CITY
UNIVERSITY OF LONDON
EST 1894

84th IFIP 10.4 Meeting – Arcos de Valdevez, Portugal

Session 3 summary

Presented by Ilir Gashi

Overview

- Title of session: **Share your view on the future of dependable computing and fault tolerance**
- The Future of Dependable Distributed Systems is Simple
  - **Alysson Bessani**, University of Lisboa, Portugal
- Dependability in practice: How to do it?
  - **Razvan Beuran**, JAIST, Japan
- The Future of Dependability: Perspectives
  - **Elias Duarte**, Federal University of Paraná, Brazil
- Dependable future mobile networked systems
  - **Ahmed Helmy**, University of North Carolina at Charlotte, US
- Testing Software Out-of-House: How to Make it Reliable while Ensuring Code Privacy
  - **Ibéria Medeiros**, University of Lisboa, Portugal

The Future of Dependable Distributed Systems is Simple

- The context of the talk is on consensus-based systems for doing replication.
- First gave an overview and distinction between group communication vs coordination services
- Explained Practical BFT system (PBFT) – practical version of paxos
- After PBFT several works tried to improve the performance of PBFT
  - 1st generation: Fast & Complex
  - 2nd generation: Resilient and Modular
  - 3rd generation: Blockchain inspired (Chained consensus, Simple block approval protocol
- Alysson concluded with the view that "**Distributed computing real world impact is driven by simplicity. Simple designs always win**"
  - "**Simplicity is pre-requisite for reliability**" – Edsger Dijkstra
- Some more details from questions and discussion:
  - **Need diversity on the replicas** to provide better dependability
  - Degree of the simplicity of the systems will come at the cost of the assumptions you have to make about the environment.

Dependability in practice: How to do it

- Started with the view that theoretical aspects of dependability are well established, but not always clear on applicability to practical situations
- Context was exemplified by the use case of “Society 5.0”, and **smart buildings**: intelligent buildings that use a multitude of sensors and a central management system (Building OS) and strive for achieving predictive maintenance, operation efficiency, comfort, high security etc (examples, smart factories, smart hospitals etc)
- They are working on defining an IoT trustworthiness assurance framework. Using different assurance levels to differentiate requirements and assessment methods (with current focus on smart buildings)
- His question to the group was “How to address dependability/trustworthiness assurance for complex systems in practice”
- A suggestions from Robert during Q&A was to look at the EU project called **DSoS on Dependable Systems of Systems** (Robert to forward a reference). Aad also suggested to look at Formal methods paper on systems of Systems from John Fitzgerald at Newcastle (link on Slack), and also at the special interest group on SoS from INCOSE (link on Slack).

The Future of Dependability: Perspectives

- Nice comic-book-style talk from Elias
- My take on it was that since systems are getting ever more complex with ever more complex requirements which are difficult to specify and build correctly, then dependability challenges will remain (and so will the need for groups such as 10.4)
- A comments from the Q&A that with these ever more complex systems comes the need for more interdisciplinary collaborations to study dependability challenges (e.g. with CHI conference on HCI issues etc), as well as the need to make our “bible” better understood and more approachable from a wider community.

Dependable Future Mobile Networked Systems

- Started with a description of multicast routing as an example of a complex system that then became even more complex with the advent of mobility and increasing complexity of new applications and environments (including smart cities etc)
- Listed a few network challenges going forward:
  - ➢ Identifying breaking points for dynamic unexplainable networks
  - ➢ State space coverage
  - ➢ Building on unreliable blocks
  - ➢ Human in the loop, unpredictable behavior
  - ➢ Need multi-disciplinary approaches
- Identified as the “main challenging frontier” subjects related to medicine (Connected health, precision medicine, biotech)
- The Q&A discussed some aspects (and difficulties) of doing multidisciplinary (or interdisciplinary) research effectively.

Testing Software Out-of-House: How to Make it Reliable while Ensuring Code Privacy

- Challenge: software continues to have many vulnerabilities, due to, for example, competitive pressure to rush to market means many aspects are not tested properly
- Static analysis is one of the tools available to detected vulnerabilities, biut concerns about privacy if code has to go "out-of-house" for testing.
- Idea:
  - ➢ Encrypt the code and, without decrypting it, do searches over it to find vulnerabilities
  - ➢ The code can be stored in a public storage
  - ➢ Code privacy is preserved
- Challenges:
  - ➢ How to get code privacy with support to code analysis?
  - ➢ Which data structure is able to maintain code privacy while performing code analysis?
  - ➢ How to find vulnerabilities over encrypted code when static analysis cannot understand the data?
- Some initial analysis on finding vulnerabilities (SQLi and XSS) on web applications look promising (89% precision).
- The Q&A discussed some reasons for some many vulnerabilities (cost of doing testing; applications are wanted faster, better but also cheaper, so costs are usually cut on testing)

Thank you!

- Correction/editions/clarifications are welcome (from authors and audience).
- A slack channel was also created and there have been some contributions and questions from participants, so please have a look: https://bit.ly/ifipsession3