

Cross Domain Solution (CDS) Framework Toolkit simplifies development of CDS security policies



Customer Profile

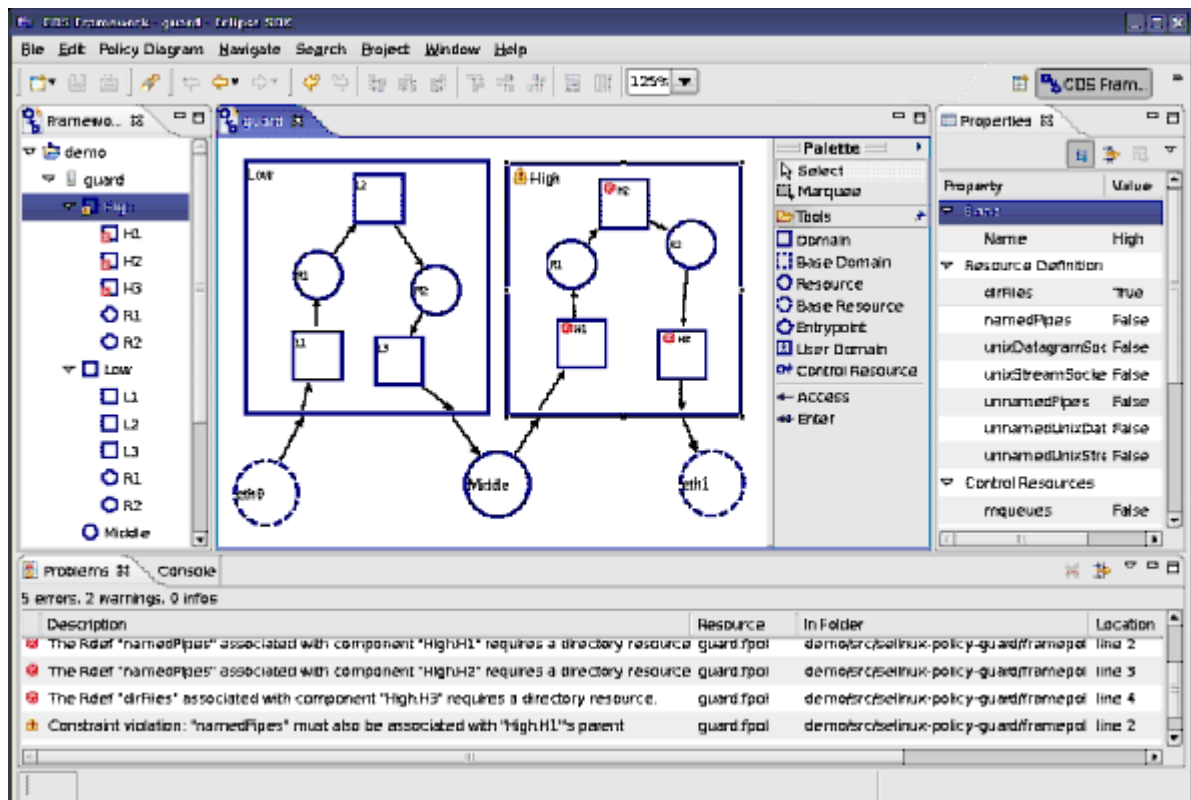
This U.S. Government agency provides solutions, products, and services that enable defensive information operations. They are also focused on securing information infrastructures critical to U.S. national security interests. A key requirement is to ensure the secure exchange of information between and among different Department of Defense and Intelligence agency organizations.

Business Challenge

Security engineering is critical to designing secure applications. However, emphasis on security design frequently takes a back seat to functionality. For government high-risk systems it is essential to design security into the solution from the start. Building solutions that meet stringent security standards and guidelines requires an operating system with a security model that can meet government assurance criteria – while still being robust, flexible and configurable. Security enhanced Linux (SELinux) meets those requirements. It provides the best and most pragmatic implementation of Mandatory Access Control (MAC) available in a commercially-supported operating system. However, SELinux requires extensive expertise to develop policies specific to solution requirements.

Solution

Tresys responded to this need with the Cross Domain Solution (CDS) Framework. CDS Framework is a toolkit and language definition project. Sharing information across domains inherently exposes the sharer to greater risk that his secrets may be unintentionally revealed. As a result, Tresys' designed and implemented SELinux Type Enforcement policies that run in hardened "trusted" computer platforms that function as a guard between two security domains. These systems only allow data that meets very specific criteria to pass from one domain to another. This approach is new to the CDS market and distinct - it supports the transfer of information that would otherwise be precluded by established models of computer/network/data security (e.g. Bell-LaPadula and Clark-Wilson).



CDS Framework also simplifies representation of type enforcement (TE) concepts, such as domains, resources, and access. To make type enforcement capabilities available to non-developers, Tresys developed a graphical front end, allowing designers to draw information flow architecture and compile it into SELinux type enforcement language.

Summary And Benefits

Modern military and intelligence operations critically depend on the timely sharing of information. Cross domain solutions can expedite this process in ensuring information flows and expediting the sharing of information that was previously mixed with sensitive information. However, building applications to meet these requirements are complex. Not only does the CDS Framework toolkit make it easier to develop these solutions but it also ensures consistency in the security and quality of the implementation. This translates into a higher return on investment as compared to traditional methods.

About Tresys

Tresys innovates and applies advanced technologies to quickly solve the needs of customers requiring agile responsiveness to security requirements. By leveraging secure open source software, our products and services support the most sensitive security missions around the world. As a result Tresys enjoys a distinct reputation for shifting the way governments and businesses approach security. For more information, visit: www.tresys.com.

