

# Assurance of Compositions and Federations

Gary Vecellio

770-739-8598 • [vecellio@mitre.org](mailto:vecellio@mitre.org)

Army-Contract MOIE

The logo for the MITRE Technology Program, featuring a stylized graphic of stacked blocks in yellow, orange, and blue to the left of the text.

**MITRE**  
Technology  
Program

# Problem

- **For the majority of high confidence systems, development and validation of the software are far more difficult than for "ordinary" systems.**
- **Current techniques for validating systems built on compositional frameworks and federation technologies introduce assurance argument coupling.**
- **Assurance argument coupling is brittle, making it expensive and time consuming to modify and revalidate the system once it has been deployed.**

# Background

- **Software compositions and federations result from the aggregation of independently developed functionality (i.e., components and services).**
- **Compositional frameworks and federation technologies support the deployment and execution of component- and service-based systems.**
- **Loosening the coupling that current verification methods impose on this type of software will decrease revalidation costs (time and dollars).**
- **Looser coupling can be supported by adding generic property enforcement mechanisms to the composition and federation infrastructure.**

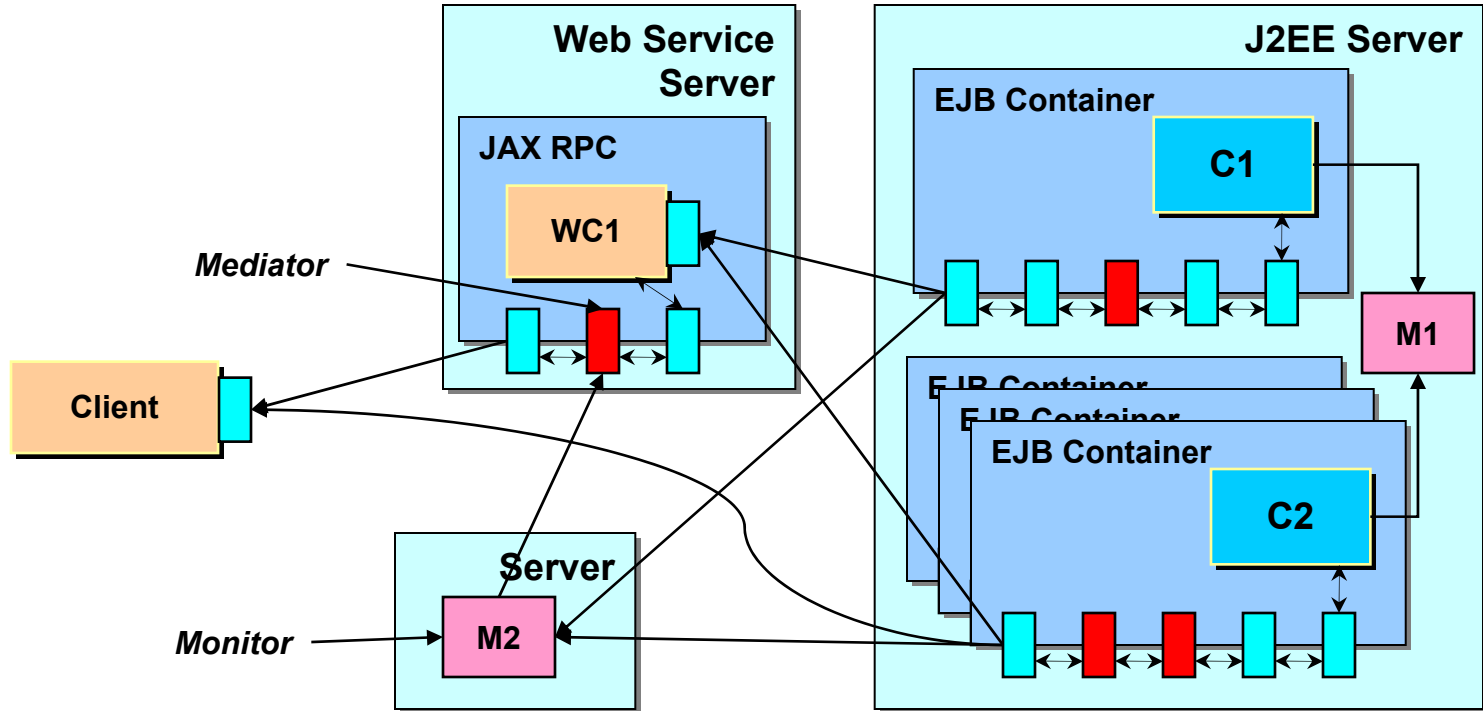
# Objective

- Investigate principles, methods, and mechanisms for infrastructure-level policy and property enforcement
- Demonstrate the enforcement of application type-specific policies and properties on a variety of commercial infrastructures
- Propose ways to loosen the component and service "verification coupling" present in current compositions and federations

# Activities

- **Conduct investigations of build time and runtime policy and property enforcement**
- **Augment the JBoss EJB and JAX RPC Web service infrastructures to support property enforcement**
- **Develop software that demonstrates the augmented infrastructures**
- **Engage the J2EE and Web service communities through open source and standards activities**
- **Engage the academic community through participation in conferences and workshops**

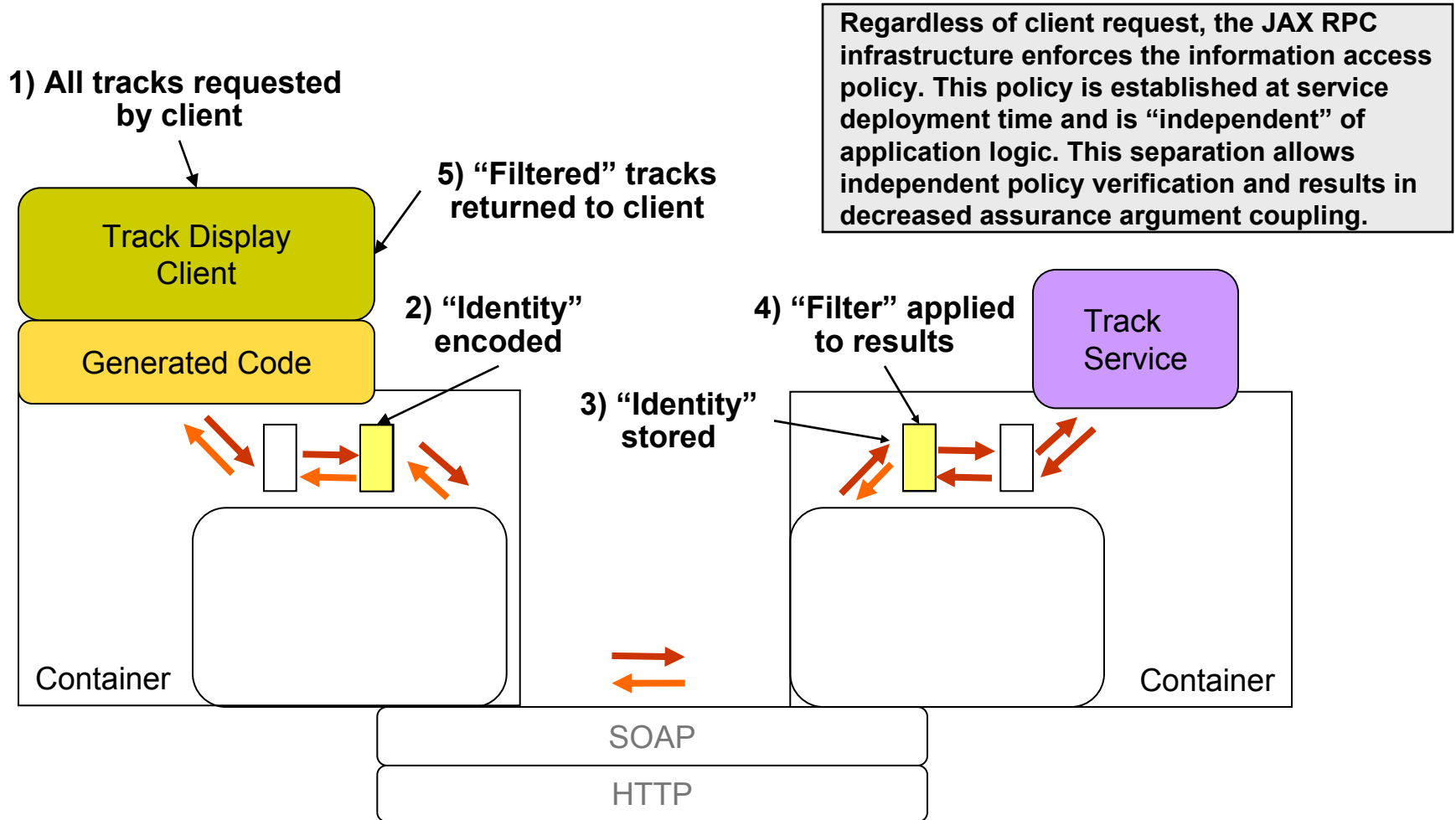
# Highlight



- Mediators enforce properties during invocations (e.g., used to establish method-level pre-conditions & post-conditions).
- Monitors enforce global properties (e.g., used to establish application- or service-level invariants).
- Both can be configured at deployment time.
- Policies and properties implemented in this way are verified independent of the application or service functionality.

# Demonstration: Information Guard Example

(Animation)



The definition of "Identity" is flexible, particularly not limited to a role. "Filtering" could be any operation, e.g., applying an XSLT transform to eliminate "sensitive" information.

# Impacts

- **Lessons learned shared with DISA's Network-Centric Enterprise Services project**
- **Results of investigations presented to industry and academia**
  - **Component- and aspect-oriented programming workshops**
  - **J2EE and Web service vendors**
  - **High confidence software community**
  - **Information assurance community**
  - **Standards and open source groups**

# Future Plans

- **Extend investigations and analysis to include enterprise service bus technologies**
  - **This type of technology should prove essential for the integration of heterogeneous enterprises.**
  - **Our initial investigations of this technology indicate the applicability of our policy enforcement patterns and mechanisms.**
- **Investigate the applicability of this technology to additional domains and policy types**