Correct or Usable? The Limits of Traditional Verification (Impact Paper Award)

Daniel Jackson
Massachusetts Institute of Technology, USA
dnj@mit.edu

Mandana Vaziri
IBM, USA
mvaziri@us.ibm.com

ABSTRACT

Since our work on verification sixteen years ago, our views of the role of verification, and the centrality of correctness, have evolved. In our presentation, we'll talk about some of our concerns about the limitations of this kind of technology, including: usability as a key factor; the unknowable properties of the environment; and the inadequacy of specifications as a means of capturing users' desires. We'll describe two approaches we're currently working on to mitigate these concerns — (1) moving to higher level abstractions with correctness by construction and (2) focusing on the conceptual structure of applications — and will argue that, combined with traditional verification tools, these offer the possibility of applications that are both usable and correct.

CCS Concepts

• **Software and its engineering→Software verification**

Keywords

Software Verification; Software Design

FSE'16, November 13–18, 2016, Seattle, WA, USA
© 2016 ACM. 978-1-4503-4218-6/16/11...$15.00
http://dx.doi.org/10.1145/2950290.2994161

BIOGRAPHIES

Daniel Jackson is Professor of Computer Science at MIT, a MacVicar teaching fellow, and an Associate Director of the Computer Science and Artificial Intelligence Laboratory, where he leads the Software Design Group. He is the lead designer of the Alloy modelling language, and author of "Software Abstractions: Logic, Language, and Analysis" (MIT Press; second ed. 2012). He was chair of the National Academies' study "Software for Dependable Systems: Sufficient Evidence?" (2007). His research currently focuses on a new approach to software design, on new programming paradigms, and on cybersecurity.

Mandana Vaziri is a Research Staff Member at IBM's T.J. Watson Research Center. She has worked on different projects in the area of Programming Languages and Software Engineering, most notably data-centric synchronization (Atomic Sets), the IDE for IBM's X10 language (X10DT), and a spreadsheet interface for IBM's Stream Processing Language (ActiveSheets). She holds a PhD from MIT working with Daniel Jackson on analyzing imperative code with a SAT solver.