

PROJECT PROFILE

Secure Active Network Prototypes

Objective

Current Active Network research efforts propose to make the network packets themselves an active and dynamic part of the network, so the services offered by the network evolve as the packets travel through the network. The dynamic and proactive nature of an active network increases the security risks of unauthorized or destructive modification of the overall network behavior. It is important that security issues be considered now, as active network efforts progress, rather than being retrofitted after active network designs have solidified. Although each of the current active network efforts has stated its recognition of the importance of security, none has as yet addressed security in full. NAI Labs will investigate the security issues applicable in an active network, define security requirements, develop mechanisms to meet the requirements and develop prototypes that demonstrate security solutions.

Approach

An active packet injects new functionality or services into the network as it passes through the network by modifying each network node's state and behavior, either temporarily or permanently. NAI Labs is defining the security requirements of active networks and developing mechanisms governing the authorization for modification of an individual node and access to its resources. This project addresses such problems as authorization of the packet's ability to inject new functionality and authorization of the packet to access state shared with other active packet streams. The approach is to create a series of prototypes for increasingly complex environments, starting with a simple enterprise environment. Work on subsequent prototypes involves iteratively relaxing the assumptions to make the security issues more complex, e.g., multiple security and administrative domains, authorization that is distributed, etc.

The first secure prototype in the NAI Labs series of prototypes was intended for an active network operating in a single administrative domain with the injected feature deployed inside the packet itself. All authorizations in this environment were based on attributes represented in the packet container. NAI Labs developed the security requirements needed in this scenario and the attributes needed as a basis for enforcement of the requirements. This initial prototype demonstrated the ability to provide authentication of the originator of an active packet at each active node encountered in the network and the use of policies that are in part based on network location. The originator authentication was based on digital signatures, using pre-placed asymmetric keys. The prototype provided a wrapper for the node resources and limited the interface to the node seen by active code. A policy was implemented that restricted the active code's ability to access resources and services of the node based on the identity of the active code originator as well as on the parameters of the service requested.

NAI Labs has now developed a second prototype, which extends the security protection offered in the first prototype developed under this contract so that it now supports wide area network environments. The first prototype assumed that principal identities and their authorizations were widely and commonly known, as is appropriate for enterprise networks. These assumptions are not applicable to a wide area network. For security in a wide area active networks,

Research Focus

Strong Security Solutions for Active Networks

Adoption of active networks has been hampered by the security concerns of the clients of the technology. The prototypes developed in this project provide worked examples of strong security solutions for active networks. The prototypes provide strong end to end authentication and integrity protection and per service authorization of access. The latest prototype allows for the inclusion of authorization information in the active packet itself so that the packet can cross multiple administrative domains and still be properly controlled. Through universal credential identifiers and ubiquitous policy language, the prototype provides for end user control over authorization of access to its created state in the network. This assures the end user that its data and service can be protected according to its wishes. The latest prototype also provides for a mandatory node policy, assuring the node that its data can be protected according to its wishes.

- Sandy Murphy
Principal Investigator,
Network Security Group

Approach (continued)

NAI Labs has redefined the active network packet to include credentials representing the end source principal's authorizations. Credentials are identified by globally known references in the form of fully qualified domain names. The approach uses DNSSEC to provide a secure network-wide distributed authentication infrastructure for the storage and retrieval of credentials. Credentials are carried in X.509v3 certificates, where extensions are used to carry aggregate security attributes, such as "roles". Credential validation is implemented through the chain of issuers in the X.509v3 certificate format. KeyNote, a DARPA funded trust management system, is used both as a policy language and as the enforcement engine. The enforcement engine, which is implemented in the active node operating system layer, performs all authorization and access control checking. The enforcement engine integrates the KeyNote assertion checking with the Java 2 security architecture. To support end source authentication, static payload data must be separated from the payload data modified during the active packet's path through the network. This requires a change in the active packet format, which NAI Labs is recommending to the research community as necessary for adequate security protection of the network. The NAI Labs implementation supports source authentication and authorization based on this packet format.

A secure shared data storage capability is needed to support the needs of active applications. In order to provide end source authorization of access to this shared data, the authorization policy is distributed within the active code that creates the shared data. This, combined with our distributed mechanism for identification and authentication, permits the end source to control access to its shared data anywhere and everywhere in the active network. The use of a ubiquitous policy language and policy engine ensures that end source authorization policies can be enforced throughout the active network.

End source authorization policies governing access to its shared data may be more lenient than local node policy. The authorization enforcement mechanism design recognizes the two sources of policy and ensures mandatory access control, so that local node policy regarding access to shared data can override the policy established by the end source.

Recent Accomplishments

- NAI Labs participated in the joint Active Network team demonstrations in September of 1999, demonstrating the secure construction of quality of service routes among multiple administrative domains.
- NAI Labs completed a second Secure Active Network prototype. The prototype implemented end source authentication based on strong cryptography as well as authorization of access to both active network node operating system services and the active node execution environment services.
- NAI Labs implemented global and flexible mechanisms that allow the Active Network end user to control authorization of access to its shared data in the network.
- NAI Labs implemented an active network authorization enforcement mechanism that has the power to enforce mandatory access control between node policy and end source policies. An active network node can permit the sharing of resources and still retain the ability to enforce its own local policies and protect its local resources, even in the face of more lenient end source authorization of access to shared resources.
- NAI Labs extended the Active Network Security Architecture to include support for strong end source authentication and authorization that can be appended at domain boundaries.

As an extension of the ANTS package, the NAI Labs prototypes run on any system supporting the Java Virtual Machine and Java 2 platforms, including Win32 operating systems, Solaris 2.5.1, and Redhat Linux 5.2. The prototypes were developed on a Sparc Ultra with 128MB RAM and have been run on Pentium platforms from 133MHz processors and 64MB RAM to 400MHz platforms with 128MB RAM.

Additional Information

For additional information on Secure Active Network Prototypes, contact Sandra Murphy (sandra_murphy@nai.com) at 443-259-2300 or visit our Web page at: <http://www.pgp.com/research/nailabs/network-security.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