Assessing and Improving Dependability and Security of CI/CD Infrastructures

Extended Abstract

Thomas F. Düllmann[1]
[1] University of Stuttgart, Germany
duellmann@iste.uni-stuttgart.de

Nowadays, Continuous Integration (CI) or even Continuous Delivery (CD) is adopted in many software development processes in companies and also in the open source community. It supports agile methods and allows developers to have their code contributions checked against the common requirements and — in case of CD — even have it deployed to production after all checks were successful.
As CI/CD have become an integral part of software development, developers are used to and heavily rely on the support by these tools. In case CI/CD would not work anymore, the workflow of the developers would be slowed down or even obstructed. Due to these consequences, we claim that CI/CD systems have become a business-critical infrastructure.
In our talk we will present our overall motivation, vision, and preliminary results to improve the dependability of CI/CD infrastructures [1].
The talk covers the following parts:
- Results of our investigations on what CI/CD pipelines are in practice, and potential vulnerabilities from a security point of view [2].
- Transformation of CI/CD pipelines (declarative Jenkinsfiles) to an abstract DSL (StalkCD) that acts as a layer to transform them to BPMN and back, which gives us the means to incorporate BPMN tooling on CI/CD pipeline workflows [3].
- Empirical analysis of publicly available data of CI builds to be able to reason about typical real-world pipelines, their performance, and workload, as well as to have a basis for abstracting them to Stochastic Petri Nets.
- Our work in progress to use the StalkCD DSL in combination with deriving performance models from real-world pipeline data.

Acknowledgements

The presented work is conducted with several colleagues, including:
Christina Paule, Oliver Kabierschke, Alireza Mir Hakamian, André van Hoorn, Cor-Paul Bezemer, also as part of the SPEC RG DevOps Performance Working Group.

References

[1] "Exploiting DevOps Practices for Dependable and Secure Continuous Delivery Pipelines" (Düllmann, Paule, van Hoorn), RCoSE Workshop, ICSE 2017
[2] "Vulnerabilities in Continuous Delivery Pipelines? A Case Study" (Paule, Düllmann, van Hoorn), QUDOS Workshop, ICSA 2019
[3] "Resilient Continuous Delivery Pipelines Based on BPMN" (Oliver Kabierschke), Master's Thesis, University of Stuttgart (Germany), 2019