PHYS.ORG

How to secure the cloud

August 1 2014, by Angela Herring

With support from the National Science Foundation, cryptography expert Daniel Wichs, an assistant professor in the College of Computer and Information Science, will work as part of a multi-university team to develop better encryption techniques to improve cloud security.

For many of us, the primary reason we use "the cloud" is for storage—whether it's storing email through services like Gmail and Yahoo!, photos on Flickr, or personal documents on Dropbox. Many organizations like hospitals and banks utilize the cloud to store data on patient and customer information.

But there's also a computational side to the cloud that comes into play when, say, we search for an old email or perform complex analyses of large volumes of data stored there.

Regardless of the scenario, it's clear that precious personal information is stored in the cloud, and we'd like to think it's secure up there. Enter Daniel Wichs, an assistant professor in the College of Computer and Information Science. He is part of a multi-university research team that is working to make sure the cloud is as secure as possible. The project is supported by a grant project announced Thursday by the National Science Foundation's Secure and Trustworthy Cyberspace program and is a part of a larger NSF effort to support foundational cybersecurity research and education.

The collaborative "Frontier" project includes researchers from Northeastern, Boston University, the Massachusetts Institute of Technology, and the University of Connecticut. The team will deploy and test the mechanisms they develop in this project using the Massachusetts Open Cloud—a partnership of state government, industry, and universities including Northeastern that is designed to create a new public cloud computing marketplace to help spur innovation.

"We're developing tools at all levels of the system," said Wichs, a cryptography expert who will focus his efforts on this area of the project.

"Encryption," he explained, "is a procedure we've been thinking about basically since the dawn of time, but we've only had good ways of doing it since the 70s." Until recently, even the best encryption strategies were limited when it comes to cloud computation, he said, adding that "The problem is that standard ways of encrypting data render it useless. Once encrypted, there is no way to perform any computation over it."

Patient data is a prime example. If a hospital wants to conduct large-scale analyses on this information, it is limited to looking at local computers because federal Health Insurance Portability and Accountability Act, or HIPAA, laws prevent it from sharing private details about patients with external entities. The hospital can easily store encrypted patient information, but it can't utilize the increased computational powers of external computers to analyze it because encryption prevents that possibility.

In recent years, a new method for computing on encrypted data has come about that has the potential to change all that. "I can send you encrypted data, you run the computation and then send me back the encrypted answer," Wichs explained. "I can decrypt the answer because I have the secret key, but you never learn anything."

This breakthrough presents great promise, but the approach is still too inefficient to be widely useful, Wichs said. With this grant, Wichs will try to change that. By developing new theoretical methods for encrypting data and performing computations on that data, he hopes to provide a new level of security to cloud-based computing.

"We want to take a standard program and convert it to work on encrypted data," he said. Prior approaches needed to first convert the program into a much less efficient circuit representation before being able to evaluate it on encrypted data. Wichs is working to build new encryptions schemes that can evaluate standard programs directly.

The research project aligns with Northeastern emphasis on use-inspired research that solves global challenges, particularly in the areas of security, health, and sustainability.

Provided by Northeastern University

Citation: How to secure the cloud (2014, August 1) retrieved 25 April 2024 from https://phys.org/news/2014-08-cloud.html