Evangelos Markatos, Ph.D.
Associate Professor

Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Crete, Greece
Roadmap of the Talk

NoAH: A Network of Affined Honeypots

• Steps of this talk
  – An idea for a proposal
  – Gather the consortium
  – Write the proposal
  – Wait for the results
  – Negotiate

Evangelos Markatos, FORTH
Step 1: The NoAH Idea

NoAH: A Network of Affined Honeypots

- **Cyberattacks** continue to plague the Internet
  - Viruses – email attachments
  - Worms: self-replicating programs
  - Keyboard loggers:
    - They record every key punch
    - They steal bank accounts, passwords, credit card numbers
- **The problem is much larger than any single organization can solve**

Evangelos Markatos, FORTH
Step 1: The NoAH Idea

NoAH: A Network of Affined Honeypots

- We need a distributed Infrastructure of honeypots to help us solve the problem
- Honeypots are “undercover” computers that do nothing
  - they wait to be attacked
- Attackers are attacked to the “honey”
  - Easily compromised computers
- Once attacked they start gathering information
  - about the attacker’s methods and motives

Evangelos Markatos, FORTH
Step 2: Assemble the Consortium

NoAH: A Network of Affined Honeypots

- We selected hard working Partners who really cared about NoAH
- 8 partners in total from 5 countries
- 5 partners have been collaborators in previous EU projects (FORTH, TERENA, VU, FORTHnet, ALCATEL)
- One of them was a collaborator in national projects (Virtual Trip)
- Two were new partners (ETHZ, DFN-CERT)
- All of them are leaders in their field of work

Evangelos Markatos, FORTH
Step 3: Write the proposal (I): The people

NoAH: A Network of Affined Honeypots

• The writing team: 9-11 people
  – Two major writers
    • Which wrote most of the text
  – Seven-Nine additional writers
    • Who wrote small parts of the proposal

Evangelos Markatos, FORTH
Goal: Enable Parallel Writing of the Proposal by geographically distributed people

– **LaTeX**:  
  • Each section of the proposal can be a different file  
  • Enables parallel writing of different sections

– **CVS**: resource control tool: enables people to  
  • checkout the most recent version of the proposal  
  • check in their changes  
  • from anywhere on the Internet

– **Excel**: for the financial tables  
  • **Excel2latex** converter to include the tables in LaTeX

– **Xfig**: for the Gantt chart

– **Dia**: for the Pert Diagram

Evangelos Markatos, FORTH
Writing of the proposal (II): the mechanisms

NoAH: A Network of Affined Honeypots

- Five day retreat (in Egypt):
  - Took five days off in a Hotel to write the major draft of the proposal
  - Good coffee, Good food
  - No Telephones – No Internet – No Interruptions
  - We were living, breathing, thinking, and sleeping of NoAH
    - Ohh, by the way we saw the pyramids as well
- Last week writing spree
  - 5 people were available every day (and most of the night) to write text, prepare figures, search the literature, etc.

Evangelos Markatos, FORTH
How much did it cost?

- Man power (for the coordinator)
  - 2 person-months of full-time work
    - Proposal writing and coordination
  - 2 person-weeks of administrative work
    - to coordinate the filling-up of the forms
- Travel
  - One trip to Amsterdam
- Email
  - 500 send/received email messages
  - as many as 20 messages in a single day

Evangelos Markatos, FORTH
NoAH: A Network of Affined Honeypots

Schedule

• 25/12/03 Wrote pre-proposal
• 30/12/03 Invitations to partners
• 26/1/04 Secured support of key US player
• 6/2/04 First Proposal Draft Circulated
• 10/2/04 Consortium Meeting in AMS
• 18/2/04 Egypt retreat for proposal writing
• 29/2-3/3/04 Assembled a party of five who
  – wrote text, prepared figures, searched literature
  – and made the final version of the proposal
• 4/3/04 NoAH submitted

Evangelos Markatos, FORTH
Then, what?

NoAH: A Network of Affined Honeypots

• Wait..........
• until 11/06 when we received a positive evaluation
• July 28th we were invited for negotiations
The Negotiations

NoAH: A Network of Affined Honeypots

- Prepare the Technical Annex
  - Reformatting
  - Addressing the reviewers comments
  - Incorporate a 25% budget reduction
- Meeting in Brussels
- Prepare second version of the TA
- Finish the negotiations

Evangelos Markatos, FORTH
How much did the negotiations it cost?

NoAH: A Network of Affined Honeypots

• Man power:
  – 3 person weeks of writing/negotiating
  – 2 person weeks of administrative work

• Travel
  – One trip to Brussels

Evangelos Markatos, FORTH
Was it worth it?

NoAH: A Network of Affined Honeypots

• Was it worth the time?
  – Every minute of it! It was fun!
• Was it worth the money?
  – Every cent of it!
• Would I do it again?
  – Absolutely!

Evangelos Markatos, FORTH
Evangelos Markatos, Ph.D.
Associate Professor

Institute of Computer Science (ICS)
Foundation for Research and Technology – Hellas (FORTH)
Crete, Greece