

The Fifth Layered Assurance Workshop

December 5 – 6, 2011
Buena Vista Palace Hotel & Spa
Orlando, Florida

Program and proceedings: <http://fm.csl.sri.com/LAW/2011>

Welcome and Opening Remarks



Rance DeLong, LynuxWorks, LAW Chair

Gabriela Ciocarlie, Coverity, LAW PC Chair

Gordon Uchenick, Coverity, LAW PC, Chair Emeritus

Overview of LAW 2011 – Rance DeLong



LAW Purpose and Philosophy

- LAW was motivated by outstanding unsolved problems encountered in the pursuit of solutions to real needs discovered in developing and applying approaches, like MILS, that would benefit from compositional assurance
- LAW should be *Progressive* if it is to deliver value relative to other venues. It should be forward looking and not dwell on current practice. LAW exists because of the shortfalls of current practice.
- LAW should challenge past and current, failed and inadequate approaches
- LAW should serve as driving force for future solutions by stimulating relevant basic research and providing a conduit for the flow of research results to other researchers, and to vendors and system integrators who are in a position to apply them

Gabriela Ciocarlie, Coverity Program Chair

Opening Remarks

Gordon Uchenick, Coverity PC, LAW Chair Emeritus

Opening Remarks

Rance DeLong, LynuxWorks LAW Chair

Overview of LAW 2011

LAW Organizing Committee



Joyce Brookins
Gabriela Ciocarlie
Rance DeLong
George W. Dinolt
Peter G. Neumann
Michael Putney
Gordon Uchenick



5th Layered Assurance Workshop

What we set out to do in 2011



- Objectives
 - Run a self-sustaining workshop - a legacy from AFRL/AF CMPO
 - Focus on the unsolved problems - stimulate pre-competitive research
 - Attract researchers - peer-reviewed submissions, web published proceedings, keep “Workshop” moniker
 - Disseminate knowledge of current state of the art – keynotes, invited talks, contributed papers, works-in-progress
 - Globalize reach – “international” Layered Assurance Workshop
- Evolutionary differences from past LAWs
 - Affiliated again with ACSAC, but without external funding support
 - Registration fee not subsidized (though discounted for ACSAC attendees)
 - More keynote and invited speakers
 - Work-In-Progress Session

LAW Program Summary



- Five distinguished invited speakers:
Bensalem, Dave, Goodenough, Miner, Shrobe
- Five contributed paper authors:
Alves-Foss, Bradetich, Greve, Hardin, Heckman
- Five work-in-progress presentations:
Boggs, DeLong, Giampapa (2), Mildner
- Panel:
Future of highly trustworthy systems, networks, and clouds
DeLong, Neumann, Shrobe, Sullivan, Vanfleet
organized and moderated by Peter G. Neumann
- Discussion session
- BREAK and LUNCH same times as other ASCAC events
- LAW attendees invited to the LAW Business Meeting
- LAW attendees invited to the ACSAC Tuesday Reception

LAW Program and Supplement



Monday 5 December and Tuesday 6 December, 2011
Orlando, Florida, USA
The Fifth Annual Layered Assurance Workshop (LAW 2011) Program

Contributed papers will be linked to the online program prior to the commencement of LAW. Presentations will be linked to the program shortly after the conclusion of LAW. See <http://fm.csl.sri.com/LAW/2011>

The LAW Business Meeting scheduled after the conclusion of sessions on Monday December 5 is open to all interested individuals. Planning for LAW 2012 will commence. Registration from the LAW community is essential to the ongoing vitality of LAW.

LAW attendees are invited to attend the ACSAC Reception on Tuesday December 6 at 6 PM.

The names of invited speakers and presenting authors are undrafted in the Program following.

Monday December 5

07:30-08:30	BREAKFAST
08:30-08:45	Welcome and Opening Remarks Rance Dalwig, L3HarrisWorks, LAW Program Chair Catalina Censic, Covaris
08:45-10:00	Keynote: Supporting us to a "Do over"? Howard Shrobe CRASH Program Manager, MRC Program Manager
10:00-10:30	BREAK
10:30-12:00	Panel: The Future of Highly Trustworthy Systems, Networks, Apps, and Clouds Moderator: Rance Dalwig Panelists: Glen G. Stavrou, CRASH CTSRD Division, SRI International Rance Dalwig, Future MRC L3HarrisWorks W. Mark Yanoff, National Security Agency / NCSC Howard Shrobe, CRASH / MRC / DARPA EO
12:00-1:30	LUNCH
1:30-1:50	Contributed Papers: Introduction to the General Programming Language and Verification System of Plain-Turned Systems Rance Dalwig David Zeman Lance Assurance Jim Abate, IBM
1:50-15:30	BREAK
15:30-16:45	Invited Talk: A Layered Assurance Perspective: Lessons from the Formal Analysis of Plain-Turned Systems Paul Mitton Senior Research Engineer, NASA Langley Research Center
16:45-17:45	Contributed Papers: Evaluation of Software Architectures for Application in H-A Systems Rance Dalwig Contributor to HGA-Arch Mark R. Heckman
18:00-18:45	LAW Business Meeting and LAW 2012 Planning

LAW@ACSAC



Layered Assurance Workshop
KEYNOTES and Invited Talks

Supporting us to a "Do over"?
 Most of our computer hardware and systems designs are the legacy of a bygone era when resources were scarce and every transistor or line of code had the sole purpose of increasing performance. That has led us to today where our biggest problem is the security, integrity and robustness of our computer systems. In this talk, I'll describe two programs sponsored by DARPA, CRASH (Clean-state Design of Resilient, Adaptive, Secure Hosts) and MRC (Mission-oriented Resilient Clouds), that are taking a clean-state approach to design systems (from hardware, through system software, middleware and application code) that are both highly resistant to attack and capable of operating usefully even after attacks have succeeded.

Howard Shrobe is long term member of the MIT Computer Science and Artificial Intelligence Laboratory. He is currently serving his second term at DARPA, having previously served from 1994 - 1997. During his first term he initiated the Information Survivability effort. He is currently leading the Cyber Security program, CRASH, Clearstate Design of Resilient Hosts and Mission-oriented Resilient Clouds (MRC). Both draw on biological and social inspiration. CRASH is trying to develop a clean-state host architecture that uses novel hardware and operating system techniques to erect strong barriers to penetration. MRC is trying to build adaptive protection that detect, generate, receive and patch novel attacks. These two approaches mimic the "immune" and "adaptive" components of the immune system. Finally diversity is used to raise the attacker's work factor further. In MRC these same ideas are applied, but at a community scale, mirroring the elements of a public health system.

Using eliminative induction and defeasible reasoning to assess assurance case confidence
 Given a claim supported by some argument or evidence, how much confidence should we have in the truth of the claim? What does "confidence" mean in this case? Should it be the likelihood that the claim is true, or should it be the degree of belief that the claim is true. We propose an approach that focuses on establishing the truth of a claim and then showing how confidence grows as each of these sources of doubt are eliminated. The approach is illustrated with a simple example. Considerable additional work is needed to assess its practicality, but it does provide a way of thinking about assurance case confidence that has several benefits.

John Goodenough is a Fellow of the Software Engineering Institute and most recently led a research project on system of systems software assurance. He and his team have worked on the assurance cases for almost ten years, investigating their application to ensuring the safety of medical devices, assessing the security of the software supply chain, and negotiating whether a software project is developing the right artifacts to be successful. He has served as the SEI's Chief Technical Officer and is a Fellow of the ACM.

- Pickup at Registration Desk

- Program and Proceedings

Available online at

<http://fm.csl.sri.com/LAW/2011>

- Program Supplement: Keynote and Invited Talk abstracts and speaker bios

We gratefully acknowledge the efforts of Michael Putney, and the resources of US AF CMPO, in the production of the Program Supplement.

Invited Speakers

**Layered
Assurance
Workshop**

- Howard Shrobe – DARPA I2O, CRASH PM and MRC PM
 - Supposing we got a “Do over”?
- Paul Miner – NASA, Senior Research Engineer
 - A Layered Assurance Perspective: Lessons from the Formal Analysis of Fault-Tolerant Systems
- John B. Goodenough – CMU SEI Fellow
 - Using eliminative induction and defeasible reasoning to assess assurance case confidence
- Saddek Bensalem – University Joseph Fourier, VERIMAG Laboratory
 - Rigorous Component-based System Design Using the BIP Framework
- Nirav Dave – SRI International, Computer Scientist
 - Bluespec Codesign Language: A Unified Language to Enable HW / SW Codesign

Panel

- Peter G. Neumann (SRI), Howard Shrobe (DARPA), Gregory Sullivan (BAE Systems), Rance DeLong (LinuxWorks), Mark Vanfleet (NSA)

Contributed Papers

1. Introduction to the Guardol Programming Language and Verification System
2. Data Flow Logic: Analyzing Information Flow Properties of C Programs
3. Layered Assurance Scheme for Multicore Architectures
4. Evaluating Multicore Architectures for Application in High-Assurance Systems
5. Composing a High-Assurance Infrastructure out of TCB Components

Work-In-Progress Presentations

1. Multi-layer Defense for Power Grid SCADA Systems
2. High Robustness
3. MILS Research - Accomplishments and Ongoing Work
4. Metric for Layered Defenses
5. Compositional Assurance for Robotic Coordination

Logistics



Breakfast - from 7:30 AM until 8:30 AM

Coffee Breaks - one-half hour at 10 AM and 3 PM

Lunch - from 12 PM until 1:30 PM

Timeliness - Full program, *please* be punctual!

LAW Business Meeting - Monday from 6:00 PM until 6:45 PM

ACSAC Reception - Tuesday at 6 PM until 8 PM

Keynote:

Supposing we got a “Do over” ?

Howard Shrobe

DARPA

Panel:

The Future of Highly Trustworthy Systems, Networks, Apps, and Clouds

Peter G. Neumann, SRI International, moderator
Gregory Sullivan, Rance DeLong, W. Mark Vanfleet, Howard Shrobe

Invited Talk:

A Layered Assurance Perspective: Lessons from the Formal Analysis of Fault-Tolerant Systems

Paul Miner

NASA

Keynote:

Using eliminative induction and defeasible reasoning to assess assurance case confidence

John B. Goodenough

CMU SEI Fellow

Invited Talk:

Rigorous Component-based System Design Using the BIP Framework

Saddek Bensalem

University Joseph Fourier, VERIMAG Laboratory

Invited Talk:

***Bluespec Codesign Language: a Unified Language
to Enable Hardware/Software Codesign***

Nirav Dave

SRI International

LAW Business Meeting

Planning for LAW 2012

LAW Business Meeting Agenda

- Volunteers needed!
 - 1st volunteer needed: Secretary for this business meeting
 - Workshop Committee, Program Committee
 - LAW Chair - serves on ACSAC committee
- What needs to be done
 - Communications - announcements, Call-For-Papers, updates
 - Workshop Theme, Format and Agenda
 - Speaker invitations – our tradition: Chair's choice
 - Program: CFP, submissions, reviews, author correspondence
- Corporate sponsorship opportunities
 - Give-aways, registration subsidies, travel expenses