Type-driven Gradual Security Typing

Ronald Garcia

Abstract:
Information-flow security-typed programming languages use types to statically enforce noninterference between potentially conspiring values, such as the arguments and results of functions. But to adopt static security types, like other advanced type disciplines, programmers must adopt the discipline wholesale.

To provide a gentler path to security typing, researchers have designed languages that blend static and dynamic checking of security types. Unfortunately most of these languages support static, type-based reasoning about noninterference if programs are entirely statically secured. This limitation substantially weakens the benefits that dynamic enforcement brings to static security typing.

This talk describes GSLref, a security-typed higher-order language that supports gradual migration between a simple type discipline and security type discipline, using the principles underlying gradual typing.

GSLref satisfies most of the criteria set forth by Siek et al. for gradually-typed languages. The one exception, called the "dynamic gradual guarantee" cannot be satisfied without violating noninterference.

To realize this design, we were led to draw a sharp distinction between syntactic type safety and semantic type soundness, each of which constrains the design of the gradual language.

Bio:
Ronald Garcia is an associate professor of Computer Science at the University of British Columbia. His research investigates how fundamental concepts in the theory, implementation, and practice of programming languages can improve the software development process.
His research has focused on static and dynamic type-based reasoning, metaprogramming, and generic programming.

Prior to his appointment at UBC, he was a Computing Innovation Fellow at Carnegie Mellon University and Postdoctoral Fellow at Rice University. He received a PhD in Computer Science from Indiana University, and an MSc and BSc in Electrical Engineering from the University of Notre Dame.