Title : Securing GitHub Workflows Against API Abuse in Software Supply Chains

Author : Mojtaba Moazen , Phd Student , KTH

Supervisor : Musard Balliu

Type of Presentation: Short -talk

Abstract :

I will present ongoing research on improving the security of GitHub workflows, which are widely used in software development pipelines. This work focuses on API abuse attacks, where compromised or hijacked GitHub Actions misuse API tokens beyond their intended scope, potentially leading to serious supply chain attacks. Our approach introduces finer-grained security enforcement mechanisms, enabling more precise control and monitoring of API usage during workflow execution.