TITLE

Modeling SELinux type enforcement security architectures in AADL

ABSTRACT

In today's world of network connectivity nearly everything from cell phones to personal entertainment devices to industrial control systems are remotely accessible. Unfortunately these software centric devices continue to be plagued by the vulnerabilities present in both COTS (common off the shelf) and custom software. So, while it's become increasingly critical that security be designed in from the start, security requirements are still addressed separately from functional requirements. This later leads to products where the security mechanisms aren't well integrated with the software and likewise fail to fully protect the system. This paper shows how this can be addressed in software centric systems built on a Linux platform. Using the Architectural Analysis and Design Language (AADL) this paper will show how SELinux type enforcement rules can be modeled alongside the functional software requirements. This results in a closer alignment of security and software in the system leading to cheaper, more resilient products in today’s attack prone environment.