

LOBSTER: Overview



An IST Proposal

LOBSTER: Large Scale Monitoring for Broadband Internet Infrastructure

Herbert Bos*

herbertb@cs.vu.nl

<http://www.cs.vu.nl/~herbertb>

Department of Computer Science
Vrije Universiteit Amsterdam

* slides adapted from an earlier version by Evangelos Markatos –ICS Forth

Roadmap of the Talk



Information Society
Technologies

An IST Proposal

- Objective
- Motivation
- State-of-the-art
- Challenges



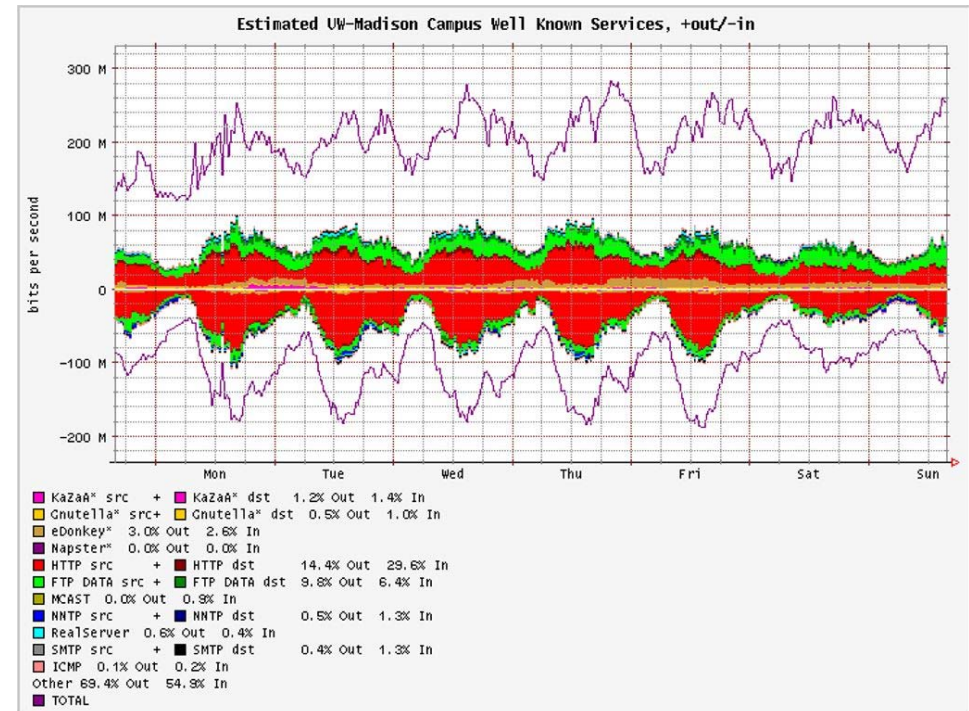
Objective

**To develop an
advanced European Infrastructure
for
Network Traffic Monitoring**

Why?



- We have a poor understanding of several aspects the Internet such as
 - Traffic characterization:
 - What % of the traffic goes to KaZaa?
 - Difficult to answer because the available tools work mostly for applications that use static ports, while KaZaa uses dynamic ports
 - Security – early warning systems
 - Are there any new worms on the loose?
 - Can we automatically identify them before they spread?

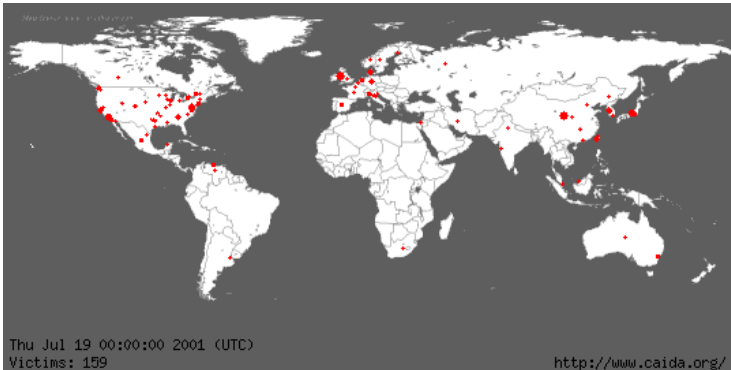


Why Do We Need It? More Security

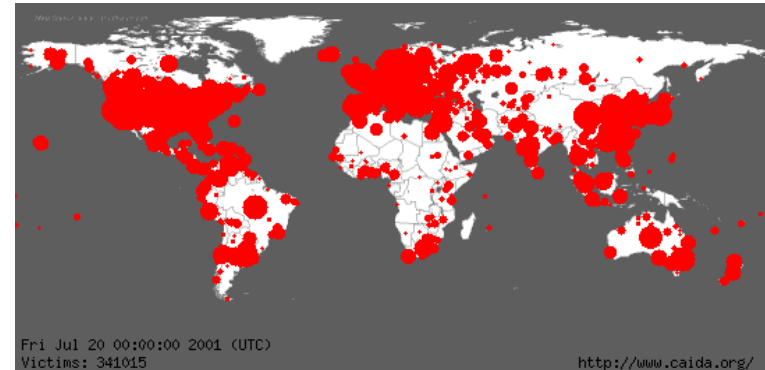


Information Society
Technologies

An IST Proposal



On Jul 19, 2001, 00:00



24 hours later...

350,000 infected computers

The expansion of CODE-RED

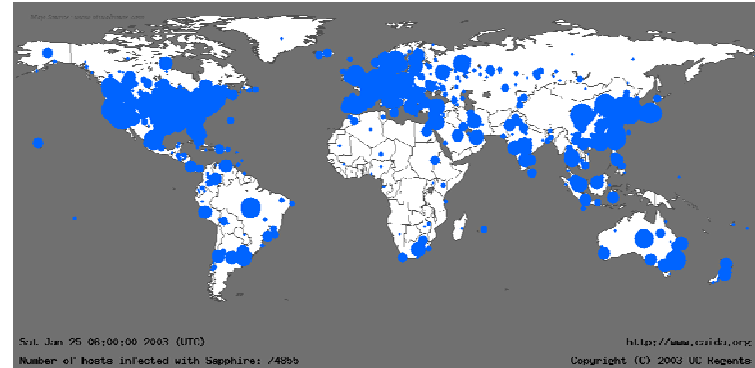
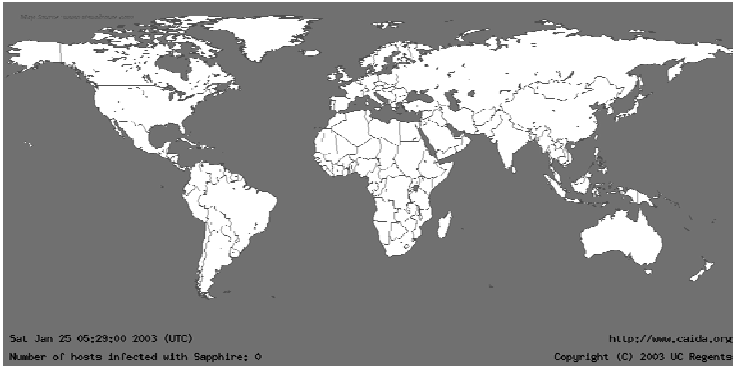
- Safety
 - Intrusion Detection
 - DoS attack detection
 - Worms
- Security vulnerabilities
 - Poorly administered home computers
 - Widespread use of p2p systems
 - worms/viruses/cyberattacks

Why Do We Need It? More Security



Information Society
Technologies

An IST Proposal



The expansion of SAPHIRE WORM

On Jan 25, 2003, 05:29

30 minutes later...74,000 victims
doubled every 8.5 seconds
even in Greenland...

- Safety
 - Intrusion Detection
 - DoS attack detection
 - Worms
- Security vulnerabilities
 - Poorly administered home computers
 - Widespread use of p2p systems
 - worms/viruses/cyberattacks

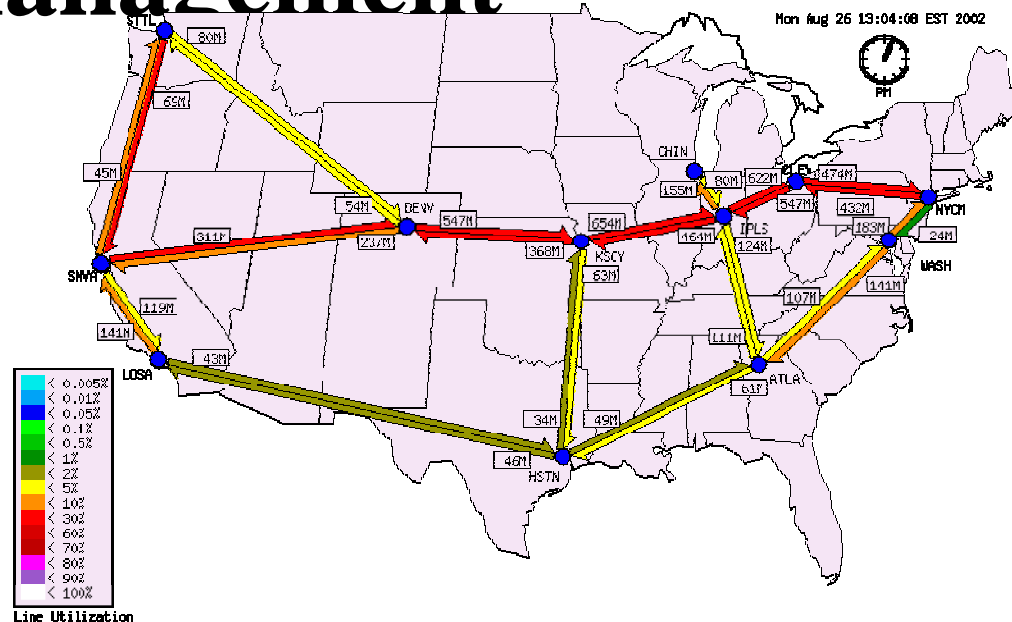
Why Do We Need It? More Security

- Denial-of-Service attacks
 - sometime happen accidentally
 - “combination of Microsoft software features and misconfigurations was essentially causing a slowly-paced massive distributed denial of service (DDoS) attack on the root name server system”

kc Claffy

Why Do We Need It? Performance – Billing - Management

An IST Proposal



- **User:** Why is my application so slow?
 - Who is to blame? Local LAN? Remote LAN? WAN?
- **Administrator:** which applications consume most of the traffic in my network?
- **Web master:** What is the latency of my web server as perceived by my clients?

Why Is It Difficult?

An IST Proposal

- It is a **moving** target
- It is not your father's Internet
- Network Monitoring tools were developed mostly
 - for slow networks
 - Mbps (not Gbps)
 - for traffic engineering/QoS
 - not all packets needed
 - sampling is fine
 - no payload inspection



What is the state-of-the-art?

- **Flow-level statistics: Netflow, IPFIX, ...**
 - Provide traffic summary
 - Not easy for intrusion detection, security, p2p traffic
- **Active Measurements provide good metrics:**
 - One-way latency, bandwidth, error rate, etc.
 - Not easy for traffic characterization/billing, security applications
- **Passive traffic collection at NLANR**
 - Mostly used for off-line analysis
 - Not clear whether it focuses on real-time security-related problems

What is our proposal?

European Infrastructure of network traffic monitors

- Based on Passive monitoring:
 - Collect all data (headers, payloads, timestamps)
- These monitors are appropriate for most monitoring applications, such as:
 - Traffic characterization:
 - What % of my traffic goes to KaZaa?
 - Security - early warning systems
 - Identify when a new worm starts to spread

What are we going to do with it?

- Real-time applications
 - Traffic characterization
 - Early-warning systems
 - Worm spread and containment
- Off-line processing
 - Gathering of packet traces
 - Processing of the traces to identify
 - Trends, security breaches, internet models, etc.
- ...

Challenges I

- Privacy: protect the privacy of the end user while being able to extract useful information from the traces
 - Anonymize the packets on the monitoring card:
 - In hardware (co-processor/FPGA)
 - Driven by user policies
 - Users define which data will be anonymized using
 - » SiSaL: Scripting Sanitization Language

Challenges II

- Speed:
 - We can probably do it at 2.5 Gbps
 - Can we do it at 10Gbps?
 - 40 Gbps? 100 Gbps?
 - Need to use special-purpose cards:
 - SCAMPI monitoring adapter
 - Co-processor-based cards from Endace

LOBSTER: Overview



An IST Proposal

LOBSTER: Large Scale Monitoring for Broadband Internet Infrastructure

Herbert Bos

herbertb@cs.vu.nl

<http://www.cs.vu.nl/~herbertb>

Department of Computer Science
Vrije Universiteit Amsterdam