

Speaker: Steven Raemaekers (TU Delft)

Title: Exploring Risks in the Usage of Third Party Libraries

Abstract: Third party libraries can be beneficial to reduce development time and costs, but there are also various risks associated with it, such as lower quality standards or security risks. The goal of this paper is to explore to what extent risks

involved in the use of third party libraries can be assessed automatically. To that end, we first of all propose a 'commonality rating' which is based on frequency of use in a corpus of 103 open source and 178 proprietary systems.

Furthermore, we propose an 'isolation rating' which measures concentration and distribution of import statements of third party libraries through packages of a system. We evaluate the proposed rating methodology by conducting a number of case studies on both open source and commercial systems, in which we compare our ratings with a qualitative assessment of library risks involved in those systems. Other system properties which could serve as risk indicators are also investigated.