

# Cobbles and Potholes – On the Bumpy Road to Secure Software Supply Chains

Henrik Plate  
*SAP Security Research, Germany*

*Abstract* — Open source software is ubiquitous – all across the stack, in the cloud and on-premise, on all devices, in commercial and non-commercial offerings. This success, the dependency of the software industry on open source, combined with recent data breaches and attacks, puts security into the spotlight. This talk will provide an overview - for sure opinionated, hopefully controversial – about the state of affairs and current trends regarding the security of software supply chains, both from consumer and producer perspective.

*Brief Biography* — Henrik Plate is a senior researcher at SAP Security Research. He received his MSc in Computer Science and Business Administration in 1999 from the University of Mannheim. His current research focusses on the security of software supply chains, esp. the use of open source components with known vulnerabilities and supply chain attacks. He is a co-author of Eclipse Steady [5], which supports the detection, assessment, and mitigation of vulnerable open source dependencies in Java and Python applications.