Bio:
Frederico Araujo is a PhD candidate in Software Engineering at the University of Texas at Dallas, where he has been working on deception-based software defenses with Dr. Kevin Hamlen. His research interests are in applied systems and software security, with a focus on language-based approaches. His PhD work has introduced a new architecture and programming language support for engineering applications with deceptive response capabilities against targeted attacks. Three of his papers have won best paper awards, including the NYU-Poli Best Applied Security Research Paper Award (2014). He has interned with IBM Research at the T.J. Watson Research Center, and has held industrial software engineering positions, most recently at Siemens. While at UT Dallas, he has received the Ericsson Graduate Fellowship and a departmental Outstanding Achievement Award. Frederico holds a BS (2007) from the University of São Paulo, Brazil, and a MS (2008) from the Ecole Centrale Paris, France.

Abstract:
In this talk I will introduce my research on a new science of language-based software cyber deception, featuring a suite of new technologies that arm live, commodity server software with deceptive attack-response and disinformation capabilities. These new capabilities mislead adversaries into wasting precious time and resources on phantom vulnerabilities and decoy systems, making cyber attacks significantly more costly and risky for their perpetrators, and giving defenders more time and opportunity to detect and thwart incoming attacks. To this end, I will present a new abstraction that makes software security patches invisible to attackers, and explain its implications for research in software architecture, compiler techniques, programming language theory, and program analysis.