Joint Cross Domain eXchange (JCDX):
Integrating Multilevel Command and Control into a Service Oriented Architecture to Provide Cross Domain Capability

An Accredited Approach
to Cross Domain Information Sharing

Presented By:
Christopher J Raney
SSC San Diego
Multi-Level Secure (MLS)

- MLS labels every file at the appropriate security level
  - Labeled files are only accessible to users with the proper security clearance

CMW:
Compartmented Mode Workstation. The core operating system of an MLS system.
Multiple Security Levels (MSL) Challenges

- **Multiple Security Levels (MSL)**
  - A conglomeration of single-level workstations/servers used to provide information for analysis.
  - Information is passed between the two systems utilizing security guards, which strips off valuable intelligence data from remarks lines.
  - With an MLS solution such as JCDX, only a single system requires management. **MSL** environments require at least a minimum, a separate system per security level.

_MSL should not be confused with MLS:_

*Multiple Security Levels are limited to separate application displays and downgrading of information can result in loss of valuable data.*
What is JCDX today?

- A certified, operational, multi-level secure (MLS), PL4, all-source data management, display, fusion processing and near real-time dissemination capable system
- JCDX labels incoming data (tracks / messages / other products) from multiple sources / classification levels, manages that data (correlation, manipulation) and transmits data out to multiple sources at multiple classification levels
Cross Domain Solution Architectures

**Generic Architectures Today**

- **HIGH Data**
- **LOW Data**
- **‘Other’ Data**

**Data Sanitizer**

**Network Guard**

**SYNCORIZATION TOOL**

**Multiple Security Levels (MSL)**

**J CDX pre SOA**

- **MLS Server**

- **High-Side Network**
- **Low-Side Network**
- **‘Other’ Network**

**Multi-Level Security (MLS)**

No guard; security is inherent within the system
JCDX Architecture with SOA Extensions

**PROS:**
- Clients only access content releasable to their domain (Mandatory Access Control)
- Data producers only need to “Post Once” for data to be available to all applicable domains
- No unnecessary data loss from sanitizers

**Clients on different WANS:**
- Query message and intel product archive
- Profile message and intel product archive for updates
- Post data for collaboration between security domains
- Receive tracks for display

No guard; security is inherent within the system
SOA Architecture

Web Services

- Federated Search Provider
- cPDS

JWSS

Local Search Provider

 MLS Store

JCDX

Adjudication Server

Trusted O/S Services
Classification Policy Decision Service (cPDS)
- provides other systems with methods for handling labeled data such as label comparison

Federated Search Provider
- allows users and applications to search multi-level data stores from single level networks and provides a “read down” capability to all lower level domains
Current NCES Security Services only implements role based access control

First attempt to authorize the user via NCES RBAC, and then attempt to authorize the user’s clearance via JCDX cPDS
Other cPDS methods

- **isValid**: takes a classification and returns whether the classification is valid
- **getRelationship**: takes two arguments, a Subject Clearance and an Object Classification and returns the relationship. The relationship can be one of the following: Subject Strictly Dominates, Equal, Object Strictly Dominates, and Incomparable
- **getAggregateClassification**: takes a list of classifications and produces a classification that is the ‘sum’ of the arguments. (e.g. `getAggregateClassification 'SECRET REL GBR' 'SECRET' 'UNCLASSIFIED' yields 'SECRET').
- **getGroupClearance**: takes a list of user clearances and produces a group clearance. This group clearance is the highest classification that can be read by all of the users in the group
- **iSReleasableTo**: takes a data classification and a list of clearances and determines whether the data can be released to all of the users whose clearances were used as arguments
- **canReceive**: The `canReceive` method takes a user clearance and a list of data classifications and determines whether the user can see all of the data whose classifications were used as arguments
Federated Search Provider

- Allows searching of the JCDX MLS PL4 data repository through a Web Service
- Authenticates the search request via NCES and cPDS and then returns messages at the appropriate classification (including “read-down”)
Applying JCDX Design Approach to Achieve Enterprise Wide CDS Capability

* Architecture Simplified for Illustrative Purposes
Other Critical Pieces (Future Work)

- Trusted Editor
- Trust Service
- Labeling Service
- Accreditation / Policy Changes
Content producers need a method to produce labeled content
  – Must be able to “trust” the label

Unreasonable to expect all users to have MLS clients
  – Microsoft Windows has a very low “trust” level
Trust Service

- Transferring labeled data between two **systems** must involve a trusted interaction
- In non-SOA these trust relationships are statically defined
- SOA needs an automated method to determine which services on the network are trusted
- Trust service could be queried to determine the level of trust that a given service/system has
Labeling Service

- Must be able to transition unlabeled content into labeled content
- Labeling service would provide an interface to allow the submission of content for labeling
  - assign a security label to the content based on a pre-defined ruleset
  - then “sign” the associated label to allow other services to verify the given label
Summary

- JCDX has begun to bridge the gap between traditional MLS systems and SOA and has developed an architecture that can be applied to other MLS systems.
- JCDX Web Service Gateway’s can be used to extend MLS capabilities to single level clients.
- Extending MLS systems to a SOA enables coalition operations.
# Points of Contact

<table>
<thead>
<tr>
<th>PEO C4I PMW160</th>
<th>CDR Wayne Slocum</th>
<th>619-524-7511</th>
<th><a href="mailto:Wayne.slocum@navy.mil">Wayne.slocum@navy.mil</a></th>
</tr>
</thead>
<tbody>
<tr>
<td>PEO C4I PMW160 APM</td>
<td>Maureen Myer</td>
<td>619-553-9748</td>
<td><a href="mailto:Penney.myer@navy.mil">Penney.myer@navy.mil</a></td>
</tr>
<tr>
<td>PEO C4I PMW160 Chief Engineer</td>
<td>Robert Fish</td>
<td>619-553-6406</td>
<td><a href="mailto:Robert.fish@navy.mil">Robert.fish@navy.mil</a></td>
</tr>
<tr>
<td>JCDX Chief Engineer</td>
<td>Paul Kennedy</td>
<td>619-553-9541</td>
<td><a href="mailto:Paul.kennedy@navy.mil">Paul.kennedy@navy.mil</a></td>
</tr>
<tr>
<td>JCDX Chief Scientist</td>
<td>Chris J. Raney</td>
<td>619-553-5282</td>
<td><a href="mailto:raneyc@spawar.navy.mil">raneyc@spawar.navy.mil</a></td>
</tr>
<tr>
<td>PEO C4I FMS Case Manager</td>
<td>Steve Reddick</td>
<td>619-524-7274</td>
<td><a href="mailto:Steven.reddick@navy.mil">Steven.reddick@navy.mil</a></td>
</tr>
</tbody>
</table>