Layered Assurance Workshop

KEYNOTE AND INVITED SPEAKERS

2014 Layered Assurance Workshop

December 8-9, 2014
Hyatt French Quarter, New Orleans, Louisiana, USA

Affiliated workshop of the
30th Annual Computer Security Applications Conference (ACSAC)

Modular Construction of Systems and Layered System Architectures by Rich Subsystem Specs

Manfred Broy
Institut für Informatik,Technische Universität München (DE)

Time: 08:45
Date: December 8th 2014

Abstract

Cyber-physical systems are artifacts consisting of mechanics, hardware and software, which are tightly integrated. In contrast to approaches to software and other disciplines, cyber-physical systems need an integrated interface specification on which a modular composition is based. For that, the system model has to combine a number of concepts for describing the system interface behaviour and its modular construction. It is shown how a rich model for system interface behaviour and a notion of composition allow the construction of a system in a layered modular way taking care of all kinds of different quality aspects of systems such as safety security, reliability and many more.

Biographical Sketch

Manfred Hans Bertold Broy studied Mathematics and Computer Science at the Technical University of Munich. He graduated in 1976 with the Diplom in Mathematics and Computer Science. In February 1980, Manfred Broy received his Ph. D., and in 1982, he completed his Habilitation Thesis: "A Theory for Nondeterminism, Parallelism, Communication and Concurrency". In April 1983, he became a full professor for computer science and the founding dean at the Faculty of Mathematics and Computer Science at the University of Passau. In October 1989, he became a full professor for computer science at the Faculty of Computer Science the Technische Universität München (former chair of Professor F.L. Bauer).

His research interests are software and systems engineering, comprising both theoretical and practical aspects. These include system models, specification and refinement of system components, specification techniques, development methods and verification. He is leading a research group working in a number of industrial projects that apply mathematically based techniques and combine practical approaches to software engineering with mathematical rigor. The main topics are: requirements engineering, ad hoc networks, software architectures, componentware, software development processes and graphical description techniques. The CASE tool AutoFocus was developed in his group.

Prof. Dr. Dr. h. c. Broy has received a number of awards for contributions to science: Gottfried Wilhelm Leibniz Award of the German Science Foundation (1994), Federal Cross of Merit (1996), Doctorate Honoris Causa, University of Passau (2003), Bavarian State Award for Education and Culture (2006) and Konrad Zuse Award for Computer Science (2007). He is a member of the: Board of Trustees of Fraunhofer Institute, European Academy of Science, German Academy of Natural Scientists „Leopoldina“, Association of Computer Sciences and acatech-Council for Technical Sciences. He has a Max-Planck Fellowship.

Throughout his academic career, Prof. Dr. Dr. h. c. Broy has maintained strong contacts with industry, through consultancy, teaching and collaborative research projects, and he has published more than 300 scientific publications. His main field is Software & Systems Engineering and his current research interests are: the System Development Processes and Tool Support, Concurrent and Embedded Systems, Theoretical Foundation of Informatics, IT Security and Requirements Engineering.

One of the mains theme of Manfred Broy is the role of software in a networked world. As a member of acatech under his leadership the study Agenda Cyber-Physical Systems was created for the Federal Ministry of Research to comprehensively investigate the next stage of global networking through the combination of cyberspace and embedded systems in all their implications and potential.

Layered
Assurance
Workshop

Designing for Assurance in High-Consequence Systems

Earl Boebert
Author and Consultant

Time: 15:30
Date: December 8th 2014

Abstract
This talk is based on the lessons learned in 40 years of work with real-time systems whose failures could cause grave damage and/or loss of human life. The talk will cover aspects of design that support both formal and informal assurance.

Biographical Sketch
I wrote my first computer program in 1958 as an undergraduate at Stanford. After graduating, I became an electronic data processing officer in the United States Air Force.

I then joined Honeywell, where I was one of three lead designers on the Undergraduate Navigator Training System, which generated real-time synthetic landmass radar for 55 student stations. It was the largest distributed real-time system of the early 1970s, with 150 networked computers and a gigabyte of real-time storage. It and its upgrades served for 37 years and trained more than 20,000 Air Force navigators.

I also managed a group that worked on security enhancements for the Multics system. I contributed to the design and verification of software for the Saab JA37B autopilot, the first full-authority digital fly-by-wire system to fly operationally. I performed similar tasks for the Mark 48 torpedo and the Space Shuttle main engine controller, contributed to the design of the Ada programming language, and won Honeywell's highest award for technical achievement. I was also a long-time consultant on the flight software assurance to the Naval Weapons Center, China Lake.

I then became chief scientist of Secure Computing Corp., where I led the creation of the Sidewinder security server. My final position before retirement was as a senior scientist for Sandia National Laboratories.

I have served on 10 National Research Council committees and have acted as a reviewer for many National Research Council reports. In recognition of the above service, I was made a National Associate of the National Research Council in December 2011.

Layered
Assurance
Workshop

Commercial Solutions for Classified (CSfC) Overview

Jeffrey Watkins
National Security Agency

Time: 16:45
Date: December 8th 2014

Abstract

By Presidential Directive Order, the National Security Agency (NSA) determines standards and policies for our Nation's most critical National Security Systems (NSS), and NSA's Information Assurance Directorate (IAD) has the mission of protecting this critical information. Given the rapid growth of new commercial technologies and the subsequent demand by NSS customers to use them, IAD is leveraging the appropriate use of commercial technology to protect classified information. This is accomplished through the Commercial Solutions for Classified (CSfC) process, whereby commercial technologies are layered together in precise configurations to provide a commercial information assurance solution protecting classified information. This presentation will provide a high-level overview of CSfC, outline the operational benefits and designed-in assurance features to users, review the published specifications and IAD-approved security architectures, and preview what's ahead for 2015.

Biographical Sketch

Jeffery Watkins has worked at NSA for 30 years, where he currently is serving as the Commercial Solutions for Classified (CSfC) Communications Manager. He graduated Summa Cum Laude with a Bachelor of Science in Information Systems Management (University of Maryland University College, 2004). During his career at NSA, Mr. Watkins has deployed numerous secure voice system interfaces, provided information system security engineering support to the Combatant Commands/Services/Agencies and managed the certification of cross-domain solutions to meet Warfighters' requirements. Additionally, Jeff served in the field as the Senior NSA Liaison to the Defense Information Systems Agency (DISA).

Layered
Assurance
Workshop

Dancing with the Adversary: a Tale of Wimps and Giants

Virgil Gligor
Carnegie Mellon University

Time: 08:45
Date: December 9th 2014

Abstract

A system without accurate and complete adversary definition cannot possibly be insecure. Without such definitions, (in)security cannot be measured, risks of use cannot be accurately quantified, and recovery from penetration events cannot have lasting value. Conversely, accurate and complete definitions can help deny the adversary any attack advantage over a system defender and, at least in principle, secure system operation can be achieved. In this talk, I argue that although the adversary's attack advantage cannot be eliminated in large commodity software (i.e., for "*giants*"), it can be rendered ineffective for small software components with rather limited function and high-assurance layered security properties, which are isolated from giants; i.e., for "*wimps*." However, isolation cannot guarantee wimps' survival in competitive markets, since wimps trade basic system services to achieve small attack surfaces, diminish adversary capabilities, and weakened attack strategies. To survive, secure wimps must use services of, or compose with, insecure giants. This appears to be "paradoxical:" wimps can counter all adversary attacks, but only if they use adversary-vulnerable services from which they have to defend themselves.

In this talk, I will illustrate the design of a practical system that supports wimp composition with giants, and extend the wimp-giant metaphor to security protocols in networks of humans and computers where compelling (e.g., free) services, possibly under the control of an adversary, are offered to unsuspecting users. These protocols produce value for participants who cooperate. However, they allow malicious participants to harm honest ones and corrupt their systems by employing deception and scams. Yet these protocols have safe states whereby a participant can establish (justified) beliefs in the adversary's (perhaps temporary) honesty. However, reasoning about such states requires techniques from other fields, such as behavioral economics, rather than traditional security and cryptography.

Biographical Sketch

Virgil D. Gligor received his B.Sc., M.Sc., and Ph.D. degrees from the University of California at Berkeley. He taught at the University of Maryland between 1976 and 2007, and is currently a Professor of Electrical and Computer Engineering at Carnegie Mellon University and co-Director of CyLab, the University's laboratory for information security, privacy and dependability. Over the past forty years, his research interests ranged from access control mechanisms, penetration analysis, and denial-of-service protection to cryptographic protocols and applied cryptography. He was a consultant to Burroughs Corporation, IBM, and SAP and has served on Microsoft's Trusted Computing Academic Advisory Board since 2003. Gligor was an editorial board member of several ACM and IEEE journals and the *Editor in Chief* of the IEEE Transactions on Dependable and Secure Computing. He received the *2006 National Information Systems Security Award* jointly given by NIST and NSA, the *2011 Outstanding Innovation Award* of the ACM SIG on Security Audit and Control, and the *2013 Technical Achievement Award* of the IEEE Computer Society.

Layered
Assurance
Workshop

High-Assurance Cyber-Physical Systems

Natarajan Shankar
Computer Science Laboratory, SRI International

Time: 15:30
Date: December 9th 2014

Abstract
Cyber-physical systems are composed of physical and computational components interacting through multiple control loops and at multiple time scales. These systems are realized through a distributed network of sensors, controllers, and actuators. They are vulnerable to both physical and electronic attacks, and must be resilient to hardware and software failures. We describe a framework for building high-assurance cyber-physical systems based on

1. The eight-variables model of interaction between the plant, sensors, controller, actuator, and operator.

2. A quasi-synchronous model of computation (MoC) where sensor, controller, and actuator nodes operate at fixed but independent periods with bounded clock drift and message latencies.

3. The Robot Architecture Definition Language (RADL) for capturing the logical and physical architecture of a cyber-physical system within a high-assurance build process.

4. The Evidential Tool Bus for defining workflows for producing evidence-based assurance cases that integrate multiple verification and validation tools.

We describe our experience applying the above framework within the DARPA HACMS program.

Biographical Sketch
Dr. Shankar is a Principal Scientist at the SRI International Computer Science Laboratory, where he is part of a research group focused on automated formal verification and is involved in the development of formal verification tools such as PVS, SAL, and Yices. He has used formal verification tools to prove metatheorems such as the tautology theorem, Gödel's incompleteness theorem, and the Church-Rosser theorem. He is author of "Metamathematics, Machines, and Gödel's Proof", published by Cambridge University Press (1994). He graduated with a B.Tech in EE from Indian Institute of Technology, Madras in 1980, and a Ph.D. in CS from University of Texas at Austin in 1986.

In 2009 Dr. Shankar was named an SRI Fellow, a recognition of exceptional staff members for their outstanding contributions to science.