The software safeguard

Professor Dino Distefano is a world leader in software security, developing routines and systems to ensure that complex programs are secure and reliable and contain no hidden errors that could lead to unintended consequences.

ROYAL ACADEMY OF ENGINEERING

Research area

Dino Distefano is a Professor of Software Verification at Queen Mary, University of London and a pioneer in the growing area of software security. He leads both academic and commercial research teams developing mathematical models that find mistakes in software – errors that, in some applications, could be safety-critical. In the same way that compiler tools do checks in computer programs for incorrect syntax, Professor Distefano' s tools construct a mathematical model of what software programs will do when they run and identify when they might misbehave.

From a background of applying mathematical logic to verify the correctness of systems, Professor Distefano has concentrated on software verification for the past 10 years and is credited with development of the first separation logic program analysis tool. The core theory behind this work is to separate the computer code into discrete areas and test the each area individually rather than the entire code at once. For example, the separation logic program analysis tool would only check the memory used by the program, and not the entire system, and therefore would work much faster than conventional proving tools. Under the RAEng/EPSRC Research Fellowship, he has been working on automating verification of industrial and large-scale software: programs of the kind that are used where errors can have safety and reliability implications. He and his co-researchers founded a company, Monoidics, to commercialise the results of their research.

Key achievements

Developed Space Invader, the first separation logic program analyser

Shortlisted for Times Higher Education Supplement Research Project of the Year, 2008

Winner, Roger Needham Award for contributions to computer science, British Computer Society 2012

Microsoft Research developed internal software tool for software verification based on his work

Professor Distefano's start-up company, Monoidics, was acquired by Facebook in July 2013

Academy support

Professor Distefano was backed by the RAEng/EPSRC Research Fellowship which helped him focus and achieve the goal of automating the software checking routines. He said, "I think it's one of the greatest things the UK has that it gives support to young engineers and scientists to enable them to concentrate on their research and be relieved of teaching and admin duties. I don't think I could have done what I've done without this support."

Other support

Professor Distefano' s work has been an inspiration for many other research programmes, including University of California, Berkeley and Princeton University. His collaborations span across academic organisations and commercial entities such as Microsoft Research Laboratories at Cambridge. His company, Monoidics, works with leading commercial software companies and is part of a €4.1 million European-funded research programme. He is also backed by EPSRC (The Engineering and Physical Sciences Research Council) funding of more than £750,000.

Research impact

"Software engineering is everywhere but it is still a very new discipline. In other parts of engineering that have been around for a long time, such as building bridges, for example, you have a strong mathematical foundation that gives engineers tools that enable them to build a model and know that the bridge isn't going to collapse. Software engineering is a young branch of engineering and we are just now developing these kinds of mathematical tools," Professor Distefano said. The automatic verification essentially constructs a mathematical model of what a complex software program will do when it runs and identifies any undesired behaviours. The tools deduce the behaviours without actually running the software and flag up errors.

"For industrial software, to do this manually would take an army of PhD people but now an engineer can just press the button and it does it automatically," Professor Distefano said.

The initial impact of this work has been in areas where software performance is safety critical: aerospace, automotive industries, defence and power. Modern aircraft and cars, for example, have tens of millions of lines of code inside them, often controlling critical functions. Leading companies, therefore, have long been keen to verify the software they use. Professor Distefano believes that automation will soon make this a mainstream technology: "Before, it was elite and expensive, and you needed experts to do it. Now everyone can use it."

Professor Distegano sees particular application in areas such as the operating systems of mobile phones, where the software suppliers and network operators are under extreme pressure to innovate constantly. "This provides a means to keep the quality standards that they need while remaining innovative," he said.

One of Professor Distefano's major and most recent achievements has been the acquisition of Monoidics, a company he co-founded in 2009, by Facebook. "Monoidics specialises in automatic formal verification and analysis of software. Its aim is to bring verification and program analysis research to the forefront of industrial practice", he said.

Future challenges

Professor Distefano sees his work developing in two particular directions: one is cyber security, which is coming to the fore with the ubiquitous mobile phone but which is likely to grow further with embedded software in many other products used everyday. The other direction he expects his work to take comes with the continued increase in computing power, particularly through multicore processors, the full use of which requires more complex software.

Biography/ Career Progression

1999 to 2003 PhD in systems verification, University of Twente, The Netherlands

2003 to 2007 Postdoctoral researcher, Queen Mary, University of London

2007 to 2013 RAEng/EPSRC Research Fellowship

2009 to Present Founding partner and originally CEO of Monoidics

2012 to Present Professor of Software Verification, Department of Computer Science, Queen Mary, University of London

"We are dealing with real problems in software and our contacts with industry are giving us some very interesting real-life issues to work on."

Professor Dino Distefano