Project Partners

The NoAH project involves eight partners from the academic, research and commercial sectors and represents a total investment of almost 2.5 million euro, 60% of which is funded by the Research Infrastructures Programme of the European Union (contract no. RIDS-011923).

The project started on 1 April 2005 and will run until 31 March 2008. The project is coordinated by the Foundation for Research and Technology - Hellas (FORTH).

Alcatel·Lucent
www.alcatel-lucent.com

DFN-CERT Services GmbH
www.cert.dfn.de

vrije Universiteit
www.vu.nl

VIRTUAL TRIP Ltd
Internet Technologies
www.vtrip.net

forthnet
www.forthnet.gr

SIXTH FRAMEWORK PROGRAMME

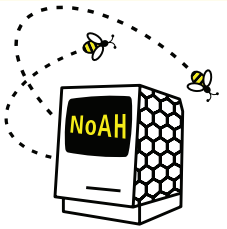
www.ics.forth.gr

ETH
Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich
www.ethz.ch

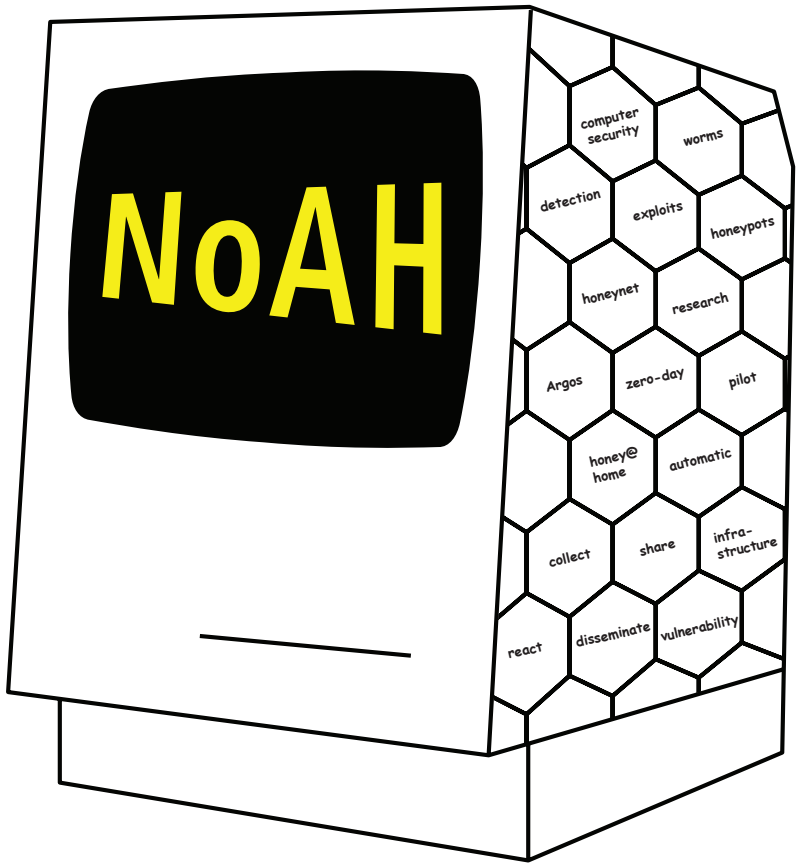
TERENA
www.terena.org

Participation in the NoAH network is open to everybody. To participate, download and install the honey@home software from **www.honeyathome.org**

For more information, visit the NoAH website: **www.fp6-noah.org** and subscribe to the NoAH mailing list: **info@fp6-noah.org**



http://www.fp6-noah.org



A design study for a distributed infrastructure to perform zero-day detection of cyberattacks

What is a honeypot?

A honeypot is an Internet-connected server that appears vulnerable to cyberattacks. A monitoring system will observe the activity of the attacker and restrict the access to only a limited set of the server's resources. Many break-in attempts are carried out nowadays by automated programs trying to exploit the known or not-yet-known vulnerabilities of software. Honeypots can be used as sensors to detect, monitor and automatically report on such activities.

NoAH Project Objectives

Viruses, worms and Trojans have grown more intelligent in trying to exploit vulnerabilities in applications and operating systems. Large amounts of bandwidth are filled with unwanted traffic that is only spreading malware. Networks can be taken over in minutes and distributed denial-of-service attacks may bring legitimate traffic to a halt faster than human network operators could react. The only way to stop such threats would be to employ an automated system that detects and contains the attacks in real time.

NoAH advances the state of the art in this domain by working towards the following objectives:

- Design a geographically dispersed network of honeypots to detect and correlate data on cyberattacks.
- Develop techniques for the automatic identification of attacks and investigate mechanisms to distribute attack identification information to firewalls and other containment systems.
- Install and operate a pilot honeypot infrastructure to demonstrate the usefulness and effectiveness of the NoAH approach.
- Collect information on cyberattacks to examine trends, refine security models and support Internet-related research efforts in general.
- Disseminate the results of the project, including open-source software and anonymised traffic data to operators of National Research and Education Networks, Internet Service Providers, Computer Security and Incident Response Teams and network security analysts.

Publications of the NoAH project can be found at:
http://www.fp6-noah.org/publications/

Argos

Argos is a secure system emulator designed for use in honeypots. It encapsulates the honeypot environment in a safe software enclosure that allows automated monitoring and tracking of cyberattack activity inside the honeypot. Argos examines step-by-step the execution of software. It detects any attempts made to alter the sequence of instructions as a sign of malicious use. This is done by using a technique know as "dynamic taint analysis" that identifies illegal and potentially unsafe data that has arrived from the network.

When such an attack is detected, the potentially unsafe data within the memory footprint of the applications running inside the emulator is saved and the emulator terminates its execution. This data together with a record of the network traffic received by the emulator is used for off-line analysis and characterisation of the attack.

Argos is installed by the partners of the NoAH project as part of the core honeypot infrastructure.

honey@home

Honey@home is a Windows® application which runs on a regular PC connected to the Internet. The role of honey@home is to forward all traffic addressed to an unused IP address on the local network, without any classification, to a remote honeypot located in the NoAH core. The traffic redirected by honey@home is used by the NoAH core to determine the type of the cyberattack and analyse the methods used for the break-in attempt.

With honey@home, users may take advantage of the NoAH architecture and help researchers study Internet threats by providing a wealth of data in real time. As the NoAH project collaborates directly with Computer Security and Incident Response Teams, installing honey@home also benefits the user because it allows computer security professionals to learn about new threats.