Design and Verification of Systems for Cyber Resiliency

October 10, 2017

Abstract: The state-of-the-art in systems engineering is very adept at engineering systems for a variety of non-functional properties. These properties include such things as reliability, durability, and availability, also including safety and performance. Colloquially, these properties are known as the –ilities. Unfortunately, cyber properties are not included in the systems engineering domain. A new program at DARPA is looking to advance the state-of-the-art in formal methods technologies to allow systems to be designed for cyber resiliency. This talk will highlight the technical challenges and the approached being developed by the Cyber Assured Systems Engineering (CASE) program. Technical challenges being addressed on the CASE program include:

- Deriving cyber resiliency requirements
- Supporting the human designer to
- Verify resiliency properties at design time
- Make rational tradeoffs between –ilities and resiliency, when necessary
- Designing run-time validation of resiliency requirements
- Reduce resiliency sensitivity to legacy software
- Adapt legacy software for use with resiliency requirements
- Expand the capabilities of low-level analysis tools
- Scalability
- Usable, rich feedback to the human designer

Bio for Dr. Raymond Richards: Dr. Raymond ("Ray") Richards joined DARPA in January 2016. His research interests focus on high assurance software and systems.

Dr. Richards joined DARPA from Rockwell Collins Advanced Technology Center (ATC) where he led a research group focused on automated analysis, cyber, and information assurance. In this role he helped to foster the industrial use of formal methods verification to support security accreditations. He also served as the liaison to U.S. Government S&T funding agencies for Rockwell Collins. He has performed research in the formal modeling and analysis of high assurance systems. He led the software development for a high-assurance cross-domain guard, and the formal modeling and analysis effort of a real-time operating system, in support of a Common Criteria EAL6+ evaluation. Dr. Richards has over 20 years of experience in leading the development of state-of-the-art computer hardware, software and systems. Dr. Richards has experience in developing real-time software ranging from high fidelity ground vehicle simulators, to safety critical software for air transport aircraft.

Dr. Richards holds an MBA degree, Ph.D. and M.S. degrees in Electrical and Computer Engineering, and a B.S. degree in Electrical Engineering, all from the University of Iowa. He has several publications in the area of formal methods/software security analysis and one patent.