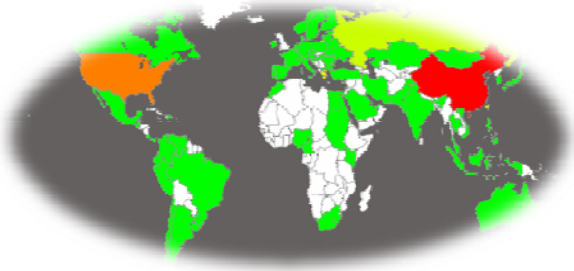
Collaboration in Systems Security

Evangelos Markatos
FORTH-ICS

The problem

- Network Security is an International Problem
  - Compromised Computers are all over the world
  - Attacks originate from every continent
    - from almost every state
  - Network (in)security does not stop at state boundaries



Geo distribution of traffic received by honeypots (source: the NoAH project)

The solution: We need to collaborate

- Why?
  - Different organizations experience different kinds of attacks
  - Different sensors see different data
  - Different environments see different attacks
    - Academia, Commercial ISPs,
    - Industrial systems, banks, etc.

We need to collaborate: How?

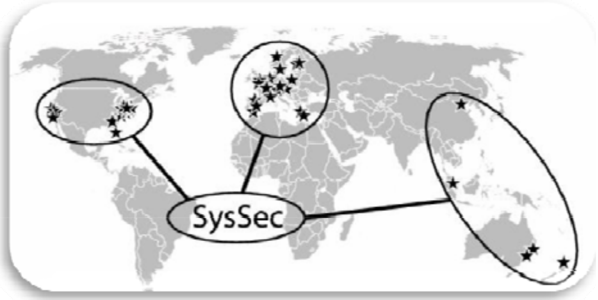
- Share data
  - SPAM repositories, malware, attack vectors
    - The more the merrier
  - Confirm hypotheses
    - has anyone else seen increased traffic in port XYZ?

We need to collaborate: How?

- Exchange People
  - Encourage student/researcher exchanges
    - Provide funding for short visits (e.g. 3-4 months)
    - Internships (e.g. from Europe to US and vice versa)
      - – Focus on collaborative papers
    - Frequent “Calls for internships” proposals - rapid evaluation cycles
- Integrate international communities
  - Provide more funding for common projects
  - Organize competitions – fun activities
    - e.g. “capture the flag” contests

SysSec: a new Network of Excellence

- SysSec proposes a *game-changing* approach to cybersecurity:
  - Currently Researchers are mostly reactive:
    - they usually track cyberattackers *after* an attack has been launched
    - thus, researchers are always one step behind attackers
  - SysSec aims to break this vicious cycle
  - Researchers should become more *proactive*:
    - Anticipate attacks and vulnerabilities
    - Predict and prepare for future threats
    - Work on defenses *before* attacks materialize.



SysSec: Goals

- Create a **virtual distributed Center of Excellence** in the area of emerging threats and vulnerabilities.
  - By forming a critical mass of European Researchers and by aligning their activities,
  - Have the gravitas needed to play a **leading role internationally**, empowered to undertake large-scale, ambitious and high-impact research efforts.
- Create a **Center of Academic Excellence** in the area
  - create an education and training program targeting young researchers and the industry.
  - lay the foundations for a common graduate degree in the area with emphasis on Systems Security.

SysSec: How can you collaborate

- Contribute to the research agenda
  - Provide feedback on emerging threats
  - Share your ideas on future security issues
- Contribute to our “systems security” University curriculum
  - Contribute homeworks/exams
  - Contribute/use lab exercises
  - Teach some of the courses at your University
  - Share some of your course material

Collaboration in Systems Security

Evangelos Markatos
FORTH-ICS