

PROJECT PROFILE

AMP -- Enabling Active Networks via Secure Exokernel Implementations

Active Networks Nodes Implemented Using Exokernels

Under this DARPA-sponsored project, NAI Labs is developing a new software base for Active Network nodes. Referred to as Amp, it will be a platform that allows active code and active network execution environments (EEs) to be executed securely, safely, and with high performance. Efficient execution of active code and constrained execution of active code/EEs are both duties that can and should be performed by the machine monitor (also known as the operating system) of an Active Network node. Amp will enable active nodes to control the execution rights of imported active code so that these executables cannot tamper with the rest of the active node. By realizing these objectives, the Amp project will deliver the technology needed to deploy an Active Network backbone, and demonstrate the security and performance of AMP nodes within the ABONE testbed.

Approach

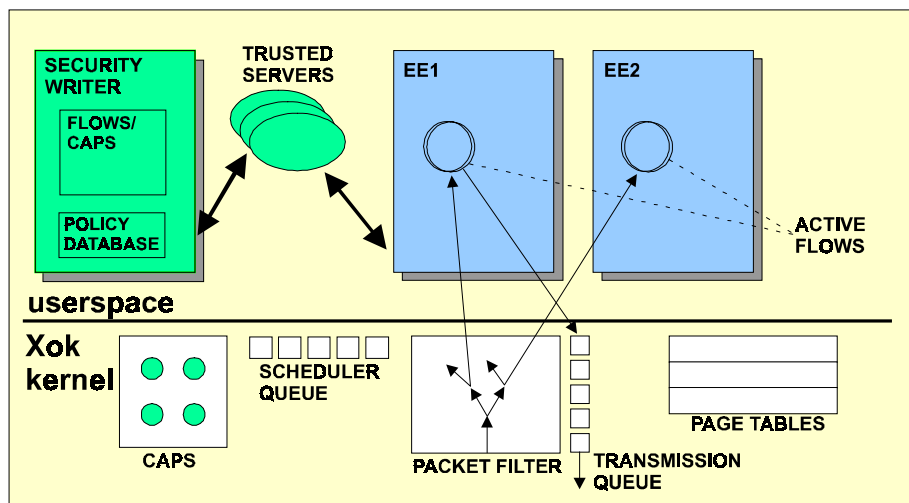
The Amp system will provide fast and lightweight support for hosting multiple EEs and active services on Active Network nodes. It will implement the set of resource abstractions defined by the Node OS Interface, a standard API being developed within the Active Networks' Node OS working group. It will provide controlled, policy-authorized access to an active node's resources and provide separation between Active Network EEs and flows, controlling sharing of specifically identified node state and resources. In addition, Amp will defend against denial-of-service attacks by enforcing resource usage limitations, and supporting on-line, fine-grained revocation.

Research Focus

Implementing an Active Net Node O/S

The relatively static character of the Internet resulting from its world wide deployment and the almost complete dependence upon it by technological society has made it extremely difficult and incredibly time-consuming to deploy new or experimental protocols and base technologies that are not direct extensions of and supported within the context of the existing infrastructure. It is impossible to rapidly tailor the underlying infrastructure to respond to immediate, urgent requirements such as dynamically defending against widespread denial-of-service attacks as they are in progress.

This situation has motivated DARPA to seek remedies to the current situation through its Active Nets research program. The program is focused on producing a flexible and extensible networking environment that accommodates the rapid evolution and deployment of networking technologies through the injection of newly designed services that support the deployment of new networking strategies. An important component of an Active Network is the node operating system environment that supports the security, reliability, availability and quality of service objectives commensurate with the underlying concept. In collaboration with other participating organizations, the AMP project is defining and implementing the Active Net node operating system.



AMP System Architecture

The research approach is to build Amp using techniques and software developed by the DARPA-funded Exokernel project. The Exokernel basis is the result of recent experience that demonstrates physical resources may be managed by user-level applications in ways that allow both efficiency and

- Dennis Hollingworth,
Manager, Security
Infrastructure Group



Approach (continued)

potential for protection. Rather than being a full operating system, the Exokernel is a set of building blocks for the efficient implementation of both operating system abstractions and protection mechanisms. The project will implement a new system that provides the resources required for an Active Network node, using Exokernel techniques for providing high-performance and controlled access to physical resources. The implementation will use access constraint primitives to construct new access control mechanisms for the node resources used by Active Network programs.

Amp will allow active programs to be imported and executed on an active node without allowing the node to be compromised by the program. Through an innovative combination of Exokernel techniques and careful implementation of security mechanisms, Amp will deliver the performance properties and the security properties required by Active Networking. An early prototype of the Amp system, supporting the ANTS, Secure ANTS, and PLAN EEs, has been implemented. The first release of an Amp system completely supporting the Node OS Interface API is slated for mid-2000, and will be aimed at providing secure nodes for experimentation on the ABONE testbed.

New Ideas

- Implement an Active Network node architecture that provides efficient, direct access to low-level resources.
- Provide a highly flexible and efficient set of security mechanisms to protect the Active Network node.
- Specialize an extensible operating system into a platform customized for controlling execution of Active Network protocols.

Impact

- Provide a platform for supporting scalable network bandwidth while protecting the network nodes from attack.
- Demonstrate support for a range of Active Network protocol implementations and execution models to facilitate interoperability.
- Facilitate the deployment of Active Network backbones.

Additional Information

For additional information contact Stephen Schwab (sschwab@nai.com) at 310-737-1600 or visit our Web page at: <http://www.pgp.com/research/nailabs/distributed/amp.asp>.

1/5/01



Who's watching your network

For more information on NAI Labs, contact your authorized NAI Sales Representative, or visit <http://www.nailabs.com>.

CORPORATE Headquarters

3965 Freedom Circle
Santa Clara, CA 95054-1203
Tel (800) 764-3337*
Fax (888) 203-9258

*Call for additional Worldwide Sales Offices