LOBSTER: Large Scale Monitoring of Broadband Internet Infrastructure

Evangelos Markatos
The LOBSTER Consortium
http://www.ics.forth.gr/~markatos
Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Roadmap of the Talk

- **Motivation**
  - What is the problem?
  - Our understanding of the Internet needs to be improved

- **Solution**
  - Better Internet traffic monitoring through the LOBSTER infrastructure

- **How can you participate?**
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?

LOBSTER – Evangelos Markatos markatos@ics.forth.gr
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?

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
Why do Cyberattacks continue to plague Internet? II

- Cyberattack
  - Detection, identification, response/deployment
    - May take several hours
  - i.e. 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?
Why do Cyberattacks continue to plague Internet? III

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

LOBSTER – Evangelos Markatos markatos@ics.forth.gr
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?
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

LOBSTER – Evangelos Markatos markatos@ics.forth.gr
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 major Internet servers

- What is going on out there?

LOBSTER – Evangelos Markatos markatos@ics.forth.gr
Win 2K and Win XP computers

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

LOBSTER – Evangelos Markatos markatos@ics.forth.gr
So, what do these all mean?

- 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
The GAP continues to widen with time...

LOBSTER – Evangelos Markatos markatos@ics.forth.gr
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
A solution should be based on two principles:

- **Distributed Collaboration**
  - among traffic monitoring sensors
  - an infrastructure of traffic monitors

- **State-of-the-art Research**
  - In passive network traffic monitoring
    - The SCAMPI monitoring system
SCAMPI: High-Performance Network traffic Monitoring

- **Passive Network Traffic Monitoring**
  - For high-speed networks

- **High-performance programmable**
  - (FPGA-based) monitoring card

- **Flexible programming environment**
  - Monitoring Application Programming Interface (MAPI)

- **Highly effective**
  - Intrusion Detection Algorithms, and
  - System Architectures (IDSEs, IPSes)

LOBSTER – Evangelos Markatos markatos@ics.forth.gr
The LOBSTER infrastructure

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

LOBSTER – Evangelos Markatos markatos@ics.forth.gr
LOBSTER is a

- Specific Support Action

Funded by European Commission

Two-year project

- Duration 1/1/05-31/12/06
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
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
Need a Common Programming Environment

- Use DiMAPI (Distributed Monitoring Application Programming Interface)
- MAPI developed within the SCAMPI project
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**
- **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
**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?

- **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
How can you get involved

- **Join our email list**
  - [lobster-news@ics.forth.gr](mailto:lobster-news@ics.forth.gr)
  - Email to
    - [lobster-news-request@ics.forth.gr](mailto:lobster-news-request@ics.forth.gr)
    - Subject: subscribe

- **Join the infrastructure**
  - expected to be operational on late 2005
Summary

- **Our understanding of the Internet**
  - needs to be improved

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

- **Join us!** ([lobster-news-request@ics.forth.gr](mailto:lobster-news-request@ics.forth.gr))

  LOBSTER – Evangelos Markatos markatos@ics.forth.gr
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)