

Security in Numbers: NMCI Compliance and the Need for Practical Secure Code Review

Ounce Labs

Contact:

Andrew Bochman

Director of Federal Markets

781-290-5333 x30

andy.bochman@ouncelabs.com

ABSTRACT:

As the saying goes, you can't manage what you can't – or don't – measure. Due to a lack of consistent and reliable application security metrics, Information Assurance technology decisions are too often made based on “best guess” analysis. At best, this results in redundant control systems. At worst, too little security where it's needed most. As part of the transition to NMCI, the determination must be made as to which applications comply with NMCI security criteria. This includes a precise, reliable measurement of the security of the organization's critical applications, information which can only be achieved through a thorough security source code review.

Historically, source code review has been a costly and time-consuming manual process. It requires significant commitment of team or contracted resources, and involves the focused attention of qualified security experts for weeks or months per application. For new applications, attempts to insert this process into the development lifecycle can add substantial cost and delay deployment. As a result, it has been neither practical nor feasible for most organizations to assess the security of more than a sample group of their applications.

However, there are now several categories of automated security tools which aid and expedite the security analysis of applications, allowing review teams to maximize their efficiency and focus their efforts on discovering design flaws and fixing the discovered security vulnerabilities.

This presentation will offer information assurance decision-makers and application owners an overview of current strategies and technologies to:

- * Most effectively analyze and report on critical applications
- * Use vulnerability metrics to help determine which applications are written most (and least) securely
- * Speed time to production by discovering and eliminating vulnerabilities earlier in the development lifecycle
- * Set a maximum acceptable security baseline for both in-house and outsourced applications
- * Realize the maximum security ROI from their investments

By analyzing source code for security vulnerabilities, organizations can quickly and cost-effectively gain insight into the security status of Navy and Marine Corps applications. Furthermore, a better understanding of vulnerabilities in key applications can also lower software security costs and help determine where to deploy more stringent security solutions based on application vulnerability and criticality to the organization and mission.