

NATIONAL UNIVERSITY OF SINGAPORE

School of Computing

C S S E M I N A R

Title: Network Verification in Microsoft Azure

Speaker: Nikolaj Bjorner
Principal Researcher
Microsoft Research, Redmond

Date/Time: 11 April 2017, Tuesday, 02:00 PM to 03:30 PM

Venue: Executive Classroom, COM2-04-02

Chaired by: Dr Jaffar, Joxan, Professor, School of Computing
(joxan@comp.nus.edu.sg)

Abstract:

Modern large-scale cloud infrastructures are inherently complex to configure and deploy: Network access restrictions are enforced at multiple points, forwarding and filtering policies are programmed or configured in various formats targeting devices that span different vendors and generations. On the other hand, well-designed infrastructures, such as Microsoft Azure, are based on a set of transparent well-motivated principles. These principles can be captured using a set of high-level contracts that can be enforced throughout the life-cycle of a deployment. Contracts typically capture partial specifications (e.g., a DNS port of a DNS server must be permitted in firewall rules), and it is possible to formulate more comprehensive contracts that capture how forwarding logic must be configured in data-centers. Many contracts can be captured in fragments of first-order logic. We describe a set of Network Verification tools based on the Satisfiability Modulo Theories solver Z3. The SecGuru tool checks cloud contracts in the Microsoft Azure public cloud infrastructure. SecGuru models network configurations using quantifier-free logical formulas over bit-vectors. We also describe several techniques for checking reachability properties in networks. These techniques include using symmetries and surgeries for simplifying reachability checking in large data-center networks and using trie-based data-structures to represent equivalence classes of IP forwarding networks. We think that Network Verification is an important and exciting new opportunity where formal methods and modern theorem proving technologies play an important role.

Biodata:

Nikolaj Bjorner is a Principal Researcher at Microsoft Research, Redmond, working in the area of Automated Theorem Proving and Software Engineering. His current main line of work with Leonardo de Moura and Christoph Wintersteiger is around the state-of-the art

theorem prover Z3, which is used as a foundation of several software engineering tools. Z3 received the 2015 ACM SIGPLAN Software System award and most influential tool paper in the first 20 years of TACAS in 2014. Previously, he developed the DFSR, Distributed File System - Replication, and Remote Differential Compression protocols, RDC, part of Windows Server since 2005 and before that worked on distributed file sharing systems at a startup, and program synthesis and transformation systems at the Kestrel Institute. He received his Master's and Ph.D. degrees in computer science from Stanford University, and spent the first few years of university at DTU and DIKU.