



## Malware Filtering

**Malware Filtering** is a project of Deutsche Telekom Laboratories supported by DAI-Labor. Here, on the one hand the tool NeSSi (Network Security Simulator), an evaluation environment for network security measures is build. Second, new detection algorithms enabling the detection of e-threats like malware such as worms, viruses and spam, are realized.

NeSSi allows the simulation of large, real-life IP networks and its inherent properties. In this respect, special attention was devoted to the faithful emulation of the TCP/IP protocol stack. JIAC TNG agents are employed to represent the network components of the simulation environment for efficient simulation.

Beside the pure network simulation, NeSSi offers the economical assessment of a security infrastructure set-up in a network. A security configuration can be associated with costs and by running several attack scenarios like worm propagation, virus spread or DDoS an achieve-

ved security level can be compared to the preceding investments.

In addition, NeSSi offers an open API for the plug-in of detection algorithms. This can either be conventional approaches like a virus scanner or customized as well as scientific approaches.

The second track of the project is the development of such approaches. Accordingly, there are algorithms based on biological-inspired techniques as well as on collaboration schemes. Finally, by means of network analysis, dedicated locations for the deployment of detection algorithms are exposed.

**Contact:**

DAI-Labor, Technische Universität Berlin  
Prof. Dr. Sahin Albayrak  
Phone: +49 (0) 30 - 314 74000  
Fax: +49 (0) 30 - 314 74003  
sahin.albayrak@dai-labor.de

CC SEC Manager at DAI-Labor:  
Seyit Ahmet Camtepe, Ph.D.  
Phone: +49 30 - 314 74117  
Email: ahmet.camtepe@dai-labor.de

