IDA | Research Insights

June 2018

SOAR to Better Quality and More Secure Software

David A. Wheeler (dwheeler@ida.org)

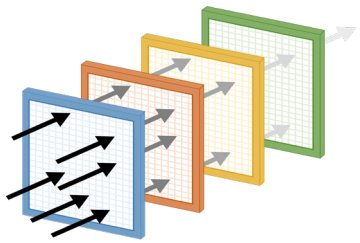
IDA researchers developed the Software Assurance State-of-the Art Resource (SOAR), which includes a process for selecting and reporting the results of software analysis tools and techniques. The SOAR assists Department of Defense (DoD) program offices in selecting the appropriate tools for informing decisions about software assurance and supply-chain risk-management efforts, as well as decisions that affect the development of software policy. Using the SOAR to select software analysis tools for identifying and removing weaknesses in software can help protect critical DoD programs.

Selecting the right tools is key to determining and reducing software risks. Although software can provide functionality, it can also introduce vulnerabilities that contribute to cybersecurity risk. Cybersecurity is a requirement for, and must be implemented across, the life cycle of DoD programs, systems, and information. Analyzing DoD's software to identify and remove vulnerabilities is critical to program protection. However, using only manual analysis techniques is costly and slow, leading to ineffective software analysis.

Software analysis tools can find vulnerabilities so that they can be fixed before attacks exploit them, but selecting the right tool is difficult given users' lack of knowledge about available software analysis tools. The SOAR addresses these issues by enabling better tool choices, more effective testing, and enhanced software security.

The SOAR is a powerful aid in selecting the best software analysis tools and reporting their results. Different tool types are better at addressing different technical objectives. The SOAR includes a matrix that shows which technical objectives can be met by which types of tools and techniques. It also allows planners and engineers to select and use the appropriate tools.

The SOAR identifies over 50 types of tools and techniques available for analyzing software, grouped into three categories—static analysis, dynamic analysis, and hybrid analysis. Using a variety of tools and techniques reveals more vulnerabilities. Applying the tools identifies, and allows for correction of, more weaknesses. It also reveals where more testing is necessary and additional tools are needed.



The figure is a conceptual illustration of the advantages of using multiple tools and techniques, particularly when they use different approaches. The arrows represent potential risks, including exposed vulnerabilities in the software, and the screens represent the applied tools and techniques.

Using multiple tools and techniques is necessary for secure software. The SOAR clearly shows that no one type of tool or technique solves all security issues. Instead, using multiple types of tools increases the likelihood that vulnerabilities will be found before attackers can exploit them. Programs have to determine proactively their objectives, select the appropriate tools to meet those objectives, and apply those tools and repair the issues they find. Doing so leads to better quality and more secure software.

Based on IDA P-8005, *State-of-the-Art Resources (SOAR) for Software Vulnerability Detection, Test, and Evaluation 2016*, D. A. Wheeler and A. E. Henninger, November 2016. Research sponsored by the Office of the Deputy Assistant Secretary of Defense for Systems Engineering.

NS D-9126

4850 Mark Center Drive
Alexandria, VA 22311-1882
ida.org