Passive Network Traffic Monitoring: the SCAMPI and LOBSTER projects

http://www.ist-scampi.org http://www.ist-lobster.org

Evangelos Markatos, Ph.D.

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

Roadmap of the Talk

- Motivation
  - What is the problem?
    - Cyberattacks continue to plague our networks
- Solution
  - Better Internet traffic monitoring through the SCAMPI/LOBSTER
- Summary

What is the problem?

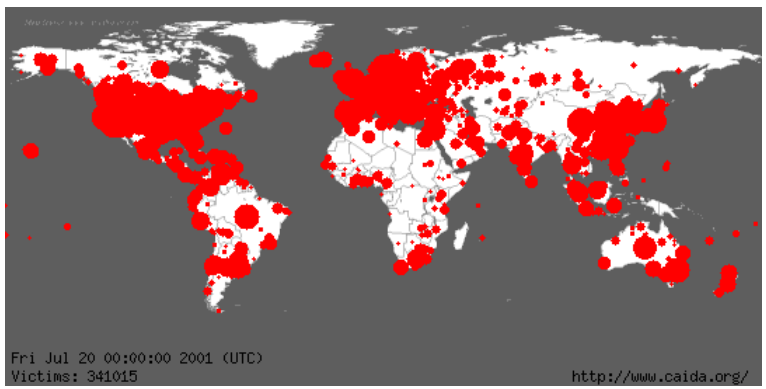
- Cyberattacks continue to plague our networks
  - Internet-based attacks
    - Viruses, worms, spyware, DoS/DDoS attacks
  - Attacks to our mobile phones
- We need to protect ourselves, our devices, and our cyber-infrastructure

What are the cyberattacks?

- Worms, Viruses, and trojians, continue to disrupt our everyday activities
- Spyware and backdoors continue to steal our credit card numbers, our passwords, and snoop into our private lives
- Keyboard loggers can empty our bank accounts if they choose to do so

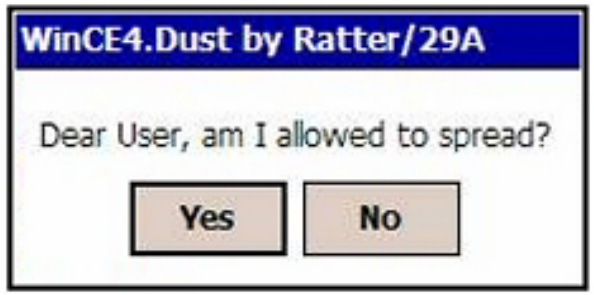
Some famous Internet worms

- 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



Cyberattacks in palmtops and mobile phones

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



Mobile phone viruses: The Mosquitos virus

- Mosquitos Virus:
  - Attaches itself to an illegal copy of “Mosquitos” game
  - Once installed it starts sending potentially expensive SMS messages to premium numbers
  - “free to download” but “expensive to play” ☺

How much does it cost?

- Worm outbreaks costs billions of euros to lost productivity
  - CodeRED Worm: $2.6 billion, Slammer: $1.2 billion
  - LoveLetter virus: $8.8 billion
- Worms have penetrated Nuclear Power plants.
  - *"The Slammer worm penetrated a private computer network at Ohio's Davis-Besse nuclear power plant in January and disabled a safety monitoring system for nearly five hours"*

    Security Focus News
- Potential Future Costs:
  - What if a medical equipment gets infected by a worm?
    - Wrong diagnosis? Wrong treatment?
  - What if my car gets infected by a worm?

Solution?

- To combat cyberattacks we need
  - Fast detection of the attacks
  - Accurate Fingerprinting of the attack mechanisms

- through better Network Traffic Monitoring
  - Faster
    - i.e. to detect and respond to worms BEFORE they infect the planet
  - More accurate

SCAMPI and LOBSTER: two steps for better Internet Monitoring

Information Society Technologies

http://www.ist-scampi.org http://www.ist-lobster.org

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

Evangelos Markatos, FORTH

SCAMPI

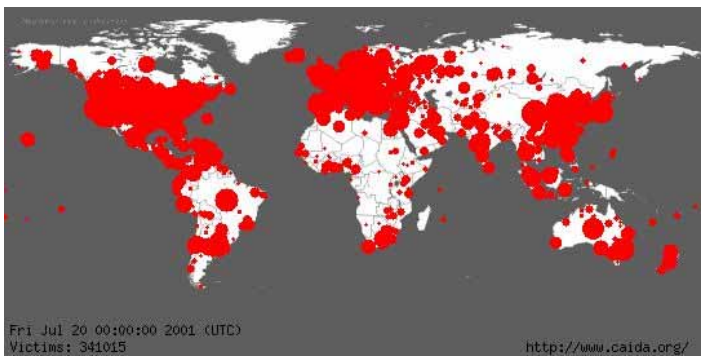
- SCAMPI is an IST project
- Funded by European Commission
- Duration: 1/4/02-31/3/05

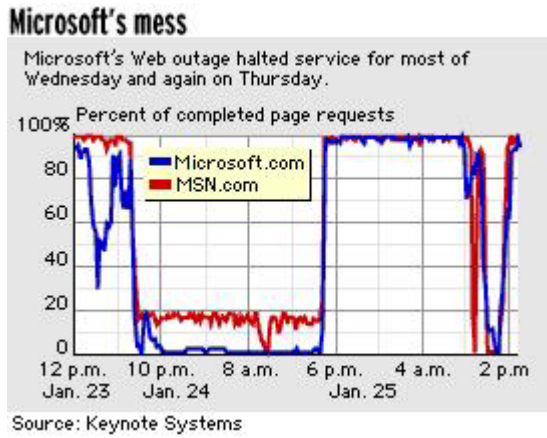
SCAMPI: What is it?

- SCAMPI develops a passive traffic monitoring platform
- Passive means:
  - capture all network traffic and examine it
  - Why?
    - To find cyberattackers/intruders/back-doors
- How does SCAMPI do it?
  - Develop a 10 Gbps FPGA-based monitoring sensor
  - Develop a Monitoring Application Programming Interface (MAPI)
  - Develop Monitoring Applications

SCAMPI: What is it good for?

- High-speed Intrusion Detection/Prevention:
  - 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
- DDOS attack detection





Evangelos Markatos, FORTH

SCAMPI: What are its benefits? (I)

- **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? (II)

- 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:

Faster monitoring applications

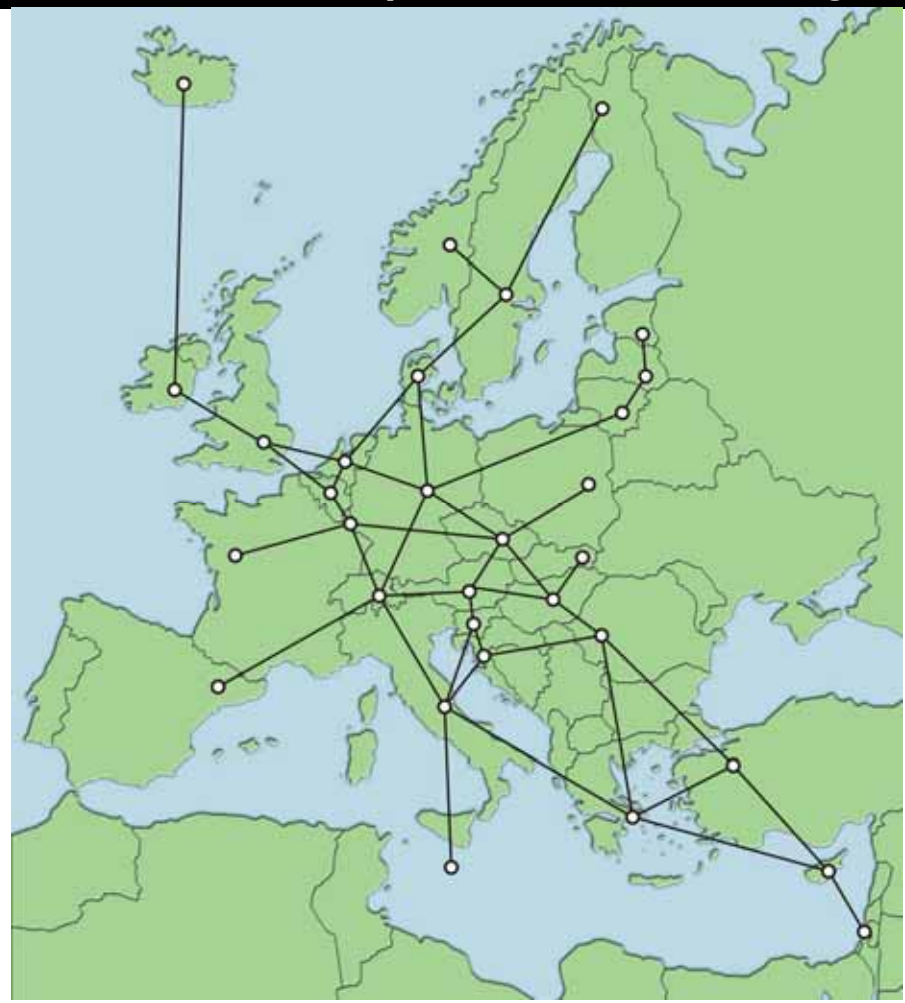
SCAMPI: What are its benefits? (III)

- **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 SSA

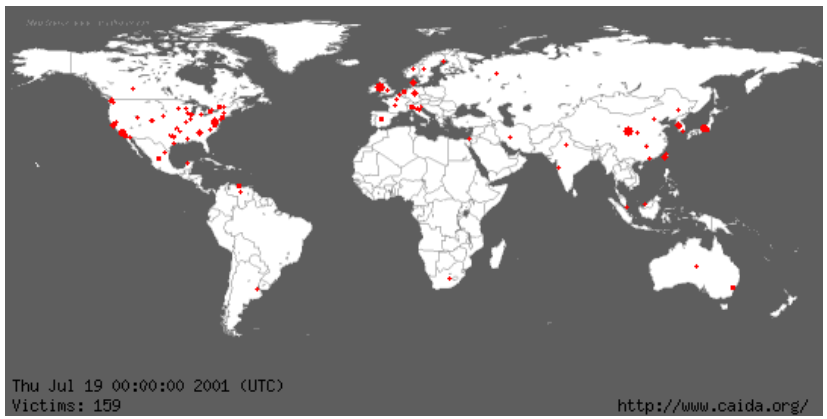
- LOBSTER is a
  - Specific Support Action
- Funded by European Commission
- Two-year project
  - Duration 1/10/05-31/12/06

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



Potential LOBSTER applications: Early-warning systems

- LOBSTER can contribute to an early-warning System
  - For automatic worm detection
  - Faster: i.e. before they manage to spread



Who can benefit from LOBSTER?

- NRNs/ISPs
  - Better Internet traffic monitoring of their networks
  - Better understanding of their interactions with other NRNs/ISPs
- Security Researchers
  - Access to anonymized security data
  - Access to anonymized security 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

Summary

- Cyberattacks cause significant damages
- We need to protect ourselves against cyberattacks
- SCAMPI/LOBSTER will provide improved security through better traffic monitoring
  - based on
    - A network of passive monitoring sensors, and
    - State-of-the-art passive monitoring research

Passive Network Monitoring: the SCAMPI and LOBSTER projects

http://www.ist-scampi.org http://www.ist-lobster.org

Evangelos Markatos, Ph.D.

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

Back up slides

What is the Root of the Problem?

- Worms are autonomous
- They do not need out help to multiply

- Let's try to understand worms
  - Self replicating programs which exploit a vulnerability (bug) of a server
  - They propagate as follows
    1. find a vulnerable (i.e. buggy) server
    2. trigger the bug in the server
    3. compromise the server
    4. replicate the worm to the server
    5. find another vulnerable server
    6. GOTO step 2.

The erosion of trust on the Internet

- We used to trust computers we interacted with on the Internet
  - Not any more…
    - Do you know that the web server http://www.microsoft.com is the one from Microsoft?
    - Are you willing to bet on it?
- We used to trust our network
  - Not any more…
    - Our network is the largest source of all attacks
- We used to trust our own computer
  - Not any more… (keyboard loggers can easily get your bank account number and password!)

LOBSTER partners

- 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

SCAMPI partners

- 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