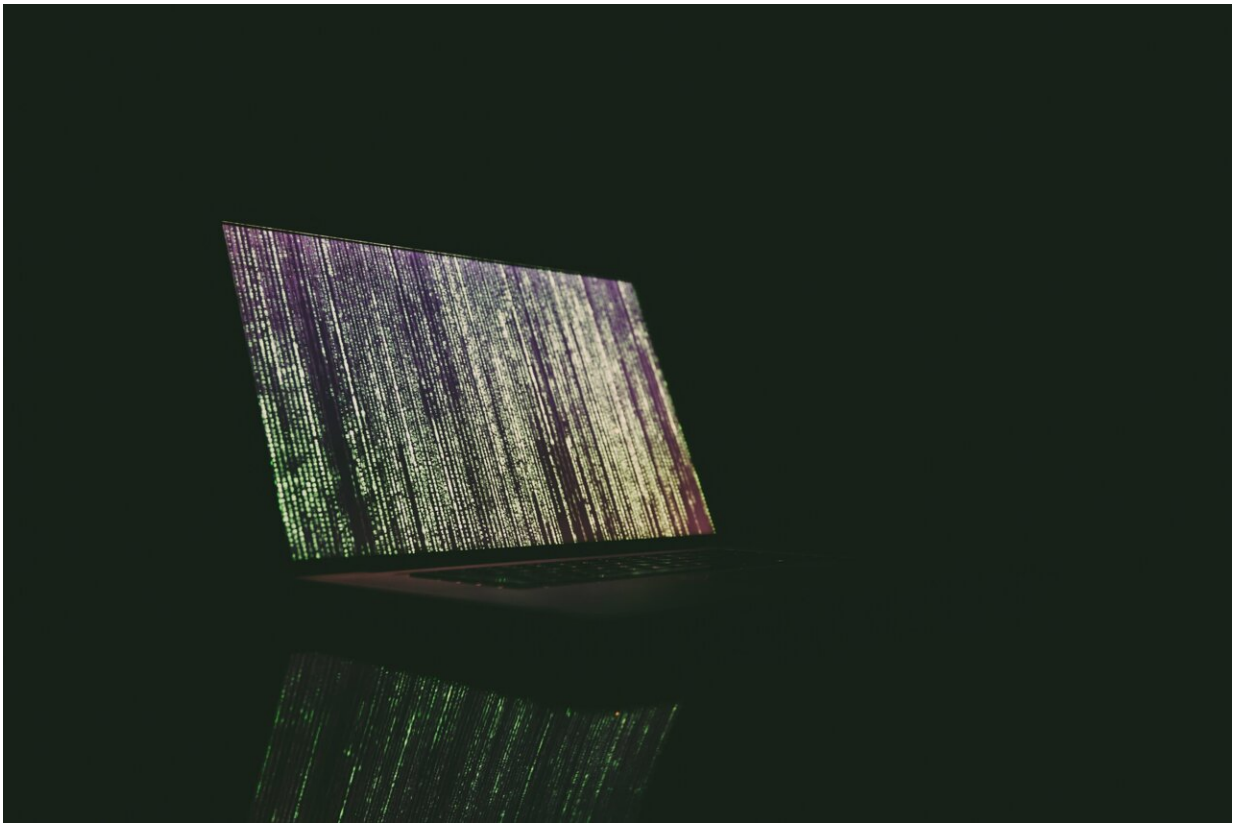
Researchers show they can steal data during homomorphic encryption

March 2 2022, by Matt Shipman



Credit: Unsplash/CC0 Public Domain

Homomorphic encryption is considered a next generation data security technology, but researchers have identified a vulnerability that allows them to steal data even as it is being encrypted.

"We weren't able to crack homomorphic encryption using mathematical tools," says Aydin Aysu, senior author of a paper on the work and an assistant professor of computer engineering at North Carolina State University. "Instead, we used side-channel attacks. Basically, by monitoring power consumption in a device that is encoding data for homomorphic encryption, we are able to read the data as it is being encrypted. This demonstrates that even next generation encryption technologies need protection against side-channel attacks."

Homomorphic encryption is a way of encrypting data so that third parties cannot read it. However, homomorphic encryption still allows third parties and third-party technologies to conduct operations using the data. For example, a user could use homomorphic encryption to upload sensitive data to a cloud computing system in order to perform analyses of the data. Programs in the cloud could perform the analyses and send the resulting information back to the user, but those programs would never actually be able to read the sensitive data.

"Homomorphic encryption is appealing because it preserves data privacy, but allows users to make use of the data," Aysu says. "While it has been theoretically possible for a while, homomorphic encryption requires a tremendous amount of computing power. As a result, we are still in the early stages of producing hardware and software to make homomorphic encryption practical."

Microsoft has been a leader in homomorphic encryption, and created the SEAL Homomorphic Encryption Library to facilitate research and development on homomorphic encryption by the broader research community.

"What we've found is that there is a way to 'crack' homomorphic encryption that is done using that library via a side-channel attack," Aysu says. "We were able to do this with a single power measurement."

The researchers were able to verify the vulnerability in the SEAL Homomorphic Encryption Library up through at least version 3.6.

"The library is constantly being updated, so we're not sure if this vulnerability will be addressed in the most recent versions—or if there may be new vulnerabilities that we haven't identified in more recent versions," Aysu says.

Side-channel attacks are well understood, and there are already countermeasures that organizations can put into place to thwart them.

"As homomorphic encryption moves forward, we need to ensure that we are also incorporating tools and techniques to protect against side-channel attacks," Aysu says.

The paper, "RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library," will be presented March 23 at the virtual DATE22 conference. First author of the paper is Furkan Aydin, a Ph.D. student at NC State. The paper was co-authored by Emre Karabulut, a Ph.D. student at NC State; Seetal Potluri, a postdoctoral researcher at NC State; and Erdem Alkim of Dokuz Eylul University.

More information: "RevEAL: Single-Trace Side-Channel Leakage of the SEAL Homomorphic Encryption Library" Presented: March 23, Design, Automation and Test in Europe Conference (DATE22) www.date-conference.com/programme

Provided by North Carolina State University

https://techxplore.com/news/2022-03-homomorphic-encryption.html