Layered Assurance Workshop

KEYNOTE AND INVITED SPEAKERS

2013 Layered Assurance Workshop

December 9-10, 2013

Hyatt French Quarter, New Orleans, Louisiana, USA

Affiliated workshop of the
29th Annual Computer Security Applications Conference (ACSAC)

Contract-based Design: a Temporal Logics Approach

Alessandro Cimatti
Fondazione Bruno Kessler

Time: 08:45
Date: December 9th 2013

Abstract

Contract-based design is an emerging paradigm for the design of complex systems, where each component is associated with a contract, i.e., a clear description of the expected behaviour. Contracts specify the input-output behaviour of a component by defining what the component guarantees, provided that its environment obeys some given assumptions. The ultimate goal of contract-based design is to allow for compositional reasoning, stepwise refinement, and a principled reuse of components that are already pre-designed, or designed independently.

In this talk, a novel, fully formal contract framework is presented. The decomposition of the system architecture is complemented with the corresponding decomposition of component contracts. The framework exploits such decomposition to automatically generate a set of proof obligations, which, once verified, allow concluding the correctness of the top-level system properties. The framework relies on an expressive property specification language, conceived for the formalization of embedded system requirements. The proof system reduces the correctness of contracts refinement to entailment of temporal logic formulas, and is supported by a verification engine based on automated SMT techniques.

The approach has been implemented in the OCRA tool, and has been applied in several research projects (FOREVER, AFECER and D-MILS) for the development of complex systems in various application domains.

Biographical Sketch

Alessandro Cimatti is a senior researcher at Fondazione Bruno Kessler, Trento, Italy, where he leads the research unit in Embedded Systems at the Center for Information and Communication Technologies. His research interests concern formal verification of industrial critical systems, methodologies for design and verification of hardware/software systems, decision procedures and their application, safety analysis, diagnosis and diagnosability.

Cimatti has published more than one hundred and thirty papers in the fields of Formal Methods and Artificial Intelligence. He has co-chaired the FMCAD and SAT conferences, and has been member of the Program Committee of the major conferences in computer-aided verification and artificial intelligence.

Cimatti is also interested in the development of software tools for verification (including the MathSAT SMT solver and the NuSMV model checker), and in their technology transfer. Cimatti has been the leader of several technology transfer projects in related fields, including projects funded by the European Space Agency and the European Railways Agency.

Layered
Assurance
Workshop

Compositional Specification and Verification of a Hypervisor OS Kernel

Zhong Shao
Yale University

Time: 15:30
Date: December 9th 2013

Abstract

Operating System (OS) kernels and hypervisors form the backbone of all system software. They can have the greatest impact on the resilience, extensibility, and security of today's computing hosts. Recent effort on formal verification of the seL4 kernel has demonstated the feasibility of building large scale formal proofs of functional correctness for a general-purpose microkernel, but the cost of such verification is still prohibitive, and it is unclear how to use such a verified kernel to reason about user-level programs and other kernel extensions.

In this talk, I'll present a new compositional approach for formally specifying and verifying OS kernels. Because the very purpose of an OS kernel is to build layers of abstractions over bare machine resources, we insist on uncovering and specifying these layers formally and then performing the verification of each kernel function at its proper abstraction layer. To support linking with other kernel extensions and user-level programs, we prove a stronger contextual refinement property for every kernel function, which states that the implementation of each such function will behave like its functional specification under any (kernel or user) program context. All our abstraction layers are defined as assembly-level machines extended with abstract kernel primitives, but almost all our kernel programs are written in a variant of CompCert Clight language, verified at the source level, and compiled and linked together using a modified version of the CompCert compiler. To demonstrate the effectivess of our new methodology, we have successfully implemented and specified a realistic hypervisor OS kernel and verified its (contextual) functional correctness property in the Coq proof assistant. Our hypervisor kernel is written in 3000 lines C and x86 assembly, and can successfully boot a version of Linux as a guest. The entire specification and proof effort took less than one person year.

Biographical Sketch

Zhong Shao is Professor of Computer Science at Yale University. He earned his PhD in Computer Science from Princeton University in 1994. During his early career, he was a key developer and author of many compilation phases used in the Standard ML of New Jersey compiler, and also one of the first to build a type-based intermediate representation in a functional-language compiler (FLINT). During the last decade, Shao and his FLINT group at Yale have led and pioneered work on certified software and proof-carrying code, certified low-level programming, language-based approaches to safety and security, and proof assistants and formal methods. He is currently a PI on the DARPA CRASH CertiKOS project and a Co-PI on the DARPA HACMS Robotics Security project.

Layered
Assurance
Workshop

An Integrated Approach to Safety and Security based on Systems Theory

Nancy Leveson
Massachusetts Institute of Technology

Time: 08:45
Date: December 10th 2013

Abstract

Safety and security have traditionally been treated as different problems. Both fields are based on very old models of accident causation that no longer are a good fit for our increasingly complex and software-intensive systems. In this talk, I will describe a new approach to safety, based on systems theory, that treats safety as a control problem rather than a component reliability problem. The same approach is applicable to security and provides the possibility of integrating the analysis methods used for both of these emergent system properties. Just as applying the new systems-theoretic model represents a major paradigm change for safety engineering, it has the potentially for a very different but much more powerful approach to security

Biographical Sketch

Dr. Nancy Leveson has worked in the field of system safety for 30 years. Currently she is Professor of Aeronautics and Astronautics and also Professor of Engineering Systems at MIT. Previously she was Boeing Professor of Computer Science at the Univ. of Washington. She is an elected member of the National Academy of Engineering (NAE) and has received many awards for her research on system safety and software engineering. She has published over 200 research papers and is author of a book, *Safeware: System Safety and Computer*s, published by Addison-Wesley and translated into Japanese and a new book *Engineering a Safer World* published by MIT Press in 2012 and currently being translated into Chinese and Japanese.

Prof. Leveson consults extensively in many industries, including aerospace, transportation, chemical plants, medical devices, nuclear power, hospitals, and oil and gas production. She served on the NASA Aerospace Safety Advisory Panel and the Baker Panel investigating safety culture in the Texas City Oil Refinery explosion and has been involved in many accident investigations including serving as an expert advisor to the Columbia Accident Investigation Board and the Presidential Oil Spill Commission (Deepwater Horizon).

Layered
Assurance
Workshop

Explaining Certification

John Rushby
Computer Science Laboratory, SRI International

Time: 15:30
Date: December 10th 2013

Abstract

Software certification for safety seems to be effective in some industries: there have been no serious accidents due to software in commercial aircraft or nuclear power, for example. But it is not at all clear why or how the processes underlying software certification achieve their effectiveness. The guidelines for assurance of aircraft software, for example, are about correctness, not safety. Furthermore, certification requires an inverse relationship between the severity and the likelihood of possible failure conditions, but certification is based on doing more correctness-based assurance for software whose faults could provoke more severe failure conditions, and it is not obvious how more correctness assurance leads to a lower rate or probability of failure.

This talk will offer an explanation how the processes of software assurance do provide a credible basis for the quantification of failure that underlies certification.

This is based on work with Bev Littlewood, Andrey Povyakalo, and Lorenzo Strigini of City University, UK.

Biographical Sketch

John Rushby is a Program Director and SRI Fellow with the Computer Science Laboratory of SRI International in Menlo Park California, where he leads its research program in formal methods and dependable systems. His research interests center on the use of formal methods for problems in the design and assurance of safe, secure, and dependable systems.

Dr. Rushby joined SRI in 1983 and served as director of its Computer Science Laboratory from 1986 to 1990. Prior to that, he held academic positions at the Universities of Manchester and Newcastle upon Tyne in England. He received BSc and PhD degrees in computing science from the University of Newcastle upon Tyne in 1971 and 1977, respectively.

Dr. Rushby is a former associate editor for Communications of the ACM, IEEE Transactions on Software Engineering, and Formal Aspects of Computing, and was recently a member of a National Research Council study that produced the report "Software for Dependable Systems: Sufficient Evidence?". He is the 2011 recipient of the IEEE Computer Society's Harlan D. Mills Award "for practical and fundamental contributions to Software & Hardware Reliability with seminal contributions to computer security, fault tolerance, and formal methods".