New, free tool adds layer of security for the software supply chain

December 15 2020

Credit: CC0 Public Domain

The software supply chain has long been a prime target for cyberattacks, putting servers, IoT devices, personal computers, and connected equipment from surgically embedded devices to avionics at risk of

sabotage. These risks will increase dramatically with the global rollout of such new technologies as 5G telecommunications, and new tools will be required to affirm the security and authenticity of software projects. Against this backdrop, in-toto, an open-source tool developed by researchers at the NYU Tandon School of Engineering that provides an unprecedented level of assurance against such attacks, announces it has hit a significant milestone with the release of its first major version.

In-toto, a free, easy-to-use framework that cryptographically ensures the integrity of the software supply chain, was developed in 2016 by Justin Cappos, a professor of computer science and engineering, and Santiago Torres-Arias, a former Ph.D. student at NYU Tandon, now a professor at Purdue University. Since its advent, in-toto has been adopted or integrated into several major open source software projects, including those hosted by the Cloud Native Computing Foundation, a part of the Linux Foundation. With the release of version 1.0, in-toto has reached a level of maturity where its developers can ensure its quality, and guarantee its security to potential adopters.

Like blockchain for the software development process, in-toto ensures that all steps performed on a piece of software throughout its design and development lifecycle can be trusted by providing information crucial to security. Because of the decentralized nature of software development, the multi-step process of writing, testing, packaging, and deploying new software provides many opportunities for an attacker to insert malicious code or otherwise compromise the finished product. In experiments conducted last year re-creating more than 30 real-life software supply chain compromises that impacted hundreds of millions of users, the NYU Tandon team found that in-toto would have effectively prevented at least 83% of those attacks.

Torres-Arias, who leads the in-toto project and did his dissertation on the topic, first presented the work in August 2019 at the USENIX

Security Symposium. The paper, "In-toto: Providing farm-to-table guarantees for bits and bytes" is publicly available.

"As it moves from development to testing to packaging, and finally to distribution, a piece of software passes through a number of hands," Torres-Arias affirmed. "By requiring that each step in this chain conforms to the layout specified by the developer, it confirms to the end-user that the product has not been altered for malicious purposes, such as by adding backdoors in the source code."

"These attacks are surprisingly common," Cappos explained, adding that once a compromised piece of software is downloaded or installed, there is little users or software developers can do beyond assessing the damage. According to Sonatype's 2020 State of the Software Supply Chain Report, 2020 saw a 430% increase in next-generation software supply chain attacks since the firm's 2019 report.

In-toto works by allowing each company or organization to establish a set of rules or protocols that must be followed—and by whom—during each step of software development. As each step is completed, in-toto collects link metadata—cryptographically verifiable statements attesting that the step was performed in accordance with guidelines. This process circumvents a common security pitfall within the software supply chain; namely, that it is difficult to track malicious activity that occurs during a particular step of development or packaging rather than during the transition from one step to another. The link metadata provides a high level of control over the process, ensuring that even if a compromise occurs, it can be localized and its impacts limited.

In-toto has collaborated with open source communities such as Git, Docker, Datadog and OpenSUSE. It is also part of the Cloud Native Application Bundle (CNAB), an open-source project that facilitates the bundling, installing and managing of container-native applications. Ralph

Squillace, Principal Program Manager for Microsoft Azure Computer's Application Platform team and a contributor to CNAB, noted that in-toto was picked for the specification's supply chain attestation approach in v1.0 "precisely because it was open-source and applied precisely to the problems of supply chain confidence the community expects distributed applications to have in the real world." He adds that "there are many possible ways of handling the problem, but in-toto can be used anywhere and is developed in public by an engaged community. We hope to expand its usage and support it in our work going forward."

Trishank Kuppusamy (Ph.D., '17), who worked on the project and is now staff security engineer at Datadog points out that what separates in-toto from other security systems is that "it has been designed against a very strong threat model that includes nation-state attackers."

The in-toto development team also includes developer Lukas Pühringer, Ph.D. student Aditya Sirish, and undergraduate students Yuanrui Chen, Isha Vipul Dave, Kristel Fung, Cindy Kim and Benjamin Wu, all from the Secure Systems Laboratory at NYU Tandon; and doctoral students Hammad Afzali Nanize and Sangat Vaidya, together with Professor and co-director of the Cybersecurity Research Center Reza Curtmola, all from the New Jersey Institute of Technology.

Cappos and his lab are affiliated with the NYU Center for Cybersecurity at NYU Tandon. In-toto continues his advancement of the open-source protection of software: Most large-scale cloud computing is protected by The Update Framework (TUF), and a derivative called Uptane is used by the global auto industry to protect over-the-air software updates for vehicles. Both are also projects of the Linux Foundation's Cloud Native Computing Foundation.

"Together with TUF, in-toto is the only system that I know of that offers end-to-end security anywhere between developers and end-users," said

Kuppusamy.

More information: in-toto: Providing farm-to-table guarantees for bits and bytes: www.usenix.org/conference/usen … ntation/torres-arias

Provided by NYU Tandon School of Engineering