



“Based upon threat and vulnerability reports from multiple sources, we took the proactive approach of putting into practice a process for the independent review of code being written by and for the Federal Aviation Administration. We wanted to stand up this capability quickly with very little overhead and within budgetary limits. The solution had to scale to the environment, provide actionable information, and maintain the integrity and security of the code it was reviewing. The Veracode model was able to meet those requirements.”

MICHAEL F. BROWN
Director & CISO, FAA

FAA Establishes Enterprise Software Vulnerability Assessment Program

Background

The Federal Aviation Administration’s (FAA) mission is to provide the safest, most efficient aerospace system in the world. The FAA is a large federated organization with multiple lines of business, and as with many large enterprises, it manages hundreds of applications. Contractors and subcontractors develop many of these applications, others are internally developed and modernized, and some integrate commercial-off-the shelf and open source software into the application. This enormous software portfolio has become a key foundation on which the FAA must insure the reliability and safety of the enterprise.

Business Challenge

The FAA is responsible for all aspects of the safety of civil aviation including the issuance and regulation of aircraft, Airspace and Air Traffic Control and Management systems, the operation of a network of airport towers and traffic control centers, and the operation and maintenance of Air Navigation Facilities. This includes radar, voice and data communications, and even the regulation of the U.S. commercial space industry. Security threats are growing and the focus of attacks are ever-evolving.

Industry studies such as one from U.S. CERT are finding that 90% of attacks are now at the software level and a 2009 government study found that 79% of attacks were at the application software level. The FAA understood this security risk and began looking for a way to establish a software security assurance program that could be standardized across its vast federation of departments and applications. The existing software assurance methods were not standardized from department to department, internal application security expertise varied widely, and software security compliance was not always required in contracts for externally developed applications. Creating an enterprise software assessment program was confounded by the simple fact that budgets were at best remaining steady if not being reduced.



“Not only FAA personnel benefited; but our contractors also see the benefit that they can independently validate how software assurance is built into their software.”

MARY HORN

Office of Information Systems
and Security (ISS) Compliance
Officer and Software Assessment
Program Manager, FAA

Program Goals

For an organization as large and diverse as FAA there were many goals to meet to create a software vulnerability assessment program and to select a supplier for these requirements. Goals of the program included:

- **Ease and cost effective enterprise scalability:** While identification and reduction of risk was the paramount concern, cost and maintenance of software, hardware, and training across the enterprise—the total cost of ownership—could not be ignored.
- **Ability to address a wide range of use cases:** The FAA needed a complete solution that covered internally developed applications, contractor developed applications, COTS (Commercial Off-the Shelf) purchased applications, GOTS (Government Off-the-Shelf), as well as Open Source packages that are used in many FAA information systems.
- **Automating code reviews with multiple technologies:** The FAA needed the ability to scan using multiple techniques (including both static binary analysis and dynamic web analysis) for the evaluation and assessment of software.
- **Ability to assess a large base of application languages and platforms:** The FAA needed the capability of covering the large number of programming languages (C++, Java, .Net, Cold Fusion as examples), operating systems, and platforms that comprise the diverse portfolio of applications.
- **Providing an independent code review based on industry standards:** The solution needed to be an independent source of assessment. The FAA wanted to work with a vendor that keeps their assessment tool current with the evolving threat based on federal and industry standards. Security assessments need to comply with the standards from the NIST National Vulnerability Database (NVD), and the discovered threats mapped to industry standards such as the Common Vulnerability Scoring System (CVSS) and the Common Weakness Enumeration (CWE).
- **Integration into FAA processes without major changes:** The solution should fit easily into current internal certification and accreditation processes and integrate easily into the many different Software Development Life Cycles (SDLC) used across the enterprise.
- **Maintain security and confidentiality:** The solution needed to insure that any externally supplied application was protected against unauthorized physical and logical access. In addition, assessment results needed to be protected from unauthorized access.

The software code assessments identified security risks in software across the FAA—outsourced code, legacy code, third-party code, and open source code. As a result of the compelling findings from the initial use of Veracode, the FAA issued a revised standard policy on software assurance. The policy addressed the independent assessment and use of multiple techniques for compliance with the order that applies to contractor developed and Open Source projects to be included in FAA operations. Moving forward, the FAA plans to expand the use of these techniques and policy in all of its certifications and accreditations.

Results and Lessons Learned

The Veracode solution also gave the FAA two other capabilities that provided value. The first was eLearning—online tools and training—where developers can learn how to write secure code. The second was access to the Veracode online Open Source Ratings Database where Open Source projects have been assessed. According to Mary Horn, FAA Project Manager, “The Rating Database is becoming a valuable tool when acquiring or integrating open source applications within the agency.”

The benefits were realized quickly. An enterprise program was up and running in a few weeks without hardware, software, or consultants. And within one month offices from across the FAA were submitting applications for code review, remediating vulnerabilities, and engaging in on-going training to keep updated with changing application security threats.



Veracode, Inc.
4 Van de Graaff Drive
Burlington, MA 01803

Tel +1.781.425.6040
Fax +1.781.425.6039

www.veracode.com

© 2011 Veracode, Inc.
All rights reserved.