USNA Math Department Colloquium

# *Introducing Mango: A Formal Eclipse plugin for Java Vulnerability Detection*

Frank Rimlinger (NSA)

Date: Tuesday, 9 April 2013

Time: 1545-1645

Location: Chauvenet 110

**Abstract:** Oracle has documented numerous security vulnerabilities which may inadvertently be introduced into code by Java programmers. Mango is an open-source Eclipse workbench plugin for detecting such vulnerabilities. Mango first builds a formal model of targeted code, using a custom language with roots in Lisp and ACL2. This model is exposed at a high level as Eclipse FormText, a familiar browser idiom. Model browsing enables the capture and generalization of low-level formal expressions in the model language. From this technique, a methodology emerges for vulnerability test development: a)write code exhibiting a security flaw, b) capture and generalize the "sweet spot" where the vulnerability causes undesirable behavior, and c) write rules to match against captured patterns in order to detect the vulnerability in arbitrary java code. This talk discusses the formal model and test development life-cycle, as well as questions of efficiency and training.

**Biography:** Frank Rimlinger (frankrimlinger@gmail.com) received his Ph.D. from the University of California at Berkeley, 1985. He worked for ten years as a research mathematician in the field of Combinatorial Group Theory and Low-Dimensional Topology. His thesis was published as AMS Memoir 361, Pregroups and Bass-Serre theory. Frank joined the National Security Agency in 1995, and for the last twelve years has worked in the field of software assurance. He is the inventor of US Patent 7,788,659 B1, Method of converting computer program with loops to one without loops. In 2007 this technology was transferred to the NASA Software Release Authority, and is currently available as an open-source technology, the high-assurance software tool Mango, under the NOSA 1.3 license (NASA Open Source Agreement).