Layered
Assurance
Workshop

KEYNOTE AND INVITED SPEAKERS

9th Layered Assurance Workshop

December 7-8, 2015

Los Angeles, California, USA

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

Architecture Principles and Certification Approaches for Medical Application Platforms

John Hatcliff
Kansas State University

Time: 08:45
Date: December 7th 2015

Abstract

The concept of “system of systems” architecture is increasingly prevalent in many critical domains. Such systems allow information to be pulled from a variety of sources, analyzed to discover correlations and trends, stored to enable real-time and post-hoc assessment, mined to better inform decision-making, and leveraged to automate control of system units. In contrast, medical devices have primarily been developed as monolithic stand-alone units. The movement toward devices with connectivity is accelerating, but the vendor and regulatory communities are still searching for appropriate architecture principles that allow devices with connectivity to be flexibly composed into interoperable systems following sound engineering principles that provide appropriate levels of safety and assurance.

The emerging notion of “medical application platform” (MAP) provides solution strategies to address these challenges. A MAP is a safety- and security-critical real-time computing platform for (a) integrating heterogeneous devices, medical IT systems, and information displays via a communication infrastructure and (b) hosting application programs (i.e., "apps") that provide medical utility via the ability to both acquire information from and exert control over integrated devices, IT systems, and displays. In this talk, I will present clinical motivation for MAPs and provide an overview of key elements of the safety, architecture, and engineering principles embodied in the Medical Device Coordination Framework (MDCF) -- an open-source MAP implementation that adheres to the Integrated Clinical Environment (ICE) architecture. A key focus of this talk will be principles necessary (but not sufficient) for supporting regulatory and third-party certification regimes that provide notions of compositionality and reuse of component assurance arguments across regulatory submissions. I'll describe how these principles are being manifested in the development of the AAMI/UL 2800 family of standards for safety and security of interoperable medical systems.

Biographical Sketch

Dr. John Hatcliff is a University Distinguished Professor at Kansas State University working in the areas of safety-critical systems, software architectures, and software verification and certification. He leads the Laboratory on Static Analysis and Transformation of Software (SAnToS Lab), which has received over $14 million in research funding from the Department of Defense, National Science Foundation, NASA, and NIH since 2000. Dr. Hatcliff co-chairs the Architecture Requirements Working Group of the AAMI / UL 2800 Joint Committee that is developing safety and security standards for medical device interoperability. He has been an active member of the Medical Device Interoperability Safety Working Group that is currently interacting with the FDA on interoperability safety principles under the IDE program, and he is a member of the NIH/NIBIB interoperability research project led by Dr. Julian Goldman from the Center for Integration of Medicine and Innovative Technology (CIMIT).

Layered Assurance Workshop

CHERI: A Hybrid Capability Architecture

Robert Watson
University of Cambridge

Time: 10:30
Date: December 7th 2015

Abstract

CHERI is a hybrid capability architecture: a pragmatic blend of capability-system design and conventional RISC processor architecture. While continuing to support conventional C-language-based operating systems and applications, CHERI introduces fine-grained memory protection and compartmentalization intended to provide vulnerability mitigation through top-to-bottom implementation of the principle of least privilege. Prototyped using the 64-bit MIPS ISA, but with concepts applicable to other RISC ISAs such as ARMv8 and RISC-V, we have developed informal and formal instruction-set specifications, multiple hardware prototypes in FPGA, adaptations of the FreeBSD operating system and Clang/LLVM compiler suite, and demonstrations deploying memory protection and compartmentalization within current C-language applications. The hybrid model permits CHERI features to be deployed incrementally into the most trusted TCBs (critical OS functions and privileged components), and least trustworthy applications (e.g., compression and image-processing libraries), while avoiding source-code or binary disruption of the remainder of the software ecosystem. With papers at ISCA 2014, ASPLOS 2015, and IEEE S&P 2015 describing aspects of the hardware architecture, programming-language approach, and security model, we have relied extensively on formal modeling to support our design and implementation efforts. This talk will describe the (thus-far) 5-year DARPA-funded project, the high-level architecture, aspects of CHERI's incremental adoption approach, and future directions.

Biographical Sketch

Dr. Robert N.M. Watson is a University Lecturer in Systems, Security, and Architecture at the University of Cambridge Computer Laboratory, where his research interests span Security, Networks and Operating Systems, and Computer Architecture. He leads a number of cross-layer research projects spanning computer architecture, compilers, program analysis, program transformation, operating systems, networking, and security. Current projects include CTSRD, a project in collaboration with SRI International looking at clean-slate hardware and software designs for security. This includes the BERIand CHERI processor designs, and SOAAP and TESLA, software analysis and transformation systems based on LLVM. He also has active research projects in network-stack performance, tracing, and switching. His prior work includes the Capsicum hybrid capability system and the TrustedBSD MAC Framework, a widely deployed OS access-control extensibility framework (used for sandboxing in FreeBSD, Mac OS X, Apple iOS, Junos, and other products). He has strong interests in open-source software, is on the board of directors of the FreeBSD Foundation, and has contributed extensively to the FreeBSD Project. He is a coauthor on the second edition of the Design and Implementation of the FreeBSD Operating System.

Layered
Assurance
Workshop

A Layered Assurance Experience Report

Dylan McNamee
Galois, Inc.

Time: 15:30
Date: December 7th 2015

Abstract
For the past ten years, Dylan McNamee has been applying Layered Assurance techniques to a broad range of projects at Galois, Inc. In this talk, he will describe some of the resulting successes and challenges, and will provide his perspective on future directions the community may want to pursue.

Biographical Sketch
Dylan McNamee has been on the technical staff at Galois, Inc. since 2004, where he has worked on secure operating system architectures, MILS system design, and cryptographic verification. Dylan was the file system architect for the Trusted Services Engine, a multi-level secure file store with read-down, and was the principle investigator of a "Low-cost, high-assurance separation kernel" research project for the DoD. When he's not building trustworthy systems, he is perfecting his espresso technique, building replica computers and looking for ways to help K-12 computer science education.

Layered
Assurance
Workshop

Layers of Formal Verification for Full-Scale NextGen Automated Air Traffic Control

Kristin Rozier
University of Cincinnati

Time: 8:45
Date: December 8th 2015

Abstract

We are at the dawn of a new age in air traffic control. The airspace is full in the sense that demand for flights exceeds our capacity to add new air traffic. The time-tested current method of air traffic control has hit its scalability limit and must be replaced with a new system that is more scalable while also proving at least as safe. Now that we have the chance to redefine air traffic control from scratch, the question arises: how do we do it safely?

We explore new frontiers in symbolic model checking to scalably answer the functional allocation question: instead of analyzing one design, or comparing a pair of designs, we now need to take into account a large number of permutations and combinations of functions that comprise a large set of possible designs. We compositionally model and comparatively analyze this set with regard to safety on multiple levels, considering the full space of possible system designs both in nominal conditions and in the presence of faults. Our analysis helps NASA narrow the possible design space, saving time and cost of later-phase evaluations, identifying both novel and known problematic design configurations. We look to the future, where a componsitional approach layering different verification techniques at multiple levels will be required to build up a safety case for the final design.

Biographical Sketch

Professor Kristin Yvonne Rozier heads the Laboratory for Temporal Logic in Aerospace Engineering at the University of Cincinnati; previously she spent 14 years as a Research Scientist at NASA. She earned her Ph.D. in computer science from Rice University and B.S. and M.S. from The College of William and Mary. Her research focuses on automated techniques for the formal specification, validation, and verification of safety critical systems including: design-time checking of system logic and requirements; system health management; and safety and security analysis. Her advances in computation for the aerospace domain earned her many awards including: the American Helicopter Society's Howard Hughes Award; the Women in Aerospace Inaugural Initiative-Inspiration-Impact Award; AIAA's Intelligent Systems Distinguished Service Award; the Lockheed Martin Space Operations Lightning Award; and two NASA Group Achievement Awards. She is an Associate Fellow of AIAA, a 2015 Faculty Fellow of the Schmidt Data Science for Social Good program at the University of Chicago, and the founding member of the Steering Committee of the NASA Formal Methods (NFM) Symposium.

Layered
Assurance
Workshop

Reflections on Composite Compliance as applied to global standards and regulatory requirements

Heather Hinton
IBM

Time: 10:30
Date: December 8th 2015

Abstract

In traditional IT environments, audit and compliance are largely a monolithic event: an auditor performs and extensive examination of an IT environment from the ground up, from physical facilities and environmental security up through the server management through operating systems to applications and their management and use. The move to modular architectures, open source tools, SaaS offerings, and now the widespread adopting of Infrastructure and Platform as a Service has broken this model. Providers are unwilling or unable to support the volume of ground up audits that would be required to support each individual customer. Instead, providers issue individual audit reports and rely on those as attestations of goodness about their environments and offerings. In this talk I will describe our approach to the assessment of individual audit reports and their composition to provide a full end-to-end compliance assertions. This heuristic based approach is based on the responsibility boundaries between providers and the impact of the north/south communication channels and assumed shared responsibility between providers. This approach is intended to support the adoption of composite compliance to support industry requirements including HIPAA, FFIEC, and Data Privacy requirements.

Biographical Sketch

Dr. Heather Hinton is an IBM Distinguished Engineer, an IBM Master Inventor and a member of the IBM Academy of Technology. She has over 20 years of computer security / information security experience. Heather provides technical direction, solutions and strategy for Cloud Security and Compliance solutions across the IBM Cloud Business Unit. As the CTO Compliance she has responsibility to ensure and drive strategy and architecture for cloud offerings such that they support customer requirements for compliance with local and global regulatory standards. Heather led the creation of the Security and Compliance Specialty Service Area in IBM Global Technology Services. As CTO, Heather built up a dedicated, world-wide team of over 2000 security practitioners with responsibility for internal offering architecture, standards, and customer solution reviews. Heather has also led the roll-out of global security solutions and cyber security tools and processes to all IBM users and privileged users.

Prior to joining GTS, Heather was part of IBM Software Group, where she was the Chief Security Architect for Service Process Automation. Heather has also held positions as the Technical Lead for acquisition and due diligence efforts across SWG and STG, as the initial product architect for Tivoli Federated Identity Manager and was part of the team that authored WS-Trust and SAML. In 2008 she was selected to participate in the initial IBM Corporate Services Corps program, working in DaNang, Vietnam. In 2012, Heather was a member of the Executive Service Corps team working with the Mayor of the City of Accra, Ghana. Within her local community of Austin, Texas, Heather is a volunteer with the Community Tax Foundation, Discover Engineering, US CyberPatriot, FLL and FTC Robotics, and the Boy Scouts of America as a Merit Badge and STEM counselor. Prior to joining IBM Heather was an Assistant Professor of Computer & Electrical Engineering at Ryerson Polytechnic University in Toronto, Canada. Heather holds a PhD in Computer & Electrical Engineering in the area of Computer Security from the University of Toronto, Canada.

Layered
Assurance
Workshop

Virtual Integration and Incremental Assurance of Critical System

Peter Feiler
Carnegie Mellon Software Engineering Institute

Time: 13:30
Date: December 8th 2015

Abstract

Challenging problems associated with the increasing complexity of software systems are threatening industry's ability to build and pay for the next generation of safety-critical embedded systems. Using the current best practice of building and then testing software-reliant mission- and safety-critical systems, 80% of requirements and architecture design flaws are discovered after unit testing. This late discovery of design flaws can result in rework cost that exceeds 50% of the total system cost. Contributors to these problems include the growth of software, system integration, and interaction complexity exacerbated by ambiguous, missing, incomplete, and inconsistent requirements.

In this presentation we discuss how architecture-centric approach addresses this challenge through a four-pillar strategy. First, virtual system integration leads to early discovery of defects reducing leakage to later phases by identifying mismatched assumptions and issues with system-level properties. Second, compositional analysis techniques allow for functional and non-functional system properties to be verified incrementally by evolving system designs in the context of verified higher-level specifications. Third, architecture-led requirement specification and safety analysis with focus on requirement and design uncertainty lead to increased requirement and hazard coverage. Fourth, tracking of multi-valued verification results based on automated verification of models to complement software testing throughout the life cycle identifies verification hotspots. This leads to measurement driven strategy for improving system quality and reducing qualification costs.

Biographical Sketch

Dr. Peter Feiler is a 30-year veteran and Principal Research Scientist at the SEI, working in the Architecture Practices program. His current research interest is in improving the quality of safety-critical software-intensive systems through architecture-centric virtual integration and verification to reduce rework and qualification costs. Feiler has been the technical lead and main author of the SAE Architecture Analysis & Design Language (AADL) standard. He has a PhD in computer science from Carnegie Mellon University.