Software and Hardware Assurance

DoD Establishes Federation of Software and Hardware Assurance Providers

Tom Hurt, ODASD(SE)
Ray Shanahan, ODASD(SE)

Abstract. Keeping DoD hardware and software technology secure is more critical than ever. In response to a mandate from Congress, Deputy Secretary of Defense Robert O. Work chartered the Joint Federated Assurance Center (JFAC) [1] as a federation of U.S. Military Department and agency software assurance (SwA) and hardware assurance (HwA) organizations and capabilities. According to this charter, the JFAC is charged with supporting program offices throughout the life cycle with SwA and HwA expertise, capabilities, policies, guidance, and best practices. The JFAC is responsible for coordinating with DoD organizations and activities that are developing, maintaining, and offering software and hardware vulnerability detection, analysis, and remediation support. Other roles and responsibilities of the JFAC include:

- Conducting SwA and HwA analyses and assessments in support of defense acquisition, operations and sustainment activities;
- Advocating for the advancement of DoD interests in SwA and HwA research, development, and test and evaluation activities; and
- Building relationships with other communities of interest and practice in SwA and HwA such as other government organizations, academic environments, and private industry.

Introduction

The challenge of ensuring that DoD software and hardware will operate only as intended is formidable. DoD is more dependent than ever on technological solutions for mission requirements, and this has led to heightened awareness of the possibility that adversaries could target DoD supply chains, insert malicious functionality into software and hardware, or degrade critical systems with counterfeit parts. The globalization of the defense industrial base also has led to concerns about the competitiveness, cost-consciousness, and sources of many suppliers. Given the potential gaps in DoD SwA and HwA capabilities, as well as the cost and complexity associated with increasing the effectiveness of SwA and HwA throughout the life cycle of defense programs, DoD leaders seek to develop and promote enterprise solutions for evaluating and ensuring the cybersecurity of defense systems, components, and services, and for conducting remediation actions where necessary.

In the National Defense Authorization Act for Fiscal Year 2014, [2] Congress directed DoD to establish a joint federation of capabilities to support trusted defense systems and to ensure the security of software and hardware developed, acquired, maintained, and used by the Department. On February 9, 2015, Deputy Secretary of Defense Robert O. Work signed the charter for a new organization, the Joint Federated Assurance Center (JFAC), to coordinate this effort.

The JFAC builds on several earlier initiatives that also focused on strengthening the processes for assessing and implementing SwA, HwA, and related defense system trust and assurance activities. These activities include efforts to promote Trusted Systems and Networks (TSN), Supply Chain Risk Management (SCRM), and requirements for acquisition program managers to submit updated Program Protection Plans (PPP) at each milestone of the DoD acquisition life cycle. The JFAC will support these earlier initiatives and will enhance system security engineering (SSE) through DoD policy, guidance, studies, and supporting information products, as part of a comprehensive program protection process that promotes trust and assurance in defense system hardware and software.

JFAC Purpose and Objectives

As outlined in its charter, the JFAC will facilitate collaboration among the Military Departments and agencies that provide SwA and HwA services to ensure defense programs effectively plan, implement, and employ DoD SwA and HwA capabilities and investments throughout the acquisition life cycle.

The JFAC objectives include:

- Support program offices by identifying and facilitating access to DoD SwA and HwA expertise and capabilities. The JFAC will be a resource for program offices to access SwA and HwA policies, guidance, standards, acquisition practices, best practices, training, and testing support. In addition, the JFAC will provide access to assurance-related expertise and capabilities for DoD program offices, as well as facilitate coordination and support from the service providers.
- Identify and develop requirements for research and development (R&D) initiatives in support of the DoD R&D strategy to innovate vulnerability analysis, testing, and protection tools for SwA and HwA. Through a DoD SwA and HwA capability mapping process, the JFAC will identify potential gaps and needed capabilities.
- Enable efficient coordination and use of SwA and HwA design, analysis, and test capabilities. The JFAC will facilitate the exchange of information, techniques, and best practices for promoting assurance as part of the normal systems engineering and SSE processes.
- Serve as the DoD point of contact for interdepartmental and interagency efforts concerning SwA and HwA. The JFAC will engage with representatives of other federal departments and agencies as their access point to increase mutual awareness of tools, evidence-based practices, support environments, and an expanded talent pool.
- Develop and sustain a Department inventory of SwA and HwA resources, including tool licenses. The JFAC will explore and recommend ways to enhance access to enterprise licenses for selected automated software and hardware vulnerability analysis applications. The JFAC also will consider other potential ways to provide affordable and flexible access to automated, vetted tools for assessing and improving SwA and HwA throughout the Department.

Organization

Responsibility for management and oversight of the JFAC resides with a Joint Steering Committee led by the Office of the Assistant Secretary of Defense for Research and Engineering (ASD(R&E)), in conjunction with representatives from the DoD Components. The ASD(R&E) is already charged with the development and oversight of defense policy and guidance for SSE, the Program Protection Plan Outline and Guidance [3], SwA, and HwA. The alignment of the JFAC with ASD(R&E) enables the JFAC to interact with SwA and HwA activities throughout the Department.

The JFAC Steering Committee is the governing body and provides senior-level management, oversight, and accountability for JFAC interests and concerns. Members of the Steering Committee currently include senior executive service level-representatives from the Office of the Under Secretary of Defense for Acquisition, Technology and Logistics; DoD Chief Information Officer; Departments of the Army, Navy and Air Force; Defense Information Systems Agency; National Security Agency; National Reconnaissance Office; Defense Microelectronics Activity; and Missile Defense Agency. Over time, the number of stakeholders may expand to take in additional defense organizations, issues and interests.

The JFAC currently includes three working groups and a coordination activity. The JFAC Action Officer Working Group is composed of senior staff from each organization within the JFAC Steering Committee, along with other members as approved by the JFAC Steering Committee. The JFAC SwA and HwA Technical Working Groups include subject matter experts representing the DoD service provider organizations and other technical expertise as needed. The JFAC Coordination Activity is composed of the JFAC Coordination Center (JFAC-CC) and representatives from the SwA and HwA service providers. The organizational structure is designed to facilitate open dialogue, coordination, and direct support for acquisition program managers from the federation of providers of SwA and HwA tools and services, throughout the life cycle of a program, with growing emphasis on sustainment.

Promoting Existing Assurance Capabilities

Each of the participating JFAC member organizations already manages an array of SwA and HwA capabilities and services as part of their normal program development, operations and support activities. Assembling these capabilities within a joint federated organization will bring about new opportunities to share information, promote best practices, prioritize and allocate scarce resources to address shared problems, and to inventory and license tools and resources. It will allow the organizations to standardize methods for identifying intelligence, research, development, and test and evaluation support for SwA and HwA interests and concerns.

Developing New Operational Concepts and Processes

The members of the JFAC working groups have already devoted considerable time and attention to developing a concept of operations for the federation that will encourage federation members to share information about their current SwA and HwA expertise, capabilities and capacities. For example, members can benefit from sharing information about relevant policies, standards, requirements, contract language, metrics, and procedures for acquiring, engineering, developing, testing, and evaluating trusted defense systems and services.

The members of the working groups are communicating with one another and their in-house service support organizations and other stakeholders about the roles and responsibilities of the federation in support of program offices, including applying the program protection planning process throughout the DoD acquisition life cycle. Improvements to the policy and guidance for SwA and HwA are being developed and will be applied at the next update of the Program Protection Plan Outline and Guidance, and evaluation criteria [4]. The JFAC member organizations are also developing individualized communication plans to outline process flows and methods for requesting services and support as part of the ongoing effort leading up to the declaration of Initial Operational Capability (IOC) for the JFAC.

At the declaration of IOC, which is expected to occur in the 4th quarter of calendar year 2015, the JFAC will be prepared to offer program management offices specific information about existing SwA and HwA service providers and capabilities, and guidance on how to plan and integrate these services and capabilities into their program management activities.

Assessing Capability Needs and Filling Gaps

Going forward from IOC to Full Operational Capability (FOC) over the next few years, the JFAC, in coordination with its member organizations providing SwA and HwA capabilities and services and related R&D efforts, will maintain a SwA and HwA capability map. The map will include a baseline of existing centers and capabilities of SwA and HwA services within the Department and elsewhere. The JFAC will identify and prioritize assurance capability gaps and will devise and recommend a strategy to validate and address such gaps. Potential gaps might include technical capabilities, resources and capacities, policy, assurance metrics, technical guidance, and program support tools or processes. If the necessary capabilities cannot be satisfied by existing centers and service providers, the JFAC working groups will make recommendations to the JFAC Steering Committee for consideration as the primary owners and users of assurance capabilities and services.

Fostering Cooperation

The JFAC is working with selected pilot programs nominated by their parent organizations to clarify the operational aspects of bringing together programs and assurance services without adding to the existing demands on program managers. The JFAC is committed to avoiding redundancy while helping programs identify and address SwA and HwA concerns that other quality control or testing activities might have overlooked. The pilots are looking at the Department's current SwA and HwA capabilities and interests and developing ideas regarding how the JFAC can best organize itself to support the needs of program managers, assurance service providers, and other stakeholders in an effective way.

The JFAC will align with and complement other SwA and HwA-related activities occurring in other parts of the Department, the U.S. government and industry, including the work of those involved in program protection, the DoD SwA Community of Practice, TSN, trusted suppliers, SCRM, systems engineering, SSE, and cybersecurity practice in the field, among others. The JFAC will work with and build upon these foundational activities to strengthen and promote trust and assurance in defense system hardware and software throughout the acquisition life cycle.

Promoting Trust and Assurance

In establishing its relationships with defense acquisition program managers and other stakeholders, the JFAC is committed to the following principles:

- A program's decision to participate in JFAC activities should be based on the need to bring about real and measurable improvement in the levels of trust and assurance for the program or system under development, throughout the life cycle of the program.
- The JFAC staff will seek to understand and adapt existing processes for providing SwA and HwA services to the programs to reduce the independent creation or reinvention of new processes and to control cost by blending-in best practices.
- The program's SwA and HwA needs should be specific, definable and measurable, and the assistance to be rendered by the JFAC should be within its established scope and set of capabilities.
- The JFAC will concentrate on identifying specific SwA and HwA areas of interest or concern that may not have been sufficiently addressed by program managers and other stakeholders.
- Although the JFAC's purpose is to share information, the JFAC does not intend to maintain sensitive information from programs and has established safeguards to protect sensitive program information against unauthorized release. The JFAC will share information only with those who have appropriate clearances, a need to know, and a responsibility for ensuring successful support and outcomes for the program and its stakeholders.

Supporting Needed Research and Technology Development

The JFAC is already making a positive difference in how the DoD advances SwA and HwA interests. As part of its initial assessment of existing SwA and HwA capabilities and gaps, the JFAC working groups identified several Department-wide needs for further research and technology development for SwA and HwA interests and concerns. The working groups recommended several technology development task proposals to the JFAC Steering Committee, which in turn approved and allocated funding. The results of these efforts will further the state-of-the-art for SwA and HwA facilities and organizations within DoD.

The JFAC Steering Committee also has allocated funding for analyses of SwA and HwA tools, techniques, and process. Tools such as the State-of-the-Art Resource (SOAR) for SW and HW, and the SOAR Matrix for existing SwA, provide guidance for selecting and using automated assurance tool sets across the DoD acquisition life cycle. The Steering Committee allocated funding to maintain and continue to improve the SOAR and other products of these DoD analyses for use by programs.

Engaging Other Communities of Interest and Practice

Moving forward, it is expected that the JFAC will continue to expand responsibilities to the full scope of the charter, including fostering closer cooperation with the academic community, private industry, and other federal government departments and agencies. Since R&D is a key component of JFAC operations, JFAC leaders will continue to identify, work with, and promote organizations dedicated to advancing innovative solutions for SwA and HwA inspection, analysis, detection, assessment, and remediation tools and practices.

Conclusion

DoD is establishing a joint federation of capabilities to support trusted defense systems and ensure the security of software and hardware developed, acquired, maintained, and used by the Department. As it continues to mature and develop, the JFAC will:

- Identify, operationalize, and institutionalize the Department's SwA and HwA capabilities in support of program management offices and other stakeholders.
- Evaluate the need for and impact of DoD investments in support of various SwA and HwA needs and interests.
- Collaborate across the DoD to influence R&D investments and bridge gaps in SwA and HwA capabilities.

Interested organizations are encouraged to contact the authors for more information about the JFAC.

ABOUT THE AUTHORS

Tom Hurt is the Deputy Director for Software Engineering and Software Assurance, ODASD(SE). He is the DoD lead for planning, development, and establishment of the JFAC.

Phone: 571-372-6129

Email: thomas.d.hurt.civ@mail.mil

Ray Shanahan is the Deputy Director for Anti-Tamper and Hardware Assurance, ODASD(SE). He is the DoD HwA lead supporting planning, development, and establishment of the JFAC.

Phone: 571-372-6558

Email: raymond.c.shanahan.civ@mail.mil

REFERENCES

1. Deputy Secretary of Defense. Policy Memorandum (PM) 15-001–Joint Federated Assurance Center (JFAC) Charter. Washington, D.C.: Department of Defense, February 9, 2015. <http://www.acq.osd.mil/se/docs/JFAC-Charter-Signed-9Feb2015.pdf>
2. Section 937of Public Law 113-66, National Defense Authorization Act for Fiscal Year2014. 113th Congress, December 26, 2014.<https://www.congress.gov/bill/113th-congress/house-bill/3304/text#toc-H68884858A3434A2A92CC2F59FEC83EB6>
3. Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). Program Protection Plan Outline and Guidance. Version 1.0. Washington, D.C.: DASD(SE), July 2011. <http://www.acq.osd.mil/se/docs/PPP-Outline-and-Guidance-v1-July2011.pdf>
4. Deputy Assistant Secretary of Defense for Systems Engineering (DASD(SE)). Program Protection Plan Evaluation Criteria. Version 1.1. Washington, D.C.: DASD(SE), February 2014. <http://www.acq.osd.mil/se/docs/PPP-Evaluation-Criteria.pdf>