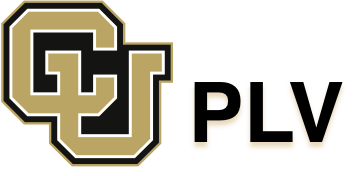
Be inspired.

Programming Languages and Verification Seminar

****

**­**

Behavioral Contracts and Security

­

Christos Dimoulas

Postdoctoral Fellow, Harvard University

ECCR 151

Tuesday, October 7, 2014

11:00 a.m. to 12:00 p.m.

Behavioral contracts are a widely used specification tool for software components, which enrich interface information with logical assertions. The rigorous enforcement of contracts provides to programmers precise guarantees about a program's execution, and offers useful feedback for debugging upon contract violations. However, almost all of research on contracts focuses on contracts as a specification tool for partial correctness of programs and ignores another vital requirement of modern software; security.

In this talk, I will demonstrate how contracts can specify and enforce security policies. Specifically, I will focus on two applications of contracts in capability-based security. First, I will describe Shill; a secure shell scripting language where contracts specify and enforce policies about which OS resources scripts intend to use and how they use them. This way, Shill's contracts help script authors and users to adhere to the principle of least privilege. Second, I will present a contract system that complements the contract system of Shill by describing and enforcing declarative policies for the flow of capabilities between components. This manner, components can specify not only what capabilities they require from their users, but also how they intend to share these capabilities with other components.

**Christos Dimoulas** is a Postdoctoral Fellow in Computer Science at the School of Engineering and Applied Sciences of Harvard University working with Stephen Chong and his group. Before coming to Harvard, Christos completed a PhD in Computer Science at the College of Computer and Information Science of Northeastern University under the supervision of Matthias Felleisen. Christos is interested in the design and semantics of programming languages. More specifically, his goal is to develop programming languages technology that facilitates the construction of secure and robust component-based software systems.

**Hosted** by Bor-Yuh Evan Chang (bec@cs.colorado.edu).



*­*

**