Recommender systems for software vulnerabilities

Linus Karlsson
Lund University

Joint work with:
Martin Hell, Pegah Nikbakht Bideh, and Nicolae Paladi

May 3, 2019

New software vulnerabilities are presented every day, and it is important to analyse and assess vulnerabilities to determine their relevance. Software today is typically built by using a plethora of external components, combined to create a final product. As the number of such external components grows, the resources required to monitor and analyse potential vulnerabilities in software libraries increases. Performing this analysis may be both costly and slow.

To address this problem, we present a recommender system for software vulnerabilities. The recommender assists analysts by prioritizing vulnerabilities based on their properties. The system is extensible and considers a variety of different vulnerability properties when creating the prioritization. An important difference compared to previous work in the area is that the recommender also considers both explicit and implicit user profiles. This allows each user to have an individual profile, and ensures that the prioritization is tailored for a single user, as opposed to currently existing metrics such as the CVSS score. An implementation of the proposed recommender was made, and an evaluation of the recommender shows promising results compared to previous metrics.

Maintaining such profile information about users may, however, also pose a security threat. A malicious third-party with access to vulnerability prioritization data may use such information to perform targeted attacks. We address this problem separately, by proposing a solution to protect the user profile information from being mapped to individual users. The proposed solution uses isolated execution environments, combined with inspiration from differential privacy. A proof-of-concept implementation is evaluated and shows that the proposed solution is practical and can complement current recommender systems.