

## PROJECT PROFILE

### Secure Virtual Enclaves

NAI Labs has developed a new concept of secure, collaborative computing, Secure Virtual Enclaves (SVEs). An SVE is a dynamically composed collection of computing resources and services protected from general use but selectively available to collaborators from multiple organizations. Until the deployment of SVEs, secure electronic collaboration was based on static associations of users and resources, such as virtual private networks (VPNs), implemented through dedicated, cryptographically secure links connecting separate organizational elements. They generally employed expensive, leased data lines and computers committed to specific users. SVEs provide significant cost savings over previous systems by allowing organizations to flexibly and securely utilize their internal networks in conjunction with public networks, such as the Internet, for collaboration.

NAI Labs has developed important, requisite capabilities for supporting secure virtual enclaves including highly specific access controls, security policy definition, and support for an array of middleware technologies.

Currently, establishing extranets such as VPNs enables organizations to share resources with partner organizations via the Internet. Current extranet technologies, however, do not provide the necessary security to permit the appropriate level of sharing yet protect truly valuable resources that must be restricted to internal use. In other words, no facility for *selectively* restricting an external partners' access to an organization's information base exists.

NAI Labs' SVE research enables organizations to securely provide limited access to internal computer resources for selected collaborating organizations by developing scalable, fine-grained controls over what resources are shared and with which other organizations' principals/roles. Further, collaborating organizations are able to protect shared resources without having to enforce one another's security policies.

### Project Objectives

- Dynamic security mechanisms for control of collaborative computing between enclaves using distributed applications over open networks;
- Distributed security policy for collaborations, where each collaborator enforces policy on its own resources;
- Unified support for multiple distributed application technologies and security technologies on COTs platforms;
- Autonomous and secure reconfiguration of policy and authorizations.

### Research Focus

#### Secure Access to Internal Resources for Collaboration

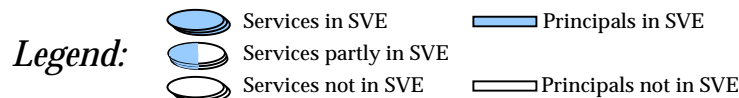
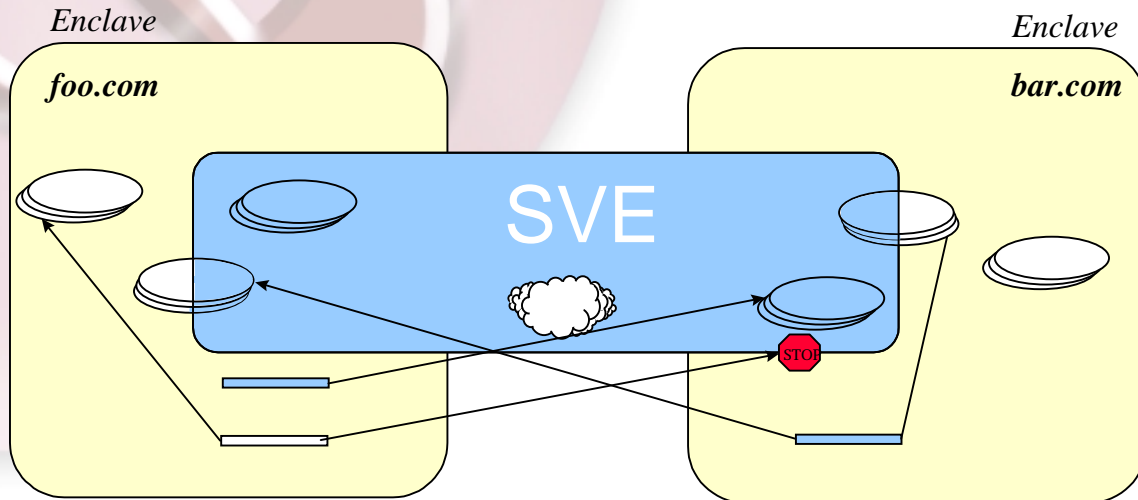
The secure, controlled sharing of resources and information by administratively independent entities is becoming increasingly important as we seek to establish intra- and inter-organizational collaborative working relationships that exploit emerging Internet technology. The resources contributed by individual collaboration participants to the sharing relationship must both be isolated from non-participant access as well as be protected from participant access that violates the established sharing policy defined by the owners of the resources. The Secure Virtual Enclaves project has conducted research into an encompassing concept and underlying requisite functionality to support this evolving need by exploiting COTS technologies.

NAI Labs' SVE research will enable organizations to securely provide limited access to internal computer resources for selected collaborating organizations by developing scalable, fine-grained controls over what resources are shared and with which other organizations' principals/roles. Further, collaborating organizations will be able to protect shared resources without having to enforce one another's security policies.

**- Deborah Shands  
Principal Investigator,  
Security Infrastructure Group**

## Project Objectives (continued)

The illustration below shows two enclaves, each comprised of the computing resources of a distinct company or organization. These enclaves work together to form a Secure Virtual Enclave. The SVE is shown in the central blue area, grouping together resources from both organizations. In some cases, an entire application is exported to the SVE for use. This is illustrated as an oval (an application server) being entirely in the blue SVE area. More commonly, however, only a subset of some application's resources will be available within an SVE, with the remainder being for internal use only. This is illustrated as an oval that is partly in the blue SVE area and partly not. In addition to exporting services to an SVE, each enclave also defines some of its principals as being part of the SVE. These principals are users (or application servers that call on other application servers) that can authenticate themselves to other enclaves.



The SVE security mechanisms enforce a policy stating which SVE resources are accessible to the SVE's principals. A principal in the SVE is shown as a rectangle shaded blue like the SVE. Principals *not* part of the SVE are white. Granted access is shown as an arrow from an SVE member principal in one enclave to an SVE resource in another enclave. In other cases, a member principal may be denied access to an SVE resource if the principal lacks access rights to it according to the SVE security policy. The SVE security mechanisms also protect each SVE resource from accessors that are not part of the SVE and are not part of the organization that owns the resources exported to an SVE. This is illustrated by an arrow from a non-SVE-member principal being stopped at the border of the SVE before it reaches an SVE resource.

## Additional Information

Contact Deborah Shands ([dshands@nai.com](mailto:dshands@nai.com)), Terry Benzel ([tbenzel@nai.com](mailto:tbenzel@nai.com)), or visit our Web page at: <http://www.pgp.com/research/nailabs/distributed/sve-project.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