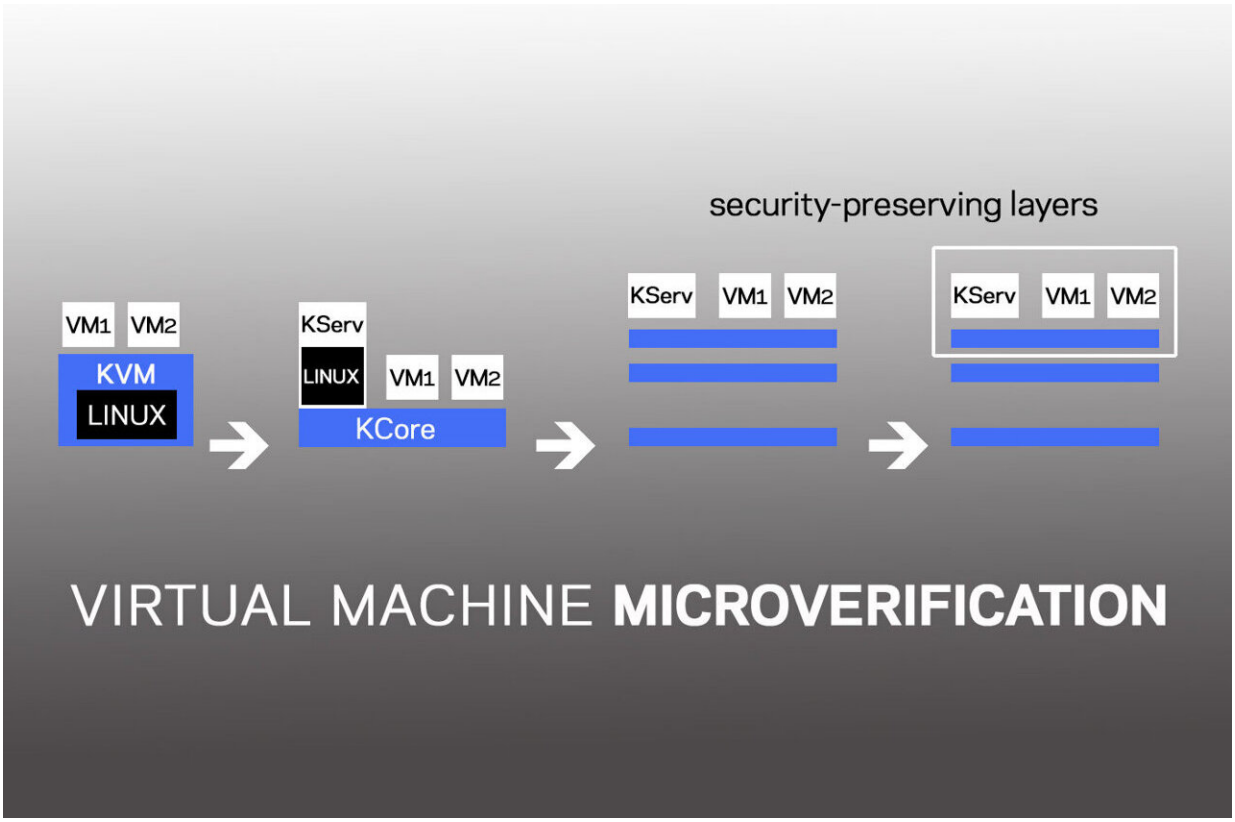
Team builds first hacker-resistant cloud software system

May 25 2021



Microverification of cloud hypervisors. Credit: Jason Nieh and Ronghui Gu/Columbia Engineering

Whenever you buy something on Amazon, your customer data is automatically updated and stored on thousands of virtual machines in the

cloud. For businesses like Amazon, ensuring the safety and security of the data of its millions of customers is essential. This is true for large and small organizations alike. But up to now, there has been no way to guarantee that a software system is secure from bugs, hackers, and vulnerabilities.

Columbia Engineering researchers may have solved this security issue. They have developed SeKVM, the first system that guarantees—through a mathematical proof—the security of virtual machines in the cloud. In a new paper to be presented on May 26, 2021, at the 42nd IEEE Symposium on Security & Privacy, the researchers hope to lay the foundation for future innovations in system software verification, leading to a new generation of cyber-resilient system software.

SeKVM is the first formally verified system for cloud computing. Formal verification is a critical step as it is the process of proving that software is mathematically correct, that the program's code works as it should, and there are no hidden security bugs to worry about.

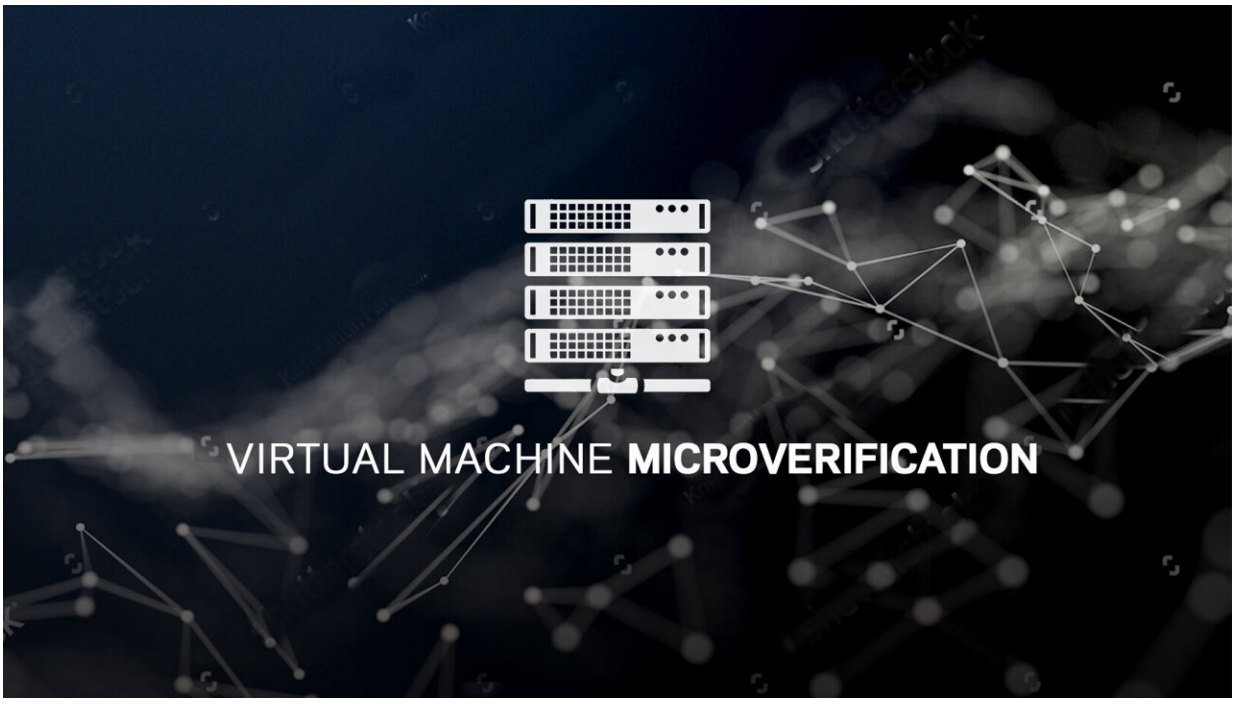
"This is the first time that a real-world multiprocessor software system has been shown to be mathematically correct and secure," said Jason Nieh, professor of computer science and co-director of the Software Systems Laboratory. "This means that users' data are correctly managed by software running in the cloud and are safe from security bugs and hackers."

The construction of correct and secure system software has been one of the grand challenges of computing. |Nieh has worked on different aspects of software systems since joining Columbia Engineering in 1999. When Ronghui Gu, the Tang Family Assistant Professor of Computer Science and an expert in formal verification, joined the computer science department in 2018, he and Nieh decided to collaborate on exploring formal verification of software systems.

Their research has garnered major interest: both researchers won an Amazon Research Award, multiple grants from the National Science Foundation, as well as a multi-million dollar Defense Advanced Research Projects Agency (DARPA) contract to further development of the SeKVM project. In addition, Nieh was awarded a Guggenheim Fellowship for this work.

Over the past dozen years, there has been a good deal of attention paid to formal verification, including work on verifying multiprocessor operating systems. "But all of that research has been conducted on small toy-like systems that nobody uses in real life," said Gu. "Verifying a multiprocessor commodity system, a system in wide use like Linux, has been thought to be more or less impossible."

The exponential growth of cloud computing has enabled companies and users to move their data and computation off-site into virtual machines running on hosts in the cloud. Cloud computing providers, like Amazon, deploy hypervisors to support these virtual machines.



Microverification of cloud hypervisors. Credit: Jason Nieh and Ronghui Gu/Columbia Engineering

A hypervisor is the key piece of software that makes cloud computing possible. The security of the virtual machine's data hinges on the correctness and trustworthiness of the hypervisor. Despite their importance, hypervisors are complicated—they can include an entire Linux operating system. Just a single weak link in the code—one that is virtually impossible to detect via traditional testing—can make a system vulnerable to hackers. Even if a hypervisor is written 99% correctly, a hacker can still sneak into that particular 1% set-up and take control of the system.

Nieh and Gu's work is the first to verify a commodity system, specifically the widely-used KVM hypervisor, which is used to run virtual machines by cloud providers such as Amazon. They proved that SeKVM, which is KVM with some small changes, is secure and guarantees that virtual computers are isolated from one another.

"We've shown that our system can protect and secure private data and computing uploaded to the cloud with mathematical guarantees," said Xupeng Li, Gu's Ph.D. student and co-lead author of the paper. "This has never been done before."

SeKVM was verified using MicroV, a new framework for verifying the security properties of large systems. It is based on the hypothesis that small changes to the system can make it significantly easier to verify, a new technique the researchers call microverification. This novel layering technique retrofits an existing system and extracts the components that enforce security into a small core that is verified and guarantees the

security of the entire system.

The changes needed to retrofit a large system are quite modest—the researchers demonstrated that if the small core of the larger system is intact, then the system is secure and no private data will be leaked. This is how they were able to verify a large system such as KVM, which was previously thought to be impossible.

"Think of a house—a crack in the drywall doesn't mean that the integrity of the house is at risk," Nieh explained. "It's still structurally sound and the key structural system is good."

Shih-Wei Li, Nieh's Ph.D. student and co-lead author of the study, added, "SeKVM will serve as a safeguard in various domains, from banking systems and Internet of Things devices to autonomous vehicles and cryptocurrencies."

As the first verified commodity hypervisor, SeKVM could change how cloud services should be designed, developed, deployed, and trusted. In a world where cybersecurity is a growing concern, this resiliency is highly in demand. Major cloud companies are already exploring how they can leverage SeKVM to meet this demand.

The study is titled "A Secure and Formally Verified Linux KVM Hypervisor."

The study will be presented at the 42nd IEEE Symposium on Security & Privacy on May 26, 2021.

More information: A Secure and Formally Verified Linux KVM Hypervisor, DOI: 10.1109/SP40001.2021.00049