NoAH: A European Infrastructure for Cyberattack Detection

dr. Catalin Meirosu
TERENA
on behalf of the NoAH project

Special acknowledgements:
Evangelos Markatos, Asia Slowinska, Klaus Moeller, Jan Kohlrausch, Spiros Antonatos

Outline

- Motivation
- The NoAH difference
- Generic architecture
- The NoAH Components
- Argos
- honey@home

Motivation

- Worms, viruses and trojans – common occurrences in our daily interaction with computers
- Zero-day exploits used for installing various malware
- Selective attacks
- Traditional approaches
  - too slow
  - too inaccurate
  - looking for *known* malware

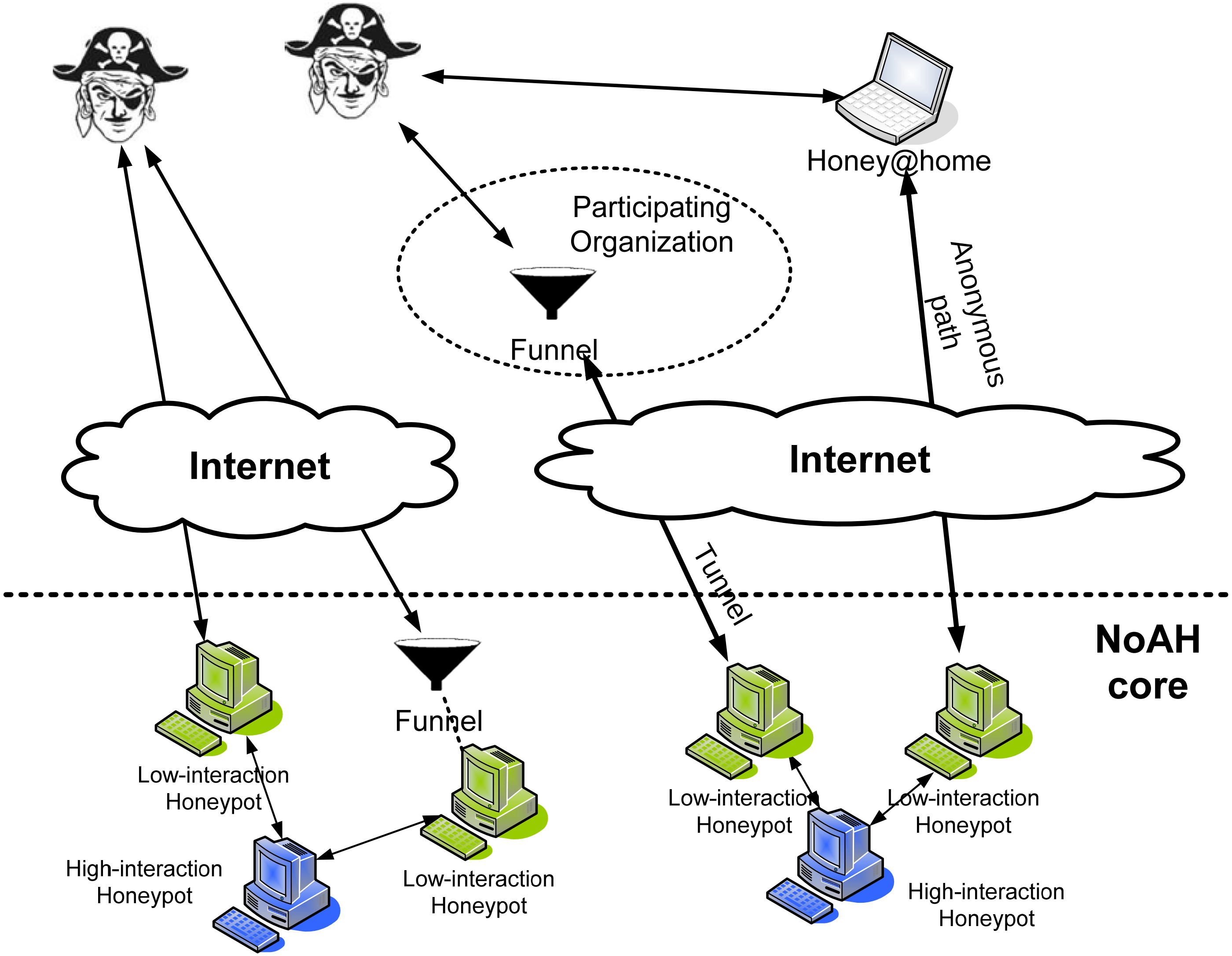
NoAH

- Network of Affined Honeypots (NoAH)
- A pilot project, funded in part under the EU 6th Framework Programme in the Research Infrastructures track
- Timeframe: April 1st, 2005 – March 31st 2008
- Partners: ICS-FORTH (coordinator), Vrije Universiteit Amsterdam, ETH Zurich, DFN-CERT, Alcatel-Lucent Research, FORTHnet, Virtual Trip Ltd, TERENA

NoAH’s electronic ark

- Goals:
  - Detect zero-day attacks and worms
  - Track down selective attacks
  - Analysis of unknown exploit code
  - Generate signatures
- Reach the goals by *building* a pilot infrastructure that allows for malware *collection, identification and analysis*
  - Based on an innovative combination of low interaction and high interaction honeypots and dark traffic redirectors

Generic architecture



Slide from [1]

Low-interaction honeypots and funnels

- Low interaction honeypots
  - For example, honeyd
  - Proxy for connections to high-interaction honeypots
  - Scalable
- Funnel component
  - Based on farpd (or router configuration)
  - Allows a wide dark address space to be handled by few honeypots
  - Aggregates and forwards traffic to the NoAH core
  - Scalable – tested with /24, /16 and /8 ranges

honey@home – basics

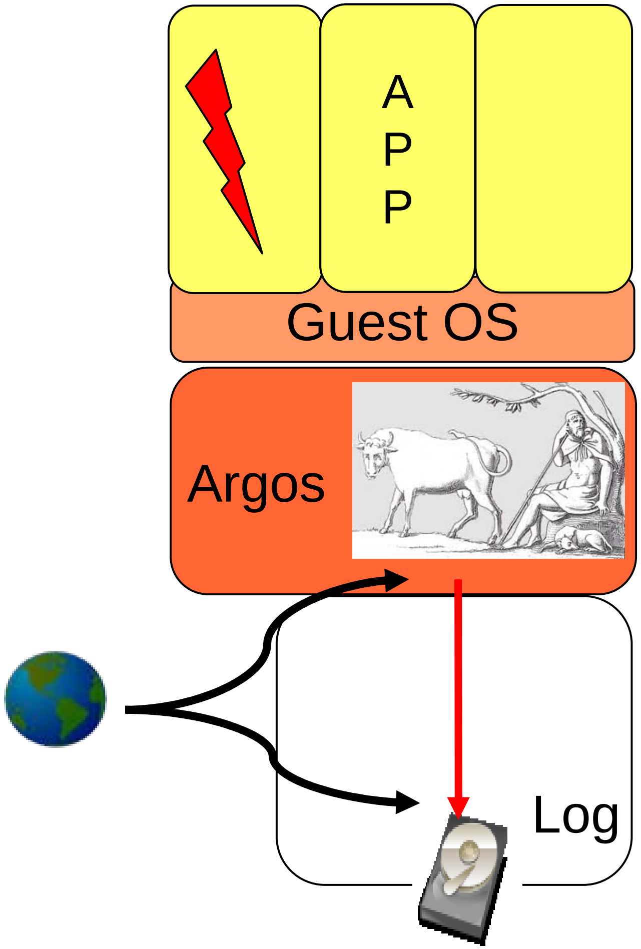
- Targeted towards home users and SOHO
- WinXP (under test) and Linux (under development) implementation
- Redirects traffic from unused IP addresses or ports to the NoAH core
- Easy to install
- http://www.honeyathome.org

honey@home - challenges

- We cannot trust the honey@home clients
  - Connection to the core via TOR (anonymous onion routing)
  - Client established himself as first router on the path (disables correlation attacks)
- DDoS against NoAH using honey@home
  - Disabling automatic download and installation of honey@home software by using animated CAPTCHAs
  - Enhanced CAPTCHAs prevent brute-force and “sweatshop” attacks

Argos

- Used as a high-interaction honeypot
- An emulator, based on Qemu
  - advantage: protects multiple OSes and applications, without modification
  - http://www.few.vu.nl/argos
- Employs “dynamic taint analysis”
  - tracks program execution and emphasises on data received from the network
  - detects attacks that divert conventional control flow (buffer overflows, etc)
  - when an attack is detected, it saves all the “tainted” memory data for further analysis and possibly signature generation



Adapted from [2]

Conclusion

- The NoAH projects builds a pilot infrastructure for cyberattack detection and analysis
- Main components
  - Argos, employed as a high-interaction honeypot
  - honey@home, a dark traffic redirector for SOHO
  - Funnels, for cooperating institutions

References

1. Introduction to NoAH: a European Network of Affined Honeypots*Evangelos Markatos, FORTH* [slides]
2. The NoAH approach to zeroday worm detection - *Asia Slowinska, 19th TF-CSIRT Meeting, Espoo, 22 Sep '06.*
3. NoAH Honeynet Project - *Klaus Moeller, 17th TF-CSIRT Meeting, Amsterdam, 24 Jan '06.*
4. Practical Experiences with the deployment of honeypots*Jan Kohlrausch, DFN-CERT* [slides]
5. E. Athanasopoulos and S. Antonatos; *Enhanced CAPTCHAs: Using Animation to Tell Humans and Computers Apart*, Proceedings of CMS'06, Heraklion, Greece, October 2006. [PDF]
6. More articles: http://www.fp6-noah.org/publications/