Attack investigation is a notoriously challenging problem due to a large volume of system audit logs and the huge dependency graphs formed from such logs, which are hard for even experienced security analysts to investigate. DepImpact provides an innovative solution to this problem: edges of interest (depicting an attack) in a dependency graph typically have a well-defined set of properties and are related to a few events. By precisely pinpointing these edges, DepImpact makes analysis on system logs exceptionally effective. In particular, to identify these edges, DepImpact provides a new metric to assign weights in a discriminatory manner for critical edges, performs backwards dependency from an interesting edge to its entry point in the system, and forward analysis to prune out edges that have no causal impact later on in the lifecycle of the system. Notably, by applying this technique, the dependency graph produced by DepImpact is three orders of magnitude smaller than existing graphs.

I found DepImpact to be exceptionally innovative for several reasons. First, it is tackling an important problem in today's world of increasingly-frustrating cyber-attacks and ineffective defense mechanisms, particularly when it comes to post-mortem analysis of attacks. Second, it is the first unsupervised attack investigation approach that is also not hampered by the lack of attack problems. Third, it is well-tested on a large real-world open dataset and its tools are available for others to deploy in the future. Hence, I would like to nominate DepImpact for the 11th Annual Best Scientific Cybersecurity Paper Competition.