The Third
Layered Assurance Workshop

August 4 – 5, 2009
San Antonio, Texas

Wednesday Morning

Layered Assurance Workshop

- Welcome and Introductions – Mr. Rance DeLong
- Hierarchies, Lowerarchies, Anarchies and Plutarchies, Dr.^{2} Peter Neumann
- Towards Assurance for Open Soft Real-Time Systems, Dr. Chris Gill
- BREAK
- Composition of Critical Properties, Dr. John Rushby
- Assurance Cases, Evidence, and Patterns Dr. Tim Kelly

Dr. Peter G. Neumann

PGN has doctorates from Harvard and Darmstadt. Ten years at Bell Labs in Murray Hill, NJ. He is an original Multician involved with MIT and Honeywell. Since '71 he has been in SRI's CS Lab. Named an SRI Fellow in '01, he is also a Fellow of the ACM, IEEE, and AAAS. He has received numerous professional society awards.

He is concerned with computer systems and networks, trustworthiness, dependability, high assurance, security, reliability, survivability, safety, and risk-related issues. His 1995 book, Computer-Related Risks is still timely.

Peter has been involved with important issues of computers and society, including voting-systems and privacy. He moderates the well-known ACM Risks Forum, edits CACM's monthly Inside Risks column, chairs the ACM Committee on Computers and Public Policy, and chairs the National Committee for Voting Integrity. He cofounded People for Internet Responsibility, and has testified before the US Senate and House, and California state Senate and Legislature.

Peter has maintained a steadfast interest in security and assurance, participating in four studies for the National Academies of Science: Multilevel Data Management Security ('82), Computers at Risk ('91), Cryptography's Role in Securing the Information Society ('96), and Improving Cybersecurity for the 21st Century ('07).

Dr. Chris Gill

Layered
Assurance
Workshop

Chris Gill is an Associate Professor of Computer Science and Engineering at Washington University in St. Louis. His research is focused on modeling, verification, implementation, and empirical evaluation of property enforcement policies and mechanisms in distributed, mobile, embedded, and real-time systems.

He developed the Kokyu real-time scheduling and dispatching framework that has been used in several AFRL and DARPA projects, and led the development of the nORB small-footprint real-time object request broker at Washington University in St. Louis.

Chris has more than 50 refereed technical publications and has an extensive record of service in conferences, workshops, review panels, and standards bodies for distributed real-time and embedded computing.

Chris has recently served on the AFRL-sponsored Mixed-Criticality Architecture Requirements project awarded to Boeing, and has a keen interest in the emerging field of cyber-physical systems.

Dr. John Rushby

John Rushby received B.Sc. and Ph.D. degrees in computing science from the University of Newcastle upon Tyne in 1971 and 1977, respectively.

He joined the Computer Science Laboratory of SRI International in 1983, and served as its director from 1986 to 1990. In 2004 John was named an SRI Fellow. He currently manages CSL's research program in formal methods and dependable systems. This program is responsible for the highly regarded and widely used PVS verification system, the SAL suite of model checkers, the Yices SMT solver, and novel methods for static analysis.

Prior to joining SRI, John held academic positions at the Universities of Manchester and Newcastle upon Tyne in England. His research interests center on the use of automated formal methods for problems in the design and assurance of secure and dependable systems.

John Rushby is a former associate editor for Communications of the ACM, IEEE Transactions on Software Engineering, and Formal Aspects of Computing. He is the author of a chapter on formal methods for the FAA Certification Handbook, and was a member of the National Research Council study that recently delivered its report "Software for Dependable Systems: Sufficient Evidence?". His publications are available online at at his web page.

Dr. Tim Kelly

Tim Kelly is a Senior Lecturer within the Department of Computer Science at the University of York. He is also Academic Theme Leader for Dependability in the UK MoD funded Software Systems Engineering Initiative (SSEI).

He is perhaps best known for his work on safety case development, particularly his work on refining and extending the Goal Structuring Notation (GSN). His research interests include safety case management, software safety analysis and justification, software architecture safety, certification of adaptive and learning systems, and the dependability of "Systems of Systems". He has supervised a number of research projects in these areas with funding and support from Airbus, BAE SYSTEMS, Data Systems and Solutions, DTI, EPSRC, ERA Technology, Ministry of Defence, QinetiQ and Rolls-Royce.

Tim has published over 100 papers on high integrity systems development and justification in international conferences and journals. He is also Managing Director of Origin Consulting (York) Limited – a consultancy company specialising in safety critical systems development and assurance – and Chair of the IET's Functional Safety Network Executive Committee.

Wednesday Panel Compositional Assurance Research and Development

- Chris Gill, Tim Kelly, John Rushby, Brian Snow
- Moderated by Michael McEvilley
- Moderator moderated by Rance DeLong (at the request of the Moderator)

Mr. Michael McEvilley

Layered
Assurance
Workshop

Michael McEvilley received B.Sc. and M.Sc. degrees in Computer Science from Tuskegee Institute and The George Washington University in ‘80 and ‘95, resp.

He served 4 years as a USAF officer supporting Tactical Intel Computer Operations, designed and implemented software enhancements and upgrades for the Command and Decision component of the Aegis Weapons System while at Computer Sciences Corporation.

He is currently in his third "tour" with The MITRE Corporation, where he has provided program management support to the Naval Research Lab for the software component of the Embedded INFOSEC Product, and has supported the NSA in a variety of capacities, including: the lastl B1 evaluation before the transition to Common Criteria; the establishment of NIAP and the Common Criteria Evaluation and Validation Scheme (CCEVS); the incorporation of a COTS separation kernel into the F22 security architecture; software partitioning feasibility study; member of the authoring team for the High Robustness Separation Kernel Protection Profile; and is currently supporting the High Assurance Platform Program Office and the Distributed SOA-based Cross Domain Solution initiative.

Michael’s primary interest is in the realization and acceptance of assurance techniques that yield "better than medium assurance" components which may be composed to provide tactical-edge and weapons platform solutions..

Mr. Brian Snow

Layered
Assurance
Workshop

Brian Snow, a mathematician/computer scientist, taught mathematics and helped found the computer science department at Ohio University in the late ‘60’s. He joined the National Security Agency in 1971 initially as a cryptologic designer and security systems engineer.

Brian spend his first 20 years at NSA performing and directing research in the development of cryptographic components and secure systems. His algorithms are used in cryptographic systems serving the US Government and military, including nuclear command and control and tactical radios for the battlefield, which involve strong assurance in a computer and network security context.

In the ‘80’s Brian created and managed NSA’s Secure Systems Design division. He has many patents, awards, and honors attesting to his creativity.

In his later years at NSA, Brian served as a Senior Technical Director in three major mission components: the Research Directorate, the Information Assurance Directorate, and the Directorate of Education and Traning - NSA’s Corporate University.

Brian earned B.A. and M.A. in mathematics, at the U of Colorado, in ‘65 and ‘67 resp. and has done post graduate work at U of Ohio and U of Maryland.

Retiring from NSA in ‘06 Brian now serves as a security consultant and ethics advisor.

Wednesday Break-Out Sessions 15:45 – 16:30

Layered Assurance Workshop

- Four parallel sessions
- Assigned Session Leaders
  - Cross Domain Solutions 2 - Michael Minette, Raytheon
  - Compositional Formal Methods - George Dinolt, NPS
  - Assurance for Pragmatic Composition of COTS HW & SW - Gordon Uchenick, OIS
  - Composition of Security Policies - Ravi Sandhu, UTSA
- Recorder / Reporter delegated by Session Leader
- Reporter: 2-3 BEST IDEAS / OBSERVATIONS of each breakout session to share in Plenary

Wednesday Break-Out Sessions (Rooms On Next Floor Up)

Layered Assurance Workshop

- Breakout 1 (Frio)
  - Cross Domain Solutions - Take 2
  - Led by Michael Minette
- Breakout 2 (Llano)
  - Compositional Formal Methods
  - Led by George Dinolt
- Breakout 3 (Pecos)
  - Assurance for Pragmatic Composition of COTS HW & SW
  - Led by Gordon Uchenick
- Breakout 4 (Directors)
  - Composition of Security Policies
  - Led by Ravi Sandhu