Open Architectures in the Defense Intelligence Community

By Derrick H. Karimi
Member of the Technical Staff
Emerging Technology Center

This blog post is co-authored by Eric Werner.

In an era of sequestration and austerity, the federal government is seeking software reuse strategies that will allow them to move away from stove-piped development toward open, reusable architectures. The government is also motivated to explore reusable architectures for purposes beyond fiscal constraints: to leverage existing technology, curtail wasted effort, and increase capabilities rather than reinventing them. An open architecture in a software system adopts open standards that support a modular, loosely coupled, and highly cohesive system structure that includes the publication of key interfaces within the system and full design disclosure. One area where the Department of Defense (DoD) is concentrating on the development of service-oriented architectures and common technical frameworks is in the intelligence community, specifically the Defense Intelligence Information Enterprise (DI2E). As this blog post details, a team of researchers at the SEI Emerging Technology Center (ETC) and the Secure Coding Initiative in the SEI's CERT Division, are working to help the government navigate these challenges in building the DI2E framework, which promotes reuse in building defense intelligence systems.

Foundations of Our Work

Our work focused on development of a framework for DI2E, the non-command-and-control (C&C) part of the Distributed Common Ground System (DCGS) and the Combat Support Agencies (CSAs). The DI2E Framework provides the building blocks for the Defense Intelligence Community to more efficiently, effectively, and securely develop, deliver, and interface their mission architectures. The core building blocks of the DI2E framework are components that satisfy standards and specifications, including web service specifications that enable a stable but agile enterprise supporting rapid technology insertion.

The key objective of the DI2E Framework is to increase operational effectiveness, agility, interoperability, and cyber security while reducing costs. The framework consists of a reference implementations (RI), a test bed, and a storefront. When completed, the DI2E will provide a fully integrated, cross-domain, globally-connected, all-source intelligence enterprise that comprises the federated intelligence mission architectures of the military services: CSAs, Combatant Commands (CCMDs), Intelligence Community (IC), and international partners.

The DI2E provides functionality that:

- transforms information collected for intelligence needs into forms suitable for further analysis and action

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
22 AUG 2014	**N/A**	

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Open Architectures in the Defense Intelligence Community	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
Werner /Derrick H. Karimi Eric	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)	8. PERFORMING ORGANIZATION REPORT NUMBER
Software Engineering Institute Carnegie Mellon University Pittsburgh, PA 15213	
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited.

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**SAR**	**5**	

- provides the ability to integrate, evaluate, interpret, and predict current and future operations or physical environment
- provides the ability to present, distribute, or make available intelligence, information and environmental content, and products that provide better situational awareness to military and national decision makers

The vision of the founders of the DI2E Framework Testbed is to use a distributed (interagency) development paradigm to implement a software repository focused on componentized reuse, enabled by an open architecture and systematic conformance testing components' interfaces to specifications allowed in the architecture.

Our work on this project—the team included Shelly Barker, Ryan Casey, David Shepard, Robert Seacord, Daniel Plakosh, and David Svoboda, in addition to Eric and myself—spans two fronts:

- We participate in a center of excellence (COE) that consists of universities and labs working with the government to execute DI2E framework processes. Our work focuses on helping the DoD develop the framework by providing feedback to the DI2E Program Management Office about processes and practices of the framework. When completed, the DI2E framework will comprise the architecture, standards, specifications, reference implementations, components, component storefront, compliance certification, and testing, as well as the configuration management and other governance processes necessary to realize the aforementioned objectives.
- On a second front, we are evaluating specific components to be included in the software reuse initiative. The evaluated software is exposed in a storefront of software components that can be reused when the defense intelligence community is building other systems.

Open Architecture Approach

As part of its approach, the government intends to reuse existing components of the DI2E enterprise, with the goal of taking advantage of free and open-source software, government-off-the-shelf software (GOTS), and commercial off-the-shelf (COTS) software.

Our team of researchers participates in the framework development by contributing to the design of the software component evaluation and developing software tools to support the evaluation process. These tools provide task automation and consistent evaluations across the distributed COE network of universities and labs. Our main focus, however, is on performing the software evaluations that are necessary to ensure quality reusable components are recommended for reuse.

Evaluating Components for Reusability

When a new or existing government program defines a new need—be it a map, login service, or some other kind of widget to build out part of its system and fulfill some requirement—the program ideally will not have to build the system entirely from scratch. Through software reuse, the program should be able to easily identify and examine components that have already been evaluated, embedded, and tested. Our role involves evaluating and testing the software components that will be housed in the DI2E storefront for programs to view and ideally reuse.

When we first began work on the DI2E Framework in 2013, together with the other COE labs, we focused on building up and designing an evaluation framework. We began in an Agile fashion, building on a checklist that now contains approximately 70 questions asking for judgments and measures of different aspects of the software including

- How easy is it to find the software?
- How easy is it to install the software?
- How complete is the testing?
- Is there a community that supports this?
- Can you go online and easily find information about it?

Next, we used the checklist to answer these questions for each piece of software that we evaluated. We tracked down information by examining and using the software and also reading and evaluating the documentation. To answer the evaluation questions that the user experience or documentation did not address, we asked the software developers to answer such questions as

- What development process do you use?
- Do you use bug tracking?
- Do you have a checklist for release?
- What is your approach to testing?
- Are you measuring unit test coverage?

In addition to the checklist of questions, our team generated other prose documents, including installation and integration how-tos. For more mature software components, these documents point back to the software component's documentation. While the checklist guides the evaluation, the prose sections capture more detailed information. The completed checklist provides a naturally indexed and self-contained summary of how applicable a piece of software is to the DI2E.

The prose documentation details the software evaluation, presenting the evidence used to justify the abbreviated checklist answers. Additional prose documents provide architectural details relevant to the DI2E, such as what deployment dependencies, data formats, and interfaces are supported. This information can rapidly inform programs of record about the suitability of reusing a component in their system. The documented and validated data formats and interfaces will allow

users to rapidly design a system from compatible components with a high level of assurance that the design is valid.

Our Evaluations

Our work on the DI2E framework also included software component evaluations that align with the ETC's areas of expertise in data-intensive scalable computing. As of July 2014, we have evaluated assets that cover the following functional requirements:

- **data-content discovery**
- **data mediation**
- **data–handling**
- **widget framework**

One of the software component evaluation documents maps the component's features to the services that the intelligence community is seeking. For example, if an agency has already identified that multiple source query capability is critical for its software, we have indexed existing software components with these services so that they may be easily identified.

Collaborations

At a higher level, our evaluation of the software components focuses on reusability, but security remains an underlying and important concern for every evaluation. One aspect of our security evaluation involves code analysis. For that aspect of our work, we are working with researchers in the CERT Secure Coding Initiative, who maintain a laboratory environment for static analysis. The Source Code Analysis Laboratory (SCALe) consists of commercial, open source, and experimental tools that are used to analyze various code bases, including those from the DoD, energy delivery systems, medical devices, and more. Using SCALe, source code auditors then identify violations of the published CERT Secure Coding rules.

In the Cloud

Given the federal government's embrace of cloud computing, it is important to note that DI2E is set up as a private cloud environment. The DI2E cloud offers Infrastructure as a Service (IaaS), where testing machines can be provisioned, and Software as a Service (SaaS), where common developer tools are available for use. Working in the DI2E cloud enabled us to have on-demand access to infrastructure machines to test different software components.

Working in the cloud also allows us to address the "it works on my machine" problem, which my colleague Aaron Cois detailed in a recent blog post. This phrase describes a common problem in which developers, often early in their career, write software code to address a problem. After testing the code and finding that it works on their machine, the developers deploy it to customers where it may fail to work

because of differences in system configuration. One positive aspect of working in the cloud is that the common environment allows configurations of systems used by collaborating organizations to be more homogenous. The configuration management systems exposed to cloud instances by the cloud administrators can enforce consistency that aids in component integration.

PlugFest and Future Work

Our research on DI2E aligns with ETC's mission, which is to promote government awareness and knowledge of emerging technologies and their application and to shape and leverage academic and industrial research. There is considerable need for this type of research since "the practice of reuse has not proven to be … simple however, and there are many misconceptions about how to implement and gain benefit from software reuse," as Raman Keswani, Salil Joshi, and Aman Jatain write in a paper presented at the 2014 Fourth International Conference on Advanced Computing & Communication Technologies. Our work also leverages various SEI skillsets, such as hands-on evaluation, construction of frameworks, and data processing.

My colleague Dan Plakosh and I also attended DI2E PlugFest, an annual demonstration of the DI2E framework. The Plugfest eXchange provided an environment of networked, interoperable, and reusable components where vendors deployed and showed their tools for providing flexible, agile, and data-driven capabilities to warfighters. At PlugFest, we were able to see first-hand which vendors were able to align their software with the ideals of the DI2E framework.

We welcome your feedback on our work in the comments section below.

Additional Resources

For more information about SEI Emerging Technology Center, please visit http://www.sei.cmu.edu/about/organization/etc/.