Cryptographic system allows users to decide how their data is accessed

March 18 2016, by Larry Hardesty

“This a rethinking of the Web infrastructure,” Frank Wang says. “Maybe it’s better that one person manages all their data. There’s one type of security and not 10 types of security. We’re trying to present an alternative model that would be beneficial to both users and applications.”

Most people with smartphones use a range of applications that collect personal information and store it on Internet-connected servers—and from their desktop or laptop computers, they connect to Web services that do the same. Some use still other Internet-connected devices, such as thermostats or fitness monitors, that also store personal data online.

Generally, users have no idea which data items their apps are collecting, where they're stored, and whether they're stored securely. Researchers at MIT and Harvard University hope to change that, with an application they're calling Sieve.

With Sieve, a Web user would store all of his or her personal data, in encrypted form, on the cloud. Any app that wanted to use specific data items would send a request to the user and receive a secret key that decrypted only those items. If the user wanted to revoke the app's access, Sieve would re-encrypt the data with a new key.

"This is a rethinking of the Web infrastructure," says Frank Wang, a PhD student in electrical engineering and computer science and one of the system's designers. "Maybe it's better that one person manages all their data. There's one type of security and not 10 types of security. We're trying to present an alternative model that would be beneficial to both users and applications."

The researchers are presenting Sieve at the USENIX Symposium on Networked Systems Design and Implementation this month. Wang is the first author, and he's joined by MIT associate professors of electrical engineering and computer science Nickolai Zeldovich and Vinod Vaikuntanathan, who is MIT's Steven and Renee Finn Career Development Professor, and by James Mickens, an associate professor of computer science at Harvard University.

Selective disclosure

Sieve required the researchers to develop practical versions of two cutting-edge cryptographic techniques called attribute-based encryption and key homomorphism.With attribute-based encryption, data items in a file are assigned different labels, or "attributes." After encryption, secret keys can be generated that unlock only particular combinations of attributes: name and zip code but not street name, for instance, or zip code and date of birth but not name.

The problem with attribute-based encryption—and decryption—is that it's slow. To get around that, the MIT and Harvard researchers envision that Sieve users would lump certain types of data together under a single attribute. For instance, a doctor might be interested in data from a patient's fitness-tracking device but probably not in the details of a single afternoon's run. The user might choose to group fitness data by month.

This introduces problems of its own, however. A fitness-tracking device probably wants to store data online as soon as the data is generated, rather than waiting until the end of the month for a bulk upload. But data uploaded to the cloud yesterday could end up in a very different physical location than data uploaded by the same device today.

So Sieve includes tables that track the locations at which grouped data items are stored in the cloud. Each of those tables is encrypted under a single attribute, but the data they point to are encrypted using standard—and more efficient—encryption algorithms. As a consequence, the size of the data item encrypted through attribute-based encryption—the table—is fixed, which makes decryption more efficient.

In experiments, the researchers found that decrypting a month's worth of, say, daily running times grouped under a single attribute would take about 1.5 seconds, whereas if each day's result was encrypted under its own attribute, decrypting a month's worth would take 15 seconds.

Wang developed an interface that displays a Sieve user's data items as a list and allows the user to create and label icons that represent different attributes. Dragging a data item onto an icon assigns it that attribute. At the moment, the interface is not particularly user friendly, but its purpose is to show that the underlying encryption machinery works properly.

Blind manipulation

Key homomorphism is what enables Sieve to revoke an app's access to a user's data. With key homomorphism, the cloud server can re-encrypt the data it's storing without decrypting it first—or without sending it to the user for decryption, re-encryption, and re-uploading. In this case, the researchers had to turn work that was largely theoretical into a working system.

"All these things in cryptography are very vague," Wang says. "They say, 'Here's an algorithm. Assume all these complicated math things.' But in reality, how do I build this? They're like, 'Oh, this group has this property.' But they don't tell you what the group is. Are they numbers? Are they primes? Are they elliptic curves? It took us a month or so to wrap our heads around what we needed to do to get this to work."

Of course, a system like Sieve requires the participation of app developers. But it could work to their advantage. A given application might provide more useful services if it had access to data collected by other devices. And were a system like Sieve commercially deployed, applications could distinguish themselves from their competitors by advertising themselves as Sieve-compliant.

"Privacy is increasing in importance and the debate between Apple's iPhone encryption and the FBI is a good example of that," says Engin Kirda, a professor of electrical and computer engineering at

Northeastern University. "I think a lot of users would appreciate having cryptographic control over their own data."

"I think the real innovation is how they use attribute-based encryption smartly, and make it usable in practice," Kirda adds. "They show that it is possible to have private clouds where the users have real privacy control over their data."

*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: Cryptographic system allows users to decide how their data is accessed (2016, March 18) retrieved 18 April 2024 from https://techxplore.com/news/2016-03-cryptographic-users-accessed.html