Keylime security software is deployed to IBM cloud

July 27 2021, by Kylie Foy

Credit: CC0 Public Domain

Keylime, a cloud security software architecture, is being adopted into IBM's cloud fleet. Originally developed at MIT Lincoln Laboratory to allow system administrators to ensure the security of their cloud environment, Keylime is now a Cloud Native Computing Foundation sandbox technology with more than 30 open-source developers contributing to it from around the world. The software will enable IBM to remotely attest to the security of its thousands of cloud servers.

"It is exciting to see the hard work of the growing Keylime community coming to fruition," says Charles Munson, a researcher in the Secure Resilient Systems and Technology Group at Lincoln Laboratory who created Keylime with Nabil Schear, now at Netflix. "Adding integrated support for Keylime into IBM's cloud fleet is an important step towards enabling cloud customers to have a zero-trust capability of 'never trust, always verify.'"

In a blog post announcing IBM's integration of Keylime, George Almasi of IBM Research said, "IBM has planned a rapid rollout of Keylime-based attestation to the entirety of its cloud fleet in order to meet requirements for a strong security posture from its financial services and other enterprise customers. This will leverage work done on expanding the scalability and resilience of Keylime to manage large numbers of nodes, allowing Keylime-based attestation to be operationalized at cloud data center scale."

Keylime is a key bootstrapping and integrity management software architecture. It was first developed to enable organizations to check for themselves that the servers storing and processing their data are as secure as cloud service providers claim they are. Today, many organizations use a form of cloud computing called infrastructure-as-a-service, whereby they rent computing resources from a cloud provider who is responsible for the security of the underlying systems.

To enable remote cloud-security checks, Keylime leverages a piece of hardware called a trusted platform module, or TPM, an industry-standard and widely used hardware security chip. A TPM generates a hash, a short string of numbers representing a much larger amount of data. If data are tampered with even slightly, the hash will change significantly, a security alarm that Keylime can detect and react to in under a second.

Before Keylime, TPMs were incompatible with cloud technology, slowing down systems and forcing engineers to change software to accommodate the module. Keylime gets around these problems by serving as a piece of intermediary software that allows users to leverage the security benefits of the TPM without having to make all of their software compatible with it.

In 2019, Keylime was transitioned into the CNCF as a sandbox technology with the help of RedHat, one of the world's leading open-source software companies. This transition better incorporated Keylime into the Linux open-source ecosystem, making it simpler for users to adopt. In 2020, the Lincoln Laboratory team that developed Keylime was awarded an R&D 100 Award, recognizing the software among the year's 100 most innovative new technologies available for sale or license.

This story is republished courtesy of MIT News (web.mit.edu/newsoffice/), a popular site that covers news about MIT research, innovation and teaching.

Provided by Massachusetts Institute of Technology

Citation: Keylime security software is deployed to IBM cloud (2021, July 27) retrieved 19 April 2024 from https://techxplore.com/news/2021-07-keylime-software-deployed-ibm-cloud.html