Final Progress Report for Award FA9550-06-1-0313

Project: Trace Effect Analysis for Software Security
PI: Dr. Christian Skalka
The University of Vermont, Burlington, VT 05405

February 28, 2010
We developed combined run-time and compile-time analyses for enforcing trace based safety properties in higher order and Object Oriented programs, called trace effect analysis. Traces are the ordered sequence of events generated by programs. A wide variety of interesting language safety mechanisms can be expressed as trace properties, such as access control, resource usage protocols, and context sensitive flow analysis. Consequently, our analyses provide a uniform framework for automatically enforcing a large class of safety properties, which can be specialized for particular applications. Formal type theory underlies most of these analyses. We have also developed new program logics for defining access control policies. Based on temporal logics, they allow for the specification and verifiable enforcement of sophisticated security policies, and are especially useful in distributed contexts.
Status of Effort

This research project has been completed, and was productive and successful. We have published work establishing a rigorous theoretical foundation for our static analysis enforcing temporal properties of programs. We have extended our basic analysis to richer language models, incorporating object oriented features such as object hierarchies and dynamic dispatch. We have also performed research on authorization logics, which allow definition of highly expressive security policies. Aside from its inherent interest, this work has also led to a new research project in software security for embedded systems that is now funded under an AFOSR YIP award.

Accomplishments

Our research has made four basic contributions. First, we have shown that temporal program logics can be integrated with type analysis to enforce temporal program properties at compile time. Second, we have shown that our analyses are scalable to object oriented models. Third, we have developed new foundations for increasing practical applications of trust management systems. All of these results enhance the foundations of software security, especially software for execution in distributed environments. They lead also to our fourth contribution, which is an underpinning of new research in programming language-based security for embedded systems via type safe staged programming. Papers reporting work on this project have been published in high-profile, highly respected venues such as the Journal of Functional Programming and ACM Computing Surveys.

Personnel Supported

This grant provided Summer support for the PI during 2006, 2007, and 2008. It supported a PhD student during the 2007/2008 school year, and a postdoctoral researcher from November 1, 2007 to May 1, 2009. The grant also supported travel to conferences by the PI and funded personnel was also supported.

Publications

During the grant period the PI has (co-)authored a number of papers relevant to supported research. Following are highlights.


Interactions: Presentations

During the grant period the PIs research has been presented at the following venues.