

Software Engineering Research Center (SERC)

Ball State, Wayne Zage, Director, 765.285.8664, wmzage@bsu.edu

Ball State, Kirsten Smith, 765.285.1889, kirstensmith@bsu.edu

Purdue, Aditya Mathur, 765.494.7823, apm@cs.purdue.edu

West Virginia University, Don McLaughlin, 304.293.0405x2514, don.mclaughlin@mail.wvu.edu

Center website: <http://www.serc.net/web/index.asp>

Provably Secure Software Systems Development through Security Typed Languages



This work has extended security-typed languages from the realm of theoretical programming language tools to an apparatus for building secure software systems. Researchers at the Software Engineering Research Center have developed software engineering practices and tools that allow mapping of high-level security goals into the applications that must realize them in a secure-typed language. These tools have been used to develop provably secure large-scale security-labeled email systems, as well as other secure systems. Past software security

techniques have attempted to isolate applications (as seen in sandboxing techniques), introspect possible vulnerabilities (as in static and dynamic analysis tools), or apply formal analysis to achieve high assurance applications. However, such approaches are often ad hoc, incomplete or difficult to use.

This work has addressed these past limitations by identifying, formalizing, and automating the complex processes of identifying security relevant data and its potential for leakage or corruption. In so doing, usable infrastructures are available for defining and developing provably secure software. This work advances the state of the art in software systems development by providing guaranteed compliance with security goals. Further efforts have identified new algorithms for important problems such as security level inference and credentials discovery. Such discoveries are being used not only in security typed languages, but are also helping the operating systems community to define policies and services tailored to the security requirements of applications. This will significantly enhance the capabilities of commercial software developers to articulate and realize security goals. The researchers are working with Motorola to evaluate how the tools can be used to make applications of embedded devices such as cellular phones more secure. For more information, contact Dr. Patrick McDaniel at The Pennsylvania State University, 814.863.3599, mcdaniel@cse.psu.edu.

