Automated Assessment Tools and the Software Assurance Marketplace (SWAMP)

James A. Kupsch, University of Wisconsin, kupsch@cs.wisc.edu

Description
Software assurance tools – tools that scan the source or binary code of a program to find weaknesses – are the first line of defense in assessing the security of a software project. These tools can catch flaws in a program that can affect both the correctness and safety of the code. This tutorial is relevant to anyone wanting to understand how those tools work, and learn how to use these automated assessment tools to minimize security flaws in the software they develop or manage.

We will start with basic background material about how these assessment tools work, so that the student can understand the capabilities and limitations of such tools. We then focus on a selection of both commercial and open source tools for C/C++ and Java, and demonstrate how to apply them to sample programs with known flaws. Next we demonstrate the SWAMP (https://continuousassurance.org) and how it simplifies the application of tools and allows users to view results from multiple tools.

Targeted Audience: The target audience for this tutorial is anyone involved with the development, deployment, assessment, or management of critical software.

Content level: 50% beginner, 25% intermediate, 25% advanced.

Tutorial length: 1.5 hours

Audience prerequisites: To gain maximum benefit from this tutorial, attendees should be familiar with the process of developing software and at least one of the C, C++ Java or scripting programming languages. This tutorial does not assume any prior knowledge of security assessment or vulnerabilities.