

Trust and Adaptability in Web Services

Joshua Guttman

781-271-2654 • guttman@mitre.org

Air Force MOIE

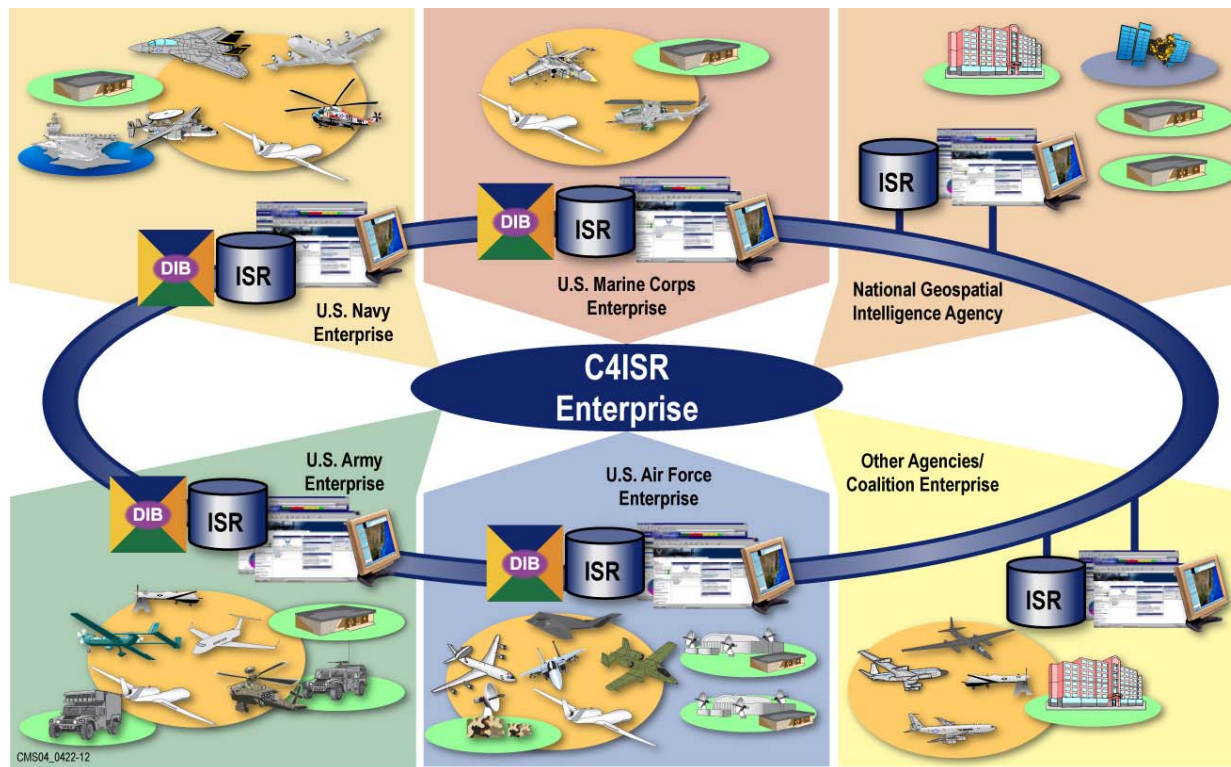


Problem

- **USAF adopting service-oriented architectures**
 - **Need major information assurance changes**
 - **Not just network + host security, also access control meaningful to applications**
- **Data-aware protocols for Web service security:**
 - **Bind transaction to authenticated peers**
 - **Sensitive to trust attributes, e.g., roles**
 - **Aware of data schema, metadata**

Background

Service-oriented architecture using Web services



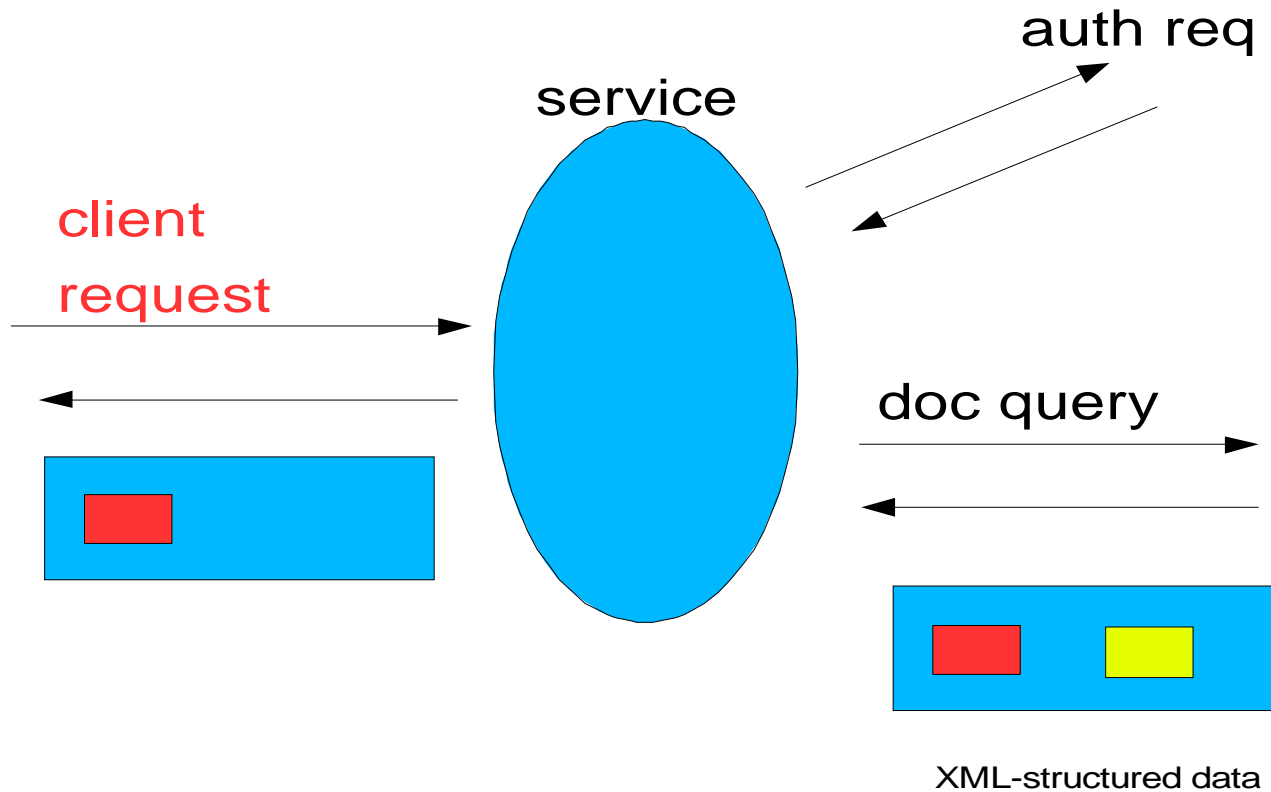
Objective

- **Crypto Protocol domain-specific languages**
 - CPPL already ties protocols to trust mgt
 - We need to add an XML data model
 - XCPL: trust engineering for Web services
- **Pay-off: Better filtering than guards**
 - Extract sub-product tailored to client
 - Depends on mission, role, sensitivity

Activities

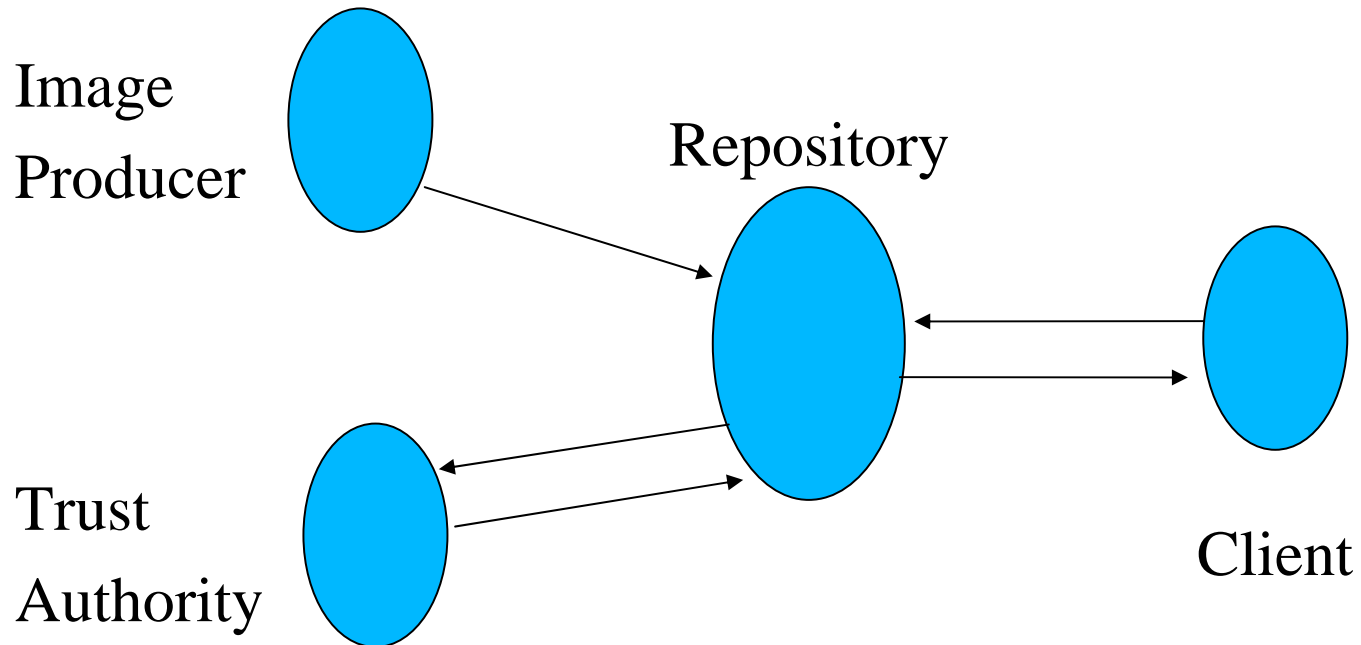
- **Integrate XML data model with CPPL**
 - **New XCPL semantics, compiler**
 - **XML query-style access to data**
- **Demo: Web service filtering with XCPL**
 - **Sensitive to recipient, authorizations, object schema and metadata**
- **Extract reusable components for standard implementations**

Highlight



Web services are security-aware transactions

Demonstration

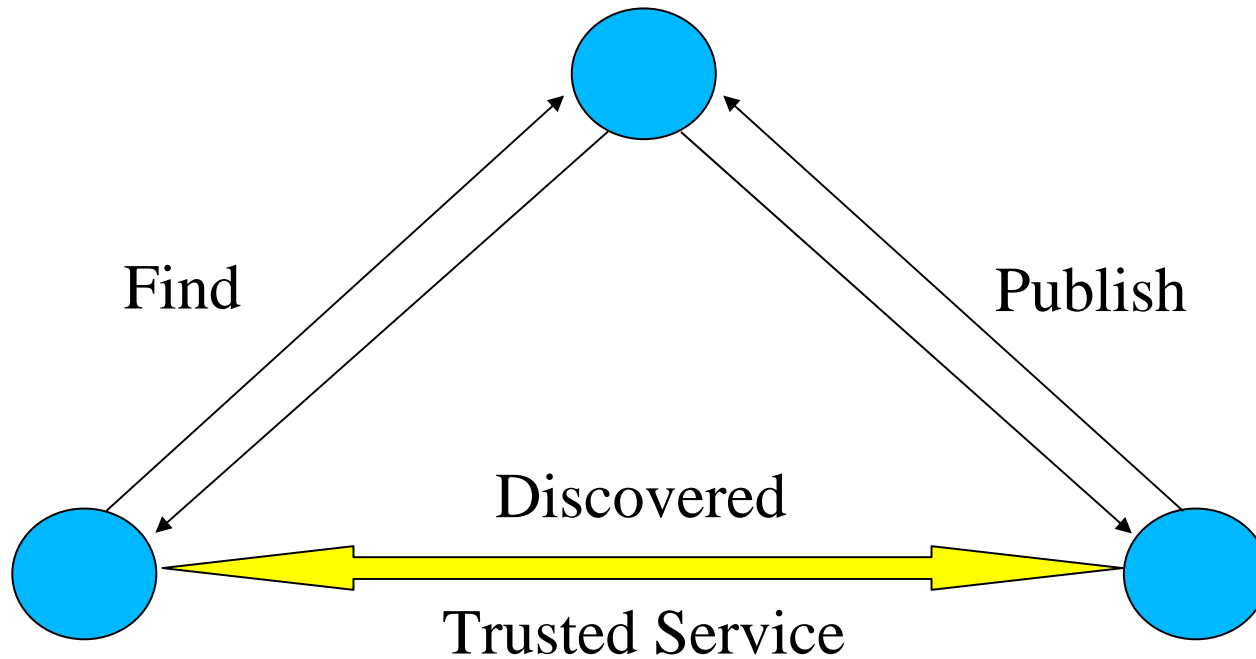


Client retrieves images from repository
subject to trust policy

Impacts

- **Fine-grained enterprise IA for Web services**
 - **Applicable to GIG IA, NCES, DCGS, AOC**
- **Better functionality than guards**
 - **Filtering driven by authorization, metadata**
 - **Cryptographically bound by protocols**
- **Transition strategy: AF programs, DISA, NSA**

Future Plans



Service discovery discloses trust constraints