Concordia University
ENCS
Engineering & Computer Science

Concordia Institute for Information Systems Engineering

THE CONCORDIA INSTITUTE FOR INFORMATION SYSTEMS ENGINEERING IS PLEASED TO PRESENT THE FOLLOWING GUEST LECTURE

Dr. Jean Goubault-Larrecq, Professor and Head, SECSI
École Normale Supérieure de Cachan and INRIA
France

ORCHIDS and Bad Weeds

ORCHIDS is an intrusion detection tool based on techniques for fast, on-line model-checking. ORCHIDS detects complex, correlated strands of events with very low overhead in practice, although its detection algorithm has worst-case exponential time complexity. The purpose of this work is twofold. First, we explain the salient features of the basic model-checking algorithm in an intuitive way, as a form of dynamically-spawned monitors. One distinctive feature of the ORCHIDS algorithm is that fresh monitors need to be spawned at a possibly alarming rate. The second goal is therefore to explain how we tame the complexity of the procedure, using abstract interpretation techniques to safely kill useless monitors. This includes monitors which will provably detect nothing, but also monitors that are subsumed by others, in the sense that they will definitely fail the so-called shortest run criterion. We take the opportunity to show how the ORCHIDS algorithm maintains its monitors sorted in such a way that the subsumption operation is effected with no overhead, and we correct a small, but definitely annoying bug in its corealgorithm, as it was published in 2001.

Jean Goubault-Larrecq was born in Rouen, France, in 1965. He studied at École Polytechnique, (France) then at the Corps des Mines; he received his Ph.D. from École Polytechnique, (France) in 1993 and his habilitation in 1997. He worked at the research center of Bull S.A. for ten years, was invited researcher at the University of Karlsruhe in 1996, worked as research engineer then project director at Dyade, a common technology transfer venture between Bull and INRIA, from 1996 to 2000. He is currently full-time professor of computer science at the École Normale Supérieure de Cachan, and head of the SECSI (Securité des Systèmes d'Information) project at INRIA Saclay. He currently teaches programming and semantics, complexity theory (both introductory and advanced), lambda-calculus and logic. His research domains include automated deduction, formal specification, models and methods for cryptographic protocols, intrusion detection, proof theory and modal logics, linear logic, algebraic topology in computer science, and, more recently, semantic models for mixed non-deterministic and probabilistic choice.

Wednesday, October 29th, 2008

4:00 P.M.

EV003.309