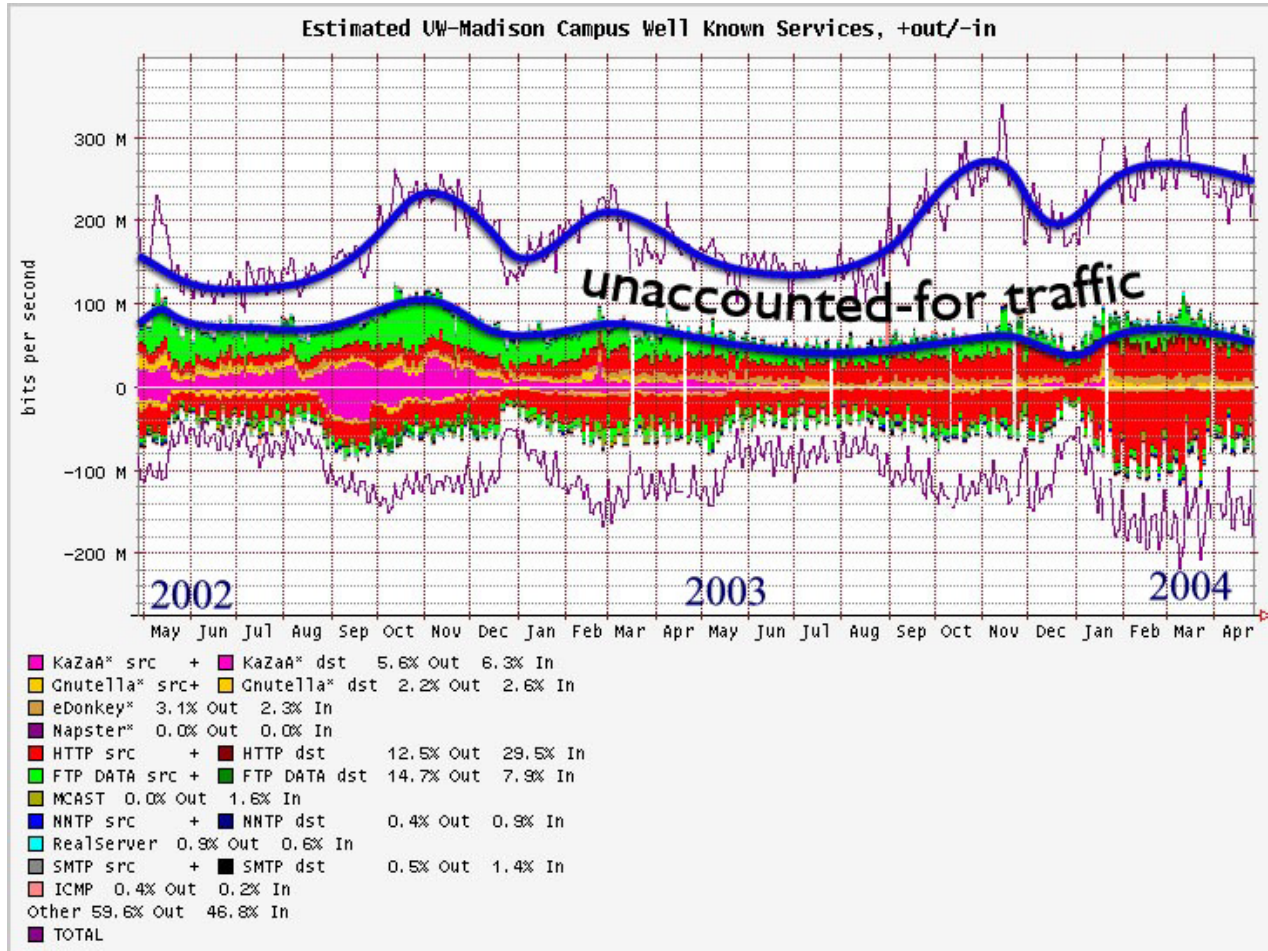
- **Our understanding of the Internet**
 - Continues to fade away
- **The gap between**
 - What we measure/understand, and
 - What is really going on down there
 - Continues to widen



The GAP



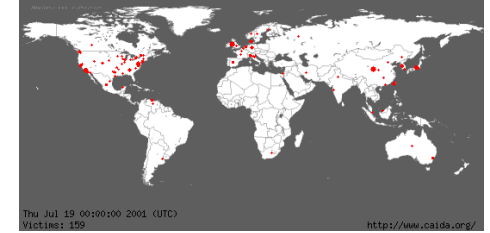
ICS-FORTH



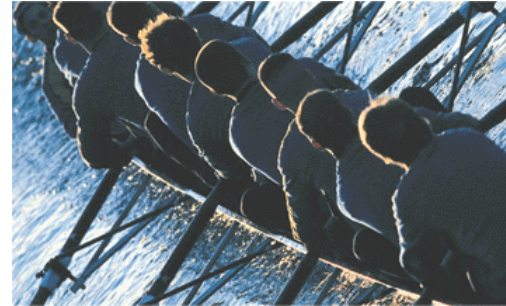
- The GAP continues to widen with time...



Solution: Better monitoring



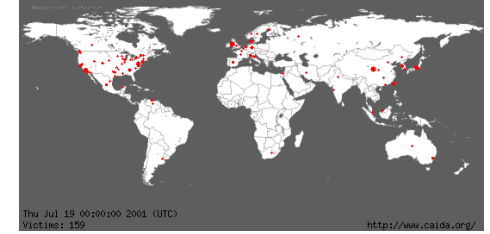
ICS-FORTH



- **A solution should be based on two principles:**
 - **Collaboration** among monitoring sensors
 - ✓ An infrastructure of monitors
 - **State-of-the-art** Research
 - ✓ The **SCAMPI** monitoring system

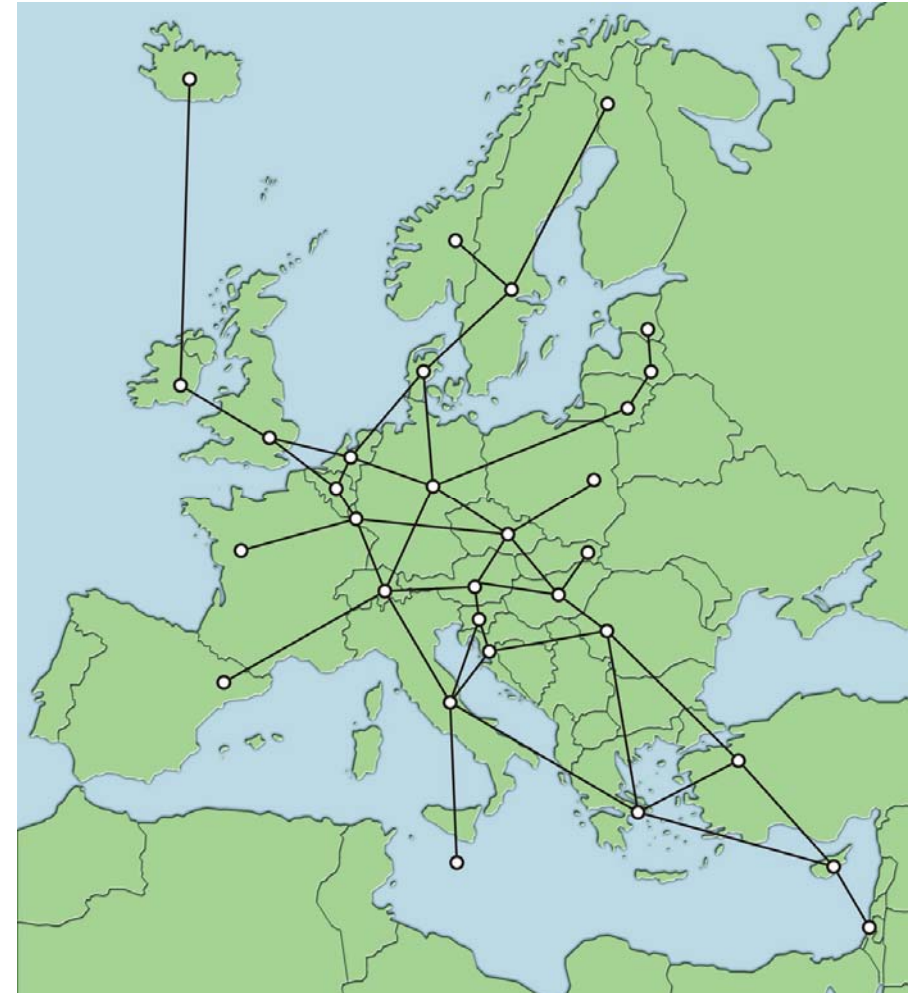


The *LOBSTER* infrastructure



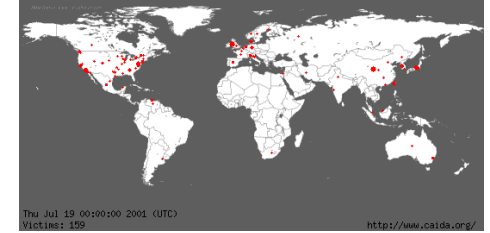
ICS-FORTH

- **LOBSTER**
 - A network of passive monitors
 - That collaborate
 - ✓ **Exchange** information and observations
 - ✓ **Correlate** results





So, what is hard about a network of sensors?



ICS-FORTH

- **Trust: cooperating sensors may not trust each other**

- Protection of private data
- Protection of confidential data

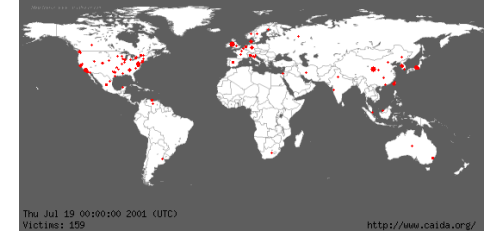


- **Solution: anonymization**

- ✓ Outside users will be able to operate on
- ✓ **Anonymized data**



What is hard about it?



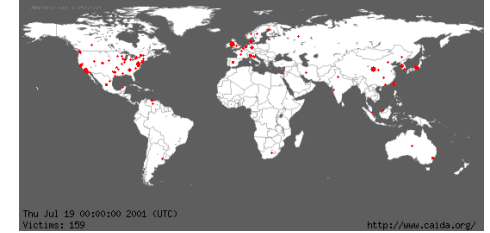
ICS-FORTH

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





What is hard about it?



ICS-FORTH

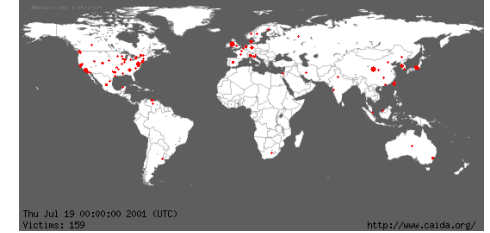
- **Resilience to attackers:
What if intruders
penetrate LOBSTER?**

- Can they have access to collected data?
- **NO!**
 - ✓ Hardware anonymization
 - ✓ LOBSTER computers do not see, store, or transfer clear-text packets





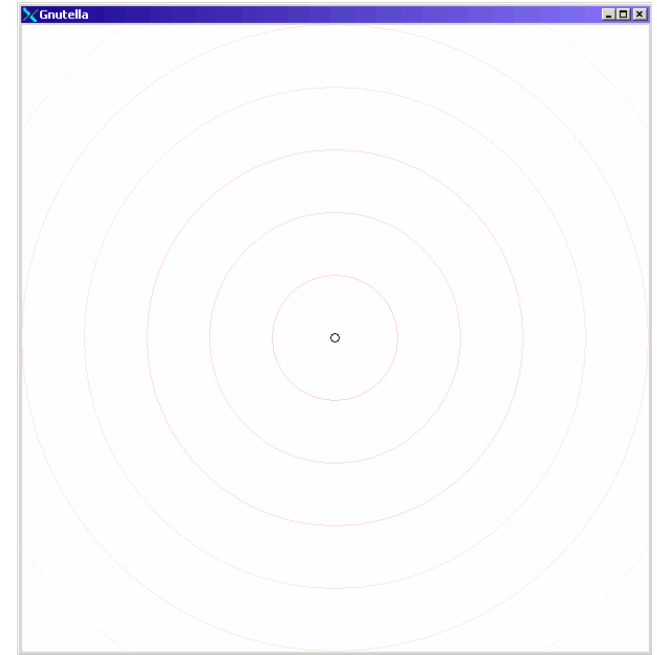
So, what can you do with **LOBSTER?**



ICS-FORTH

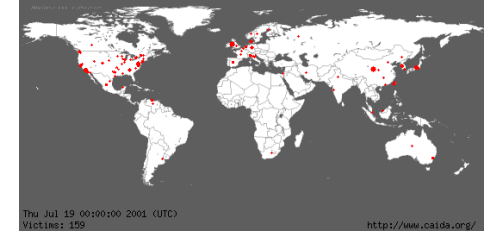
- **Accurate traffic monitoring**

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





So, what can you do with **LOBSTER?**



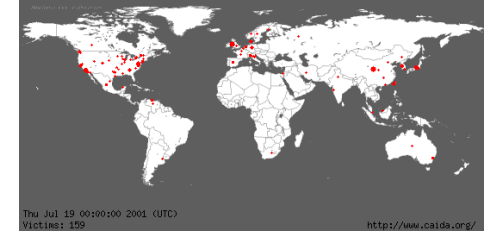
ICS-FORTH

● Performance monitoring

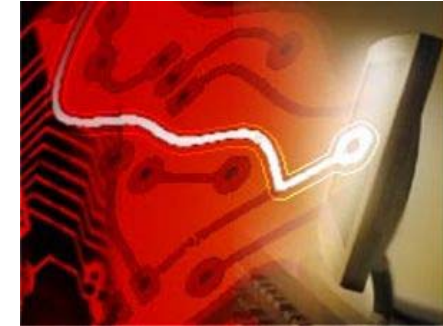
- Know what is your web server's performance for a particular client
 - ✓ e.g. how much time elapsed
 - between the **sending of a URL request** by a client and
 - the **arrival of the last response packet** by my web server?
- Know why your GRID-enabled application is so slow...



What else can you do with it?



ICS-FORTH

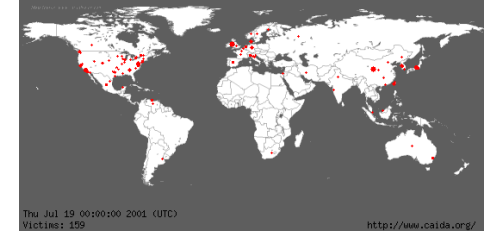


● Find cyberattacks

- Correlate data from different sensors
- if one sensor finds the worm all sensors are notified
- Find stealth (slowly-spread) worms
 - ✓ By aggregating data from different sensors
- Find worm outbreaks faster



LOBSTER SSA



ICS-FORTH

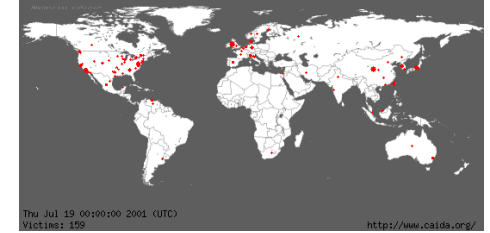


Information Society
Technologies

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



LOBSTER partners



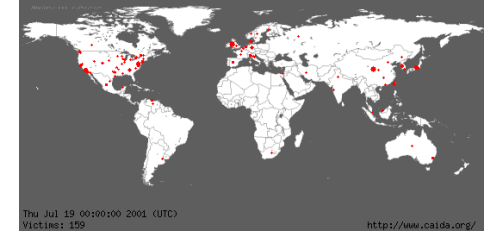
ICS-FORTH

- **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





How can you get involved



ICS-FORTH

- **Join our email list**

- lobster-news@ics.forth.gr

- Via

- <http://nemesis.ics.forth.gr/mailman/listinfo/lobster-news>

- **Talk to us**

- markatos@ics.forth.gr

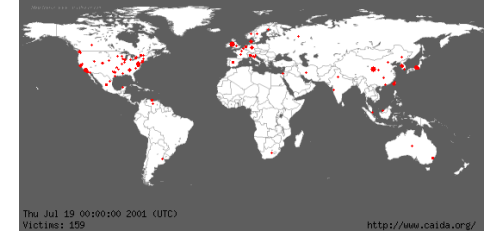
- **Join the infrastructure**

- expected to be operational on late 2005

LOBSTER – Evangelos Markatos markatos@ics.forth.gr



Summary



ICS-FORTH

- **Our understanding of the Internet continues to fade away**
- **LOBSTER will provide better monitoring**
 - based on
 - ✓ A network of passive monitoring sensors, and
 - ✓ State-of-the-art SCAMPI research
 - and by providing
 - ✓ Trusted operation in an un-trusted world
 - ✓ Common programming platform
 - ✓ Resilience to attackers
- **Join us! (lobster-news@ics.forth.gr)**

LOBSTER – Evangelos Markatos markatos@ics.forth.gr

A map of Europe with a network of nodes and lines overlaid, representing broadband internet infrastructure. The nodes are small white circles connected by thin grey lines, forming a complex web across the continent. The map is light green with white outlines for countries and water bodies.

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

Evangelos Markatos

markatos@ics.forth.gr

<http://www.ics.forth.gr/~markatos>

Institute of Computer Science (ICS)

**Foundation for Research and Technology – Hellas
(FORTH)**