MOSES:
Monitoring and Security in the Era of GRIDs

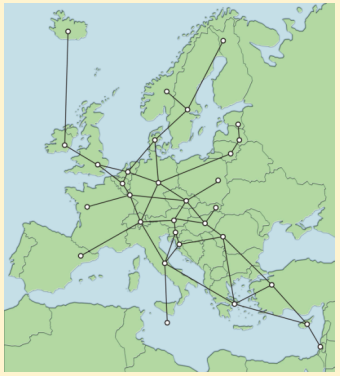
Kostas G. Anagnostakis

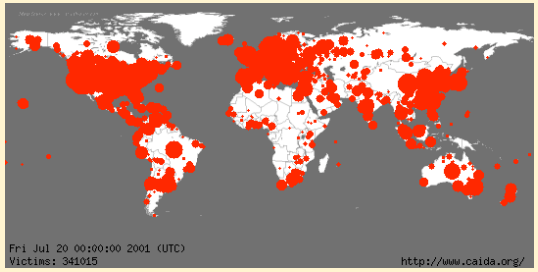
Institute of Computer Science (ICS)

Foundation for Research & Technology, Hellas (FORTH)

Background

- SCAMPI: IST-funded R&D project (2002-2005)
  - Developed a scalable monitoring platform for the Internet 10Gbit/s network monitoring card, Monitoring API, and security applications
- LOBSTER: Specific Support Action (2004-2006)
  - Rolling out a distributed monitoring infrastructure
  - Focus: security, detection of large-scale attacks
- NoAH: Specific Support Action (2005-2007)
  - Develop & roll out a distributed honeypot infrastructure
  - Honeypot tech complements passive monitoring





Motivation: opportunities & threats

- The infrastructure needed for building security services for detecting cyberattacks is a large-scale distributed system
  - Involves data sensors, processing resources and storage
  - Very similar to a GRID, but developed independently

  Can we benefit from GRID technology and existing GRID infrastructure for building better security services?

- GRIDs, being large-scale distributed systems, create new threats for large-scale distributed attacks
  - Existing GRID sec. model deals primarily with access control
  - New threats: DDoS, abuse, password/key cracking, …

  Can we benefit from security/monitoring technology for building safer GRID infrastructures?

MOSES: key objectives

- Develop the technology needed for efficiently implementing security monitoring services on GRID platforms

- Develop a distributed monitoring system and the detection technology needed to prevent abuse of GRID resources

Example #1: Shadow honepots on the GRID

- One of the biggest problems in detecting unknown (zero-day) attacks is false positives
  - Detection heuristics often flag legitimate traffic as suspect
  - Result is loss of confidence in detection ("cry wolf")
- We have recently developed a solution to this problem using "shadow honepots" (paper at Usenix Sec'05)
  - Basic idea is to add a second filter after detection, by replaying suspect traffic in a "clean room testing" environment
  - Result is zero false positives, but the cost is potentially huge
- *Opportunity: run shadow honeypot services on the GRID*

Example #2: Attack signature validation

- Once an attack becomes known, we need a signature so that end-systems/firewalls/IDSes can block the attack
  - Attack descriptions are often inexact, resulting in false positives
  - Network admins often reluctant to install new signatures
  - But really no time to think: worms can spread in minutes
- We need a signature validation service to rapidly test signature accuracy on historical traffic data
  - Help signature developers, provide assurance to network admins
  - Hard to do locally: need to test signature against TBytes of traffic
- *Opportunity: distributed signature validation on the GRID*

Next steps (short-term)

- Team up with EU & Asian partners
  - Background in GRID R&D, security R&D, or both
- Carve out a subset of important problems
  - GRID-security space is huge, so focus is the key
- Submit proposal
  - ideally (but not necessarily) in September'05

For more information and to express interest, email *kanag@ics.forth.gr*