Automated Rapid Certification of Software

Current certification practices are antiquated and unable to scale with the amount of software deployed by the Department of Defense (DoD). Two factors prevent the needed scalability. These factors are the use of human evaluators to determine if the system meets certification criteria, and a lack of a principled means to decompose evaluations. The use of humans to evaluate the quantities of assurance evidence that support software systems results in superficial, incomplete, or tremendously long evaluations. The amount of evidence needed to determine software conformance to certification can be overwhelming to human subject matter experts. Human evaluators also have individual sets of expertise, experience, and biases that influence their approach to evaluations. Moreover, because certification requirements may be vague or poorly written, evaluators often must interpret what is intended. Combined, these factors result in inconsistencies over time and across evaluations.

Currently, there is no means to compose evaluations in a principled and trustworthy manner. Composed evaluations would allow subsystems or components to be evaluated independently and the results of those evaluations leveraged as assurance evidence in the composed systems. This would amortize the effort of evaluating any component over all systems using that component. Current practice requires re-evaluation of components and their assurance evidence in every system that employs them. Our inability to use a divide and conquer approach to certification of large systems increases the cost and time of performing these certifications.

Two factors will support the acceleration of software certification through the automation of evaluations. First, the DoD has articulated its intentions to have its contractors modernize their engineering processes in the DoD Digital Engineering Strategy. The goal of this strategy is to move away from document-based engineering processes and towards design models that are to be the authoritative source of truth for systems. Such a future does not lend itself to current certification practices, but it will facilitate the automated evaluation of assurance.

Second, advances in several technologies provide a basis for confidence that automated evaluation of assurance evidence to support certification is possible. Model-based design technology, including probabilistic model checking shows an emerging capability of reasoning over a design in the face of uncertainty. So-called Big Code analytics have pioneered the application of semantic-based analytics to software and its associated artifacts. Mathematically rigorous analysis and verification provide the ability to develop software implementations that are demonstrably correct and sound. Assurance case languages provide us a means for expressing arguments on how software fulfills its certification goals, in a manner that is machine-readable.

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 foster the industrial use of formal methods verification to support security accreditations. Dr. Richards holds Master of Business Administration, Doctor of Philosophy and Master of Science degrees in electrical and computer engineering, as well as a Bachelor of Science degree in electrical engineering, all from the University of Iowa. He has nine publications in the area of formal methods/software security analysis and one patent.
Automated Rapid Certification of Software

Presentation HCSS 2019