2006 Annual Computer Security Application Conference
Work in Progress Abstract Proposal
NSA Center for Assured Software
Software Assurance Analysis Methodology

Kris Britton
rkbritt@missi.ncsc.mil
(410) 854-454

Background

The software assurance problem can be summarized very simply: there is too much software and too little assurance.

The United States is increasingly reliant on information technology systems in virtually every aspect of daily life. As such, computer software, which controls these systems, plays a key role in their reliable operation. In addition, the foundation of these systems increasingly comprises commercial off the shelf (COTS) components. Therefore, the assurance of commercial software becomes more critical to the security of our nation everyday.

As we have become more dependent upon COTS software, the systems in which these components are integrated have exploded in complexity. Our ability to gain confidence in these systems has not kept pace with this complexity and the ability of our adversaries to efficiently penetrate them through flawed implementation. Further, current software development (and evaluation) practice provide little or no mitigation to the playful or malicious introduction of extraneous functions.

To establish a coordinated approach to address these issues in the national security community, the National Security Agency has created the NSA Center for Assured Software (CAS) to identify and work with the community to establish technology and methods to more effectively establish trust in the mass of software that is controlling our nation’s most sensitive national data.

The NSA CAS goal is to provide a means by which all national security systems can be trusted to protect this data. In working toward this end, the CAS has embarked on a program to identify and create a repeatable, automated means by which to measure the trustworthiness of software. This work requires that new assurance metrics and methods be identified that can be shown to correlate with trustworthiness. In addition, a new methodology must be created that heavily employs automation. Automation will be a key property with any approach that has to deal with the vast amounts of software that comprise our national security systems.

Project Approach and Status

This project began in early 2006 with a survey of major software analysis tools to establish the nature of the current state of the art. During the course of this survey a number of software analysis pilots were performed to exercise various techniques that current tools could support. The culmination of the project will be the first draft of the CAS Software Assurance Methodology.

Thus far, we have documented our analysis of 5 software analysis tools that are available today. We have established the components of the new methodology and have an initial reading on how well current tools can support a new methodology.

The next phase of the work will begin to formally document the methodology and work on the technology gaps that need to be filled to make the methodology robust and cost effective.