SSIRI 2010: Keynote Speakers

Jim Woodcock
University of York, UK

Modeling and Implementing Complex Systems with Timebands

Abstract

We describe how to use a timeband architecture to model real-time requirements. The architecture separates requirements that use different time units, producing a family of models. Each model is characterized by its granularity and precision. These models are then linked using superposition, a kind of event refinement, and a loose synchronization of their time units, with respect to their precision. Our models are written using CSP and checked using the FDR model checker. More complicated models use Circus, the state-rich process algebra. We show how to implement such a timeband architecture using the JCSP Java class library.

Biography

Professor Jim Woodcock holds the Anniversary Chair in Software Engineering at the University of York. Previously, he was Professor of Software Engineering at the University of Oxford, where he founded the Centre of Excellence in Software Engineering. His current research interests include industrial-scale software engineering, unifying theories of programming, railway signaling, hybrid control systems, and model checking state-rich concurrent systems. His research team won the Queen's Award for Technological Achievement in 1992 for its work with IBM. He was the academic consultant for the first product certified to Information Technology Security Evaluation Criteria (ITSEC) Level E6 (in 1998), and served for over ten years as an advisor on secure systems to the British and US governments. In 2002, he won the Rudolf Christian Carl Diesel Prize from the Society for Design and Process Science. He is the Chair for UK-CRC's Grand Challenge 6 "Dependable Systems Evolution" and Joint Editor-in-Chief of Formal Aspects of Computing Journal; he has served on over sixty international conference program committees, and has chaired fifteen of them. He has given invited papers and keynote speeches at over thirty conferences, and is the author of nearly 200 scientific papers and books. He is a Chartered Fellow of the BCS. He has acted as a consulting software engineer for many organizations, including British Energy, DEC, General Dynamics, IBM, LDRA, Logica, QinetiQ, and the UK Health & Safety Executive.

Tim Grance
Program Manager
NIST, USA

Defining, Securing, and Standardizing Cloud Computing

Abstract

The presentation will discuss the NIST definition of cloud computing. It will then use that definition as a foundation upon which to discuss security advantages and challenges of cloud computing. Then the need for interoperability and portability will be highlighted with a discussion of the state of cloud computing standards and possible future directions. Finally, the presentation will further suggest steps that industry, government, and academia might take to accelerate and adopt viable standards in support of security, privacy, portability, and interoperability.

Biography

Tim Grance is a senior computer scientist in the Information Technology Laboratory at the National Institute of Standards and Technology. He leads a team of researchers in the Systems and Network Security Group and is engaged in a broad research program focused on such topics as cloud computing, access control, identity management, vulnerability analysis, privacy protections, security metrics, protocol security, smart cards, and wireless/mobile device security.

He is also the Program Manager for Cyber and Network Security (CNS) Program and exercises broad technical and programmatic oversight over the NIST CNS portfolio. This portfolio includes high profile projects such as the NIST Hash Competition, Cloud Computing, Security Content Automation Protocol (SCAP), Protocol Security (DNS, BGP, IPv6), Combinatorial Testing, and the National Vulnerability Database.

He has extensive public and private experience in accounting, law enforcement, counter-intelligence, and computer security. He has written on diverse topics including incident handling, intrusion detection, privacy, metrics, contingency planning, forensics, and identity management. He was named in 2003 to the Fed 100 by Federal Computer Week as one of the most influential people in Information Technology for the US Government. He is also is a two-time recipient of the highest award from the US Department of Commerce - a Gold Medal, from the Secretary of Commerce.

Jim Davies
Kellogg College
University of Oxford, UK

Once more, with meaning: a grand challenge in informatics

Abstract

In most applications of information technology, the limiting factor is neither computational power nor storage capacity; nor is it connectivity. Hardware can be obtained at commodity prices, and software infrastructure can be downloaded free of charge. The limiting factors are the costs of consistency, coordination, and correctness: in software development, in systems integration, and in continuing interaction with users. In this talk, we will explore how the use of semantic technologies, formal techniques, and model-driven engineering can greatly reduce these costs, and thus increase the quality, interoperability, and suitability of information technology applications.

Biography

Jim Davies is Professor of Software Engineering at the University of Oxford. He directs a program of advanced, professional education in software engineering, teaching advanced techniques to people working full-time in industry. He leads a team of researchers developing and applying semantic technologies, formal techniques, and model-driven engineering in clinical informatics, enterprise computing, and electronic governance. He is an advisor to Cancer Research UK and to the UK Medical Research Council. In 2010, he is chair of the International Conference in Distributed Computing and Internet Technology (ICDCIT), co-chair of the Brazilian Formal Methods Symposium (SBMF), and co-chair of the leading international forum in electronic governance (ICEGOV).

Wei-Ngan Chin
National University of Singapore

Software Verification via Separation Logic

Abstract

Despite their popularity and importance, pointer-based programs posed a major challenge for software verification. In this talk, we present a specification mechanism that is precise, concise and modular for automated verification of pointer-based programs. Our approach is built on top of separation logic that follows from pioneering works by Reynolds and O'Hearn.

We focus on the development of a modular specification mechanism that can be used to provide both automated and scalable verification. Key features of our approach includes the following. It can verify data structures with complex invariant properties. It provides a unified view of control flows that captures both multiple returns and exceptions. It can support more precise reasoning through structured specifications and path-sensitive error tracing. Last, but not least, we develop a way to decompose specifications into smaller fragments for more scalable verification. Our approach

has been successfully applied to verify medium-sized programs from the imperative and object-oriented programming paradigms. Our verification methodology is being aimed at programs developed from mainstream programming languages.

Biography

Wei-Ngan Chin received his BSc and MSc in Computer Science from the University of Manchester and a PhD in Computing from Imperial College, London. He is an Associate Professor in the Department of Computer Science, National University of Singapore.

His research interests are in programming languages and software engineering. He has worked on program analyses and verification techniques that are aimed at improving clarity, reliability and reusability of software. His recent research topics include software verification, memory resource analysis, OO genericity and inference on pre/post conditions. He currently leads a funded project on "Specification and Verification for Future Programmers".