New tool automates the formal verification of systems software

October 30 2023, by Bernadette Young

Tang Family Assistant Professor of Computer Science Rongui Gu (left) and Professor of Computer Science Jason Nieh (right). Credit: Columbia Engineering

Formal systems verification, which mathematically proves that code is secure in all circumstances, is a relatively new technology. Software is getting more complex and harder to get right using traditional software testing techniques. Making software correct, safe, and secure is

becoming even more critical as the use of generative AI techniques like ChatGPT to automatically write programs increases. In fact, there will be even more need for verification to ensure those automatically generated programs are correct.

Recent work directed by professors Ronghui Gu and Jason Nieh introduced a new tool, Spoq, that significantly reduces the complex efforts people must use to verify real-world software and makes it possible to verify existing C systems code without modifications.

Formal verification offers a systematic and rigorous approach to software and hardware verification, helping to ensure that systems behave correctly and meet their intended specifications. With Spoq, many aspects of formal verification can be automated, significantly reducing manual proof efforts for verification. The paper was presented at the 17th USENIX Symposium on Operating Systems Design and Implementation (OSDI) Conference on July 12, 2023.

System software forms the software foundations of our computing infrastructure. Modern system software is large, complex, and imperfect, with vulnerabilities that can be exploited to compromise the security of a system. Formal verification offers a potential solution to this problem by mathematically proving that system software can provide critical security guarantees. Unfortunately, it remains too difficult and requires too much human effort to apply in practice.

Previous tools developed by Nieh's and Gu's teams introduced verification techniques to make certain proofs possible that could not have been done before. Spoq's key feature is that it automates the tedious and time-consuming parts of many proofs. "Spoq can generate results in about an hour compared to doing it manually, which can take months or years to formally verify a system," says Xupeng Li, the paper's lead author and a Ph.D. student with both Nieh and Gu.

Over the next few months, the lab is focused on making Spoq open-source so that formal verification can be widely deployed to secure the foundations of our computing infrastructure's software.

The study is titled "Spoq: Scaling Machine-Checkable Systems Verification in Coq."

More information: Study: www.usenix.org/conference/osdi … esentation/li-xupeng

Provided by Columbia University School of Engineering and Applied Science