SCAMPI: Scientific Approach and Research Directions

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

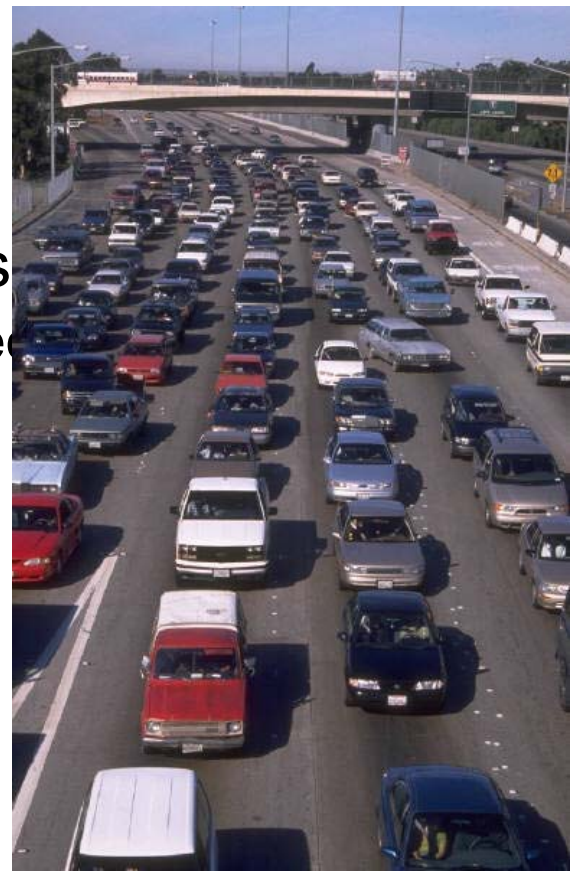
- **What is network monitoring?**
- **Why do we need it?**
- **Why is it difficult?**
- **What are we going to do about it?**
  - Research Directions

The Context: Network Monitoring

SCAMPI

ICS-FORTH

- **What is it?**
- **Network Traffic Inspection**
  - Identify performance characteristics
    - ✓ packets/sec, bytes/sec, connections/sec
      - For traffic engineering
    - ✓ QoS metrics, latency, bandwidth
      - For SLA enforcement
    - ✓ busiest applications/clients/servers
  - Security
    - ✓ Unauthorized applications running
      - Peer-to-peer, instant messaging
    - ✓ Cyberattacks



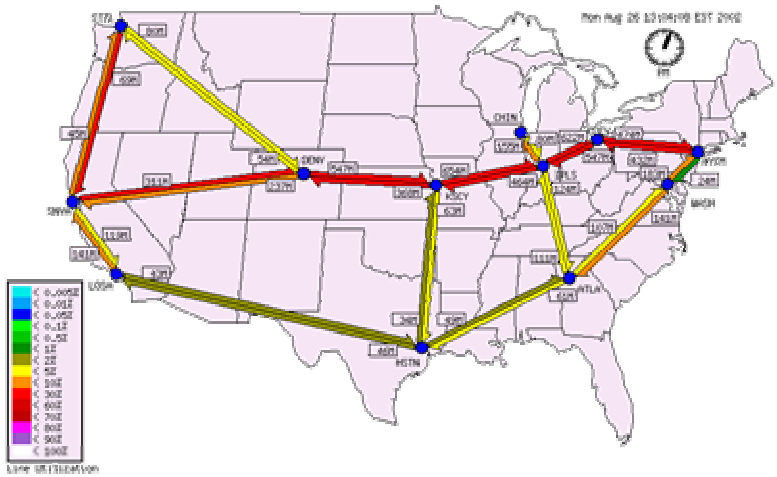
Evangelos Markatos, markatos@ics.forth.gr

SCAMPI

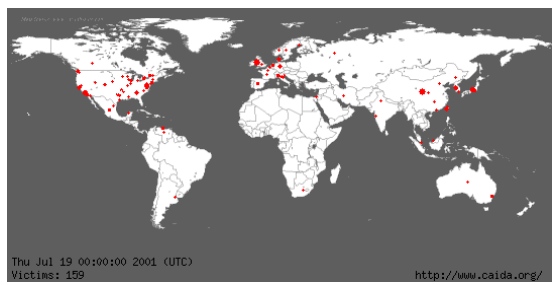
ICS-FORTH

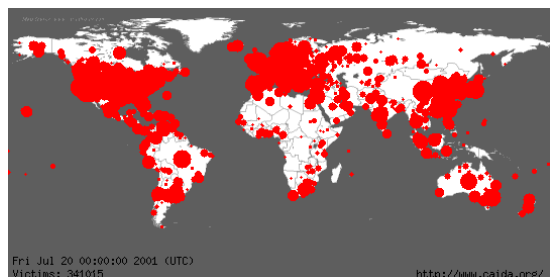
Why Do We Need It?

- **Performance - QoS**
  - Traffic Engineering
  - SLA enforcement



- **Safety**
  - Intrusion Detection
  - DoS attack detection
  - Cyber attacks





SCAMPI

ICS-FORTH

Why Is It Difficult?

- **It is a moving target**
- **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

Why Is It Difficult?

- **It is time-consuming**
  - As networks get faster
    - ✓ Monitoring gets slower…
  - As more cyber-attacks are being launched
    - ✓ Monitoring gets slower
  - As hackers get more clever
    - ✓ cyberattacks get more complex
      - monitoring gets more complicated
        - and slower…

What are we going to do about it?

- **Let users express themselves**
  - What exactly do they need to monitor?
  - Why?
- **Push functionality to lower levels**
  - from user mode
  - to kernel mode
  - even to the hardware
- **Define Better Algorithms**

Let users express themselves

ICS-FORTH

- **The more information the system has about a user's monitoring needs**
  - The better it can implement them
- **Define Monitoring API (MAPI)**
- **Provides first-class abstractions:**
  - The network flow
    - ✓ A set of packets that satisfy some condition
      - e.g every 10th packet of my web traffic
      - e.g. all email messages with "hack.exe" attachment
    - ✓ Define functions on flows:
      - e.g. Don't give me the packets themselves, just their number

Let users express themselves: MAPI

- **Network Flows:**
  - BPF – LSF – with functions
- **Hierarchical Flows**
  - sub-flows: defined by a unique quad:
    - ✓ SRC/DST IP-address/port
    - ✓ System does not keep packets
      - – Only general statistics
- **Active Measurement Flows**
  - For active monitoring
  - One-way delay/bandwidth measurements
  - SLA enforcement applications

Evangelos Markatos, markatos@ics.forth.gr

Push functionality to lower levels

- **From user to kernel**
  - Execute functions in kernel mode
    - ✓Filtering:
      - Sampling, Hashing, String searching
  - Safe execution (OKE)
- **From kernel to hardware**
  - Filtering
    - ✓In “smart” routers
    - ✓In programmable network adapters
      - FPGAs, CAMs, network processors, ….

SCAMPI

ICS-FORTH

Define better algorithms

- **For time consuming tasks like:**
  - Packet classification
  - Payload inspection
    - ✓Pattern/String matching
      - Consumes up to 80% in modern IDS

Summary

ICS-FORTH

- **SCAMPI targets**
  - Network monitoring at Gbps speeds

by

- **Improving expressing ability**
- **Pushing functionality to lower layers**
- **Define better algorithms**
  - For time-consuming tasks

The rest of the SCAMPI talks

- **Network monitoring and QoS**
  - *Steven Van den Berghe, IMEC*
- **Safe multiprogramming: The OKE model**
  - Herbert Bos, LLIACS
- **Network Monitoring at Gbps**
  - Luca Deri, NETikos

SCAMPI: Scientific Approach and Research Directions

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

Evangelos Markatos

markatos@ics.forth.gr

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

Institute of Computer Science (ICS)

Foundation for Research and Technology – Hellas (FORTH)