Compositional Assurance
R&D
Panel Session

Moderator: Michael McEvilley, MITRE
August 5th, 2009
Panel Session Overview

- Brian Snow will speak to a cross section of assurance issues
- Moderator to frame the panel discussion
- Panel discussion
Panel Discussion Context
Problem Statement

- How do we compose complete systems from a collection of parts?
  - Complete: functionally correct with a sprinkling of <insert your favorite> subjective properties (non-functional, “-ilities”)
    - Examples: safe, secure, resistant to attack, able to sustain some specified data throughput, dynamically reconfigurable, robust, reliable, affordable
    - Subjective properties makes the hard problem incredibly hard

- We are not talking about the “GRAND CHALLENGE” composition problem
  - Unbounded integration of any A with any B to achieve a complete C

- Can we constrain the Grand Challenge problem such that there is a solution that can be practically applied?
Compositional assurance is not new
- We do it every day, informally

Compositional assurance is largely an ART
- Smart people doing smart creative things
- Methods, techniques, philosophy passed down
  - But not formalized, vetted, consistently reproducible

Compositional assurance needs SCIENCE to better leverage the ART
Panel Discussion Context
The Facets of Compositional Assurance

- There are multiple facets to that which must compose
  - Requirements and specifications used to architect and implement complete solutions
  - Individual components/products integrated to implement complete solutions
  - Requirements and specification used to architect and implement components/products
  - Runtime behavior composed via “late binding” of functions

Assurance arguments for ALL the above!
Use-case to illustrate the impending need

- Cross Domain Transfer Solutions are trusted components
  - Trust must be demonstrated and approved in the context of an environment
    - Certification and Accreditation (C&A)
  - C&A is taking more time as component capability, complexity and the threat increases
    - And current solutions are relatively simple (centralized and monolithic)

- Characteristics of future cross domain transfer solutions
  - Modularized and distributed
  - Remotely managed
  - Dynamically reconfigurable to provide “just in time” services
  - Continuously available with limited human interaction
  - Dependent on having confidence in a distributed trust model

- We must transition to the future without increasing risk
General Centralized Cross Domain Transfer Solution

Sequenced Set of Data Manipulation Functions

Configuration

Status

Audit

Object

CDS Boundary

Object'

Security policy domain “YELLOW”

Trusted Multi Domain

Security policy domain “RED”
General Modularized and Distributed Cross Domain Transfer Solution

- Minimize the size and complexity of components that “touch” multiple domains
- Establish assurance in the individual parts
- Combine the parts and establish assurance of the whole

Security policy domain “YELLOW”  Trusted Multi Domain  Security policy domain “RED”
Transform the CDS into a Service Engine

- Add management and control allowing for “just-in-time” instantiation of only the functionality required for a particular cross domain flow
The Role of Compositional Assurance

Compositional assurance is a necessary aspect for the realization of the modularized and distributed CDS use case.

Compositional assurance enables:
- Aggregation and dynamic instantiation of the functional decomposition
- Distributed policy enforcement points to act as directed by their corresponding distributed policy decision points
- Secure remote management of the entire distributed solution
- Multi-threaded service invocation
Panelists

- **Chris Gill**
  - Associate Professor, Dept of Computer Science and Engineering, Washington University

- **Tim Kelly**
  - Senior Lecturer, Department of Computer Science, University of York, UK

- **John Rushby**
  - Program Director and SRI Fellow, SRI International Computer Science Laboratory

- **Brian Snow**
  - former IAD Technical Director, NSA
Panel Session Game Plan

- Posing of questions to the panel from the floor

- Intent is to remain focused on the science of the problem

- Moderator reserves the right to alter questions

- Moderator may pose prepared questions

- Moderator to be moderated by Rance DeLong

- Let's have fun ...