



Information System Security Operation Enterprise Wrappers for Information Assurance

Deploying Practical, Non-Bypassable, Enterprise Wrappers

Overview

Our focus is on three fundamental challenges for practically deploying non-bypassable wrappers across an enterprise:

- securely managing multi-platform, multi-vendor wrapper configurations over a network; and
- managing data flow, using both “push” and “pull” models, to facilitate intelligent, network-wide detection and response capabilities; and
- writing wrappers that take advantage of their new, networked environment without burdening the wrapper writer with system- and network-specific details; and

To meet these challenges, we:

- developed policy specification, built a technology base, created APIs for host and network controllers, developed a new GUI, updated the wrappers, and demonstrated the new policy function; and
- worked with Teknowledge on a boundary controller and other cross-platform components for interoperability; and
- identified extensions to our Wrapper Definition Language (WDL), database, and Wrapper Query Language (WQL) to permit high-level, abstract interactions with networked components.

Objective

Under previous DARPA funding, McAfee® Research, now the Security Research Division at SPARTA, developed software “wrapping” technology to significantly increase the security

and reliability of large software systems composed of standardized software components. Generic Software Wrappers (GSW) implement practical security and reliability policies in an abstract, portable manner. However, with an increased emphasis on networking and distributed computing, the host-based detection and response capabilities of wrappers need a way to scale to networks of computers, enterprises, and beyond. The objective of Enterprise Wrappers for Information Assurance is to do the basic and applied research necessary to field a prototype scalable cyber-defense system.

This research provided a basis for revolutionizing real-world computer security and assurance technology by combining three key elements:

- our existing multi-platform GSW technology;
- an infrastructure for network and enclave-wide wrapper management and control; and
- a suite of appropriate enterprise-wide wrappers tailored to address specific critical assurance vulnerabilities.

We built upon our existing multi-platform software wrapper technology and scale it to large networks of hosts to support dynamic, distributed deployment, and to inter-operate with high-assurance boundary controllers and other cyber-defense mechanisms.

Approach

At DARPA’s request, we scaled GSW to the enterprise. Working in concert with Teknowledge Corporation, we designed and implemented a scalable, secure, cross-platform management infrastructure for wrapping technologies, including our multi-platform GSW and

This work sponsored by DARPA through SPAWAR Contract Number N66001-00-C-8023.



Enterprise Wrappers for Information Assurance

Deploying Practical, Non-Bypassable, Enterprise Wrappers

Teknowledge Corporation's NT-based mediators. We developed a Wrapper Management Infrastructure (WMI) that complements other infrastructure elements being developed by DARPA which extends wrapper benefits to the entire enterprise. The WMI manages wrapper functionality within all hardened systems within an enclave, thus coordinating security boundaries within each hardened host with those enforced at the network's boundary controllers.

We augmented the GSW Toolkit (GSWTK) to support the WMI. This entailed modifications to existing components as well as the development of additional infrastructure components. We established a new trust model (above), with a more flexible approach than previous trust models. Additionally, we worked with other DARPA principal investigators to integrate enterprise wrappers as both a detector and response tool into a system designed to react to attacks at machine speed.

Recent Accomplishments

We made major progress in the design and implementation of enterprise wrappers. Enterprise wrappers is now the default for the GSWTK. Individual accomplishments include:

- **Policy Specification:** We chose a simple grouping of code, data, and rules to represent policy. Such groupings can be combined to provide a range of organization policies appropriate for the threat levels they may encounter.
- **Base Technology Build-up:** We improved the underlying GSWTK to support the planned

enterprise wrappers functionality. We added modularity to support both local and remote management, and designed an architecture for, implemented, and released a version of the GSWTK with additional platform independence.

- **New APIs, Host, and Network Controllers:** We designed and implemented
- **new APIs to support the new WMI.** Coincident with the development of the new APIs, we analyzed and selected communication and storage protocols that allowed for the development of the host and network controllers.
- **New GUI:** We designed and implemented a new GUI that simplifies policy management locally or throughout an enterprise. The GUI represents the policy model research that led the researchers to believe was appropriate for enterprise wrappers. The flexibility of this GUI has caused it to supplant the previous GSWTK GUI in all cases.
- **Updated Wrappers:** We updated several wrappers to make better use of the new infrastructure and made iterative improvements to the infrastructure to better support the wrappers.
- **Demonstrations and Integration:** We demonstrated enterprise wrappers' new policy management functionality at the Winter OASIS PI meeting. We are working closer with Teknowledge to provide a single management interface that transparently (or visibly, if desired) remotely manages both companies' wrapping technologies.