Thesis Proposal

Institute for Software Research
Software Engineering

Towards Practical and Trustworthy Package Management

Gabriel Ferreira

Thursday, December 12th, 2019
2:30 PM - 4:30 PM
Gates & Hillman Center 8102

The amount of third-party packages available and the fast-moving pace of software ecosystems enables attackers to compromise machines by pushing malicious updates to package dependencies that are part of the supply chains of applications. Studying the npm repository, we observed that (i) many packages are simple and do not need access to security-relevant resources such as to the filesystem or to the network, and (ii) most of the package updates are not malicious. These observations offer the opportunity (i) to enforce least-privilege on packages that are part of applications, protecting users from malicious packages when running their applications and (ii) to use anomaly detection to identify updates with potential malicious intent, protecting users from malicious updates when installing/updating their applications.

My research seeks to improve the state-of-art and state-of-practice of security of package management. In this thesis, we focus on designing and evaluating technical solutions to achieve a more practical and trustworthy package management in the Node.js/npm ecosystem with (i) a package-level permission system that enforces least-privilege on packages that use security-relevant APIs at runtime, contributing to a higher resistance to attacks while requiring low performance overhead and minimal changes in existing infrastructure, and (ii) a package update anomaly detector that defers package updates with potential malicious intent, contributing to a more timely detection of potential attacks at update-time, while being automated and integrating seamlessly with developers' workflow.

The goal of our proposed solutions is to improve the current state-of-practice, that have not been able to contain recent real attacks. Both solutions are automated and require no manual effort from developers, protecting applications against packages by deferring the installation of package updates that attempt to use security-relevant APIs without permission and against package updates with suspicious characteristics. Nevertheless, developers will be informed of potentially malicious operations by packages and package updates, creating awareness of potential security problems associated to package dependencies when searching for packages, when installing/updating packages, and when running applications with package dependencies from other npm users. Our findings inform the design of tools and open-source platforms that aim for more practical and trustworthy package management.

**Committee: Dr. Christian Kästner (Chair), Dr. Limin Jia,
Dr. Jonathan Aldrich, Dr. Jonathan Bell (George Mason University)**

isr institute for SOFTWARE RESEARCH | Carnegie Mellon University School of Computer Science