Layered Assurance Workshop

KEYNOTE AND INVITED SPEAKERS

2012 Layered Assurance Workshop

December 3-4, 2012

Buena Vista Palace Hotel & Spa, Orlando, Florida, USA

Affiliated workshop of the
28th Annual Computer Security Applications Conference (ACSAC)

Hypervisor Verification and Theory of Multi Core Systems

Wolfgang Paul

Time: 8:45
Date: Dec 3rd 2012

Abstract

Let I be the instruction set architecture (ISA) of a multi core processor, e.g. X64, POWER, ARM.

A mathematical correctness proof of a hypervisor for instruction set architecture I has to provide 3 things:

1) a specification of the hypervisors function. Among other things hypervisors provide a simulation of many processors of ISA I by one processor of ISA I.
2) a semantics of the programming language, in which the hypervisor is coded. This is usually an extension of parallel C for system programming (whatever parallel C is).
3) a proof that the code satisfies the specification. Once computational models are clear this is almost an 'ordinary' simulation theorem. In case the proof is mechanized in a formal proof tool one should also provide
4) a soundness proof of the (extended parallel) C verifier used. Such verifiers must inject proof obligations, which are completely unintuitive without a detailed understanding of low-level system architecture.

In this talk we outline the surprising and highly nontrivial computational models involved. Based on these models we explain how the 4 problems above can be solved in a pervasive theory of multicore systems. Full formal verification of modern hypervisors requires to formalize exactly this theory.

Biographical Sketch

Wolfgang Paul was born in 1951. At age 22 he completed his PhD in theoretical computer science at Saarland University. He was a post doc at Cornell University working in complexity theory and then became a tenured associate professor of mathematics at the University of Bielefeld at age 25. After finishing a professional cooking degree at a Michelin 1 star restaurant he worked from 1982 to 1986 as a research staff member in the theory group and the physics department of IBMs Almaden Research Lab. Since 1986 he is a full professor for Computer Architecture and Parallel Computing at Saarland University, where he served as chairman of computer science, dean of engineering and acting head of the universities computing center. From 2003 to 2007 he was the scientific coordinator of projects 'Verisoft' and 'Verisoft-XT', two large projects aiming at the pervasive formal verification of entire computer systems from the gate level to the applications. Wolfgang Paul holds an honorary doctorate degree from Pacific State University (Russia) and is a member of Academia Europaea. So far Wolfgang Paul has successfully supervised 57 PhD students many of which had distinguished careers in academia and in industry. Wolfgang Paul has a drivers license for motor cycles and a black belt in Karate.

Structuring safety and assurance cases: "Divide and conquer" or "Divide and fall"?

Robin Bloomfield

Time: 15:30
Date: Dec 3rd 2012

Abstract

Safety and Assurance Cases are becoming widespread. In this talk I will describe our own experience and view of Cases and in particular the Claims Argument Evidence approach we defined. This talk will discuss the research we are doing in how to structure and challenge cases and report on some of our experiences in moving the concept of Assurance Cases from safety to security and the challenges in seeking compositionality.

Biographical Sketch

Robin Bloomfield is a founder of the specialist consultancy Adelard LLP and is Professor of Software and System Dependability at City University London.

His work in safety and security in the past 30 years has combined policy formulation, technical consulting and underpinning research. He has held a variety of professional and honorary posts: he was an independent member of the UK Nuclear Safety Advisory Group (NUSAC) and is an Associate Editor-in-Chief of IEEE Security and Privacy. He holds an MA in Natural Sciences from Cambridge University and is also a chartered engineer.

Rebranding the Concept of Assurance NIST Special Publication 800-53, Revision 4

Ron Ross

Time: 8:45
Date: Dec 4th 2012

Abstract

"We have lost an entire generation who understand what assurance is and why it is important ... the consequences of which may be potentially severe or catastrophic." NIST Special Publication 800-53, Revision 4 has addressed a number of gaps with respect to previous efforts, including security assurance and trustworthy systems. The updates to 800-53 are part of an initiative to rebrand the concept of assurance, and to once again move trustworthiness to a prominent role in assessing security capability. We emphasize the roles of security functionality and security assurance in trustworthiness, and examine the role of modularity, layering, and monitoring as key assurance concepts. NIST is adding a complete set of high assurance security controls that will facilitate the development of high assurance overlays that replicate either Common Criteria EAL 6/7 or TCSEC B3/A1.

Biographical Sketch

Ron Ross is a Fellow at the National Institute of Standards and Technology (NIST). His current areas of specialization include information security and risk management. Dr. Ross leads the Federal Information Security Management Act (FISMA) Implementation Project, which includes the development of security standards and guidelines for the federal government, contractors, and the United States critical information infrastructure. His recent publications include Federal

Information Processing Standards (FIPS) Publication 199 (security categorization standard), FIPS Publication 200 (security requirements standard), NIST Special Publication (SP) 800-53 (security controls guideline), NIST SP 800-53A (security assessment guideline), NIST SP 800-37 (security authorization guideline), NIST SP 800-39 (risk management guideline), and NIST SP 800-30 (risk assessment guideline). Dr. Ross is the principal architect of the Risk Management Framework and multi-tiered approach that provides a disciplined and structured methodology for integrating the suite of FISMA standards and guidelines into a comprehensive enterprise-wide information security program. Dr. Ross also leads the Joint Task Force Transformation Initiative, a partnership with NIST, the Department of Defense, the Intelligence Community, the Office of the Director National Intelligence, and the Committee on National Security Systems to develop a unified information security framework for the federal government.

Software Assurance: Enabling Enterprise Resilience through Security Automation and Software Supply Chain Risk Management

Joe Jarzombek

Time: 15:30
Date: Dec 4th 2012

Abstract

The DHS Software Assurance (SwA) program works collaboratively with federal government and private sector partners to provide resources, tools and information to reduce the exploit potential of software. The SwA program sponsors security automation efforts that enable cost-effective, scalable processes and resources that advance the detection, prevention and mitigation of cyber threats at "machine speed." This better enables stakeholders to leverage information about exploitable weaknesses, vulnerabilities, malware and threat information to empower diverse types of organizations to easily influence corrective actions, and to choose what information share and which partners to share it with. The ultimate goal is to allow any organization's identification and analysis of suspicious code behavior and activity to inform preventive measures for the broader community as rapidly as possible. This presentation explores considerations for layered assurance in the context of resilience for enterprises through security automation and software supply chain risk management.

Biographical Sketch

Joe Jarzombek is the Director for Software Assurance within the Office of Cyber Security and Communications (CS&C) of the Department of Homeland Security. In this role he leads government interagency efforts with industry, academia, and standards organizations in addressing security needs in work force education and training, more comprehensive diagnostic capabilities, and security-enhanced development and acquisition practices. Joe served in the U.S. Air Force as a Lieutenant Colonel in program management. After retiring from the Air Force, he worked in the cyber security industry as vice president for product and process engineering. Joe also served in two software-related positions within the Office of the Secretary of Defense prior to accepting his current DHS position. He serves on several cyber security advisory groups. He is a Project Management Professional (PMP) and a Certified Secure Software Lifecycle Professional (CSSLP).