Researchers devise new method for protecting private data

April 18 2008

Companies and organizations that keep sensitive personal information on millions of Americans have become attractive targets for hackers in recent years, resulting in billions of dollars in losses for U.S. businesses and misery for countless consumers.

But now Amit Sahai, an associate professor of computer science at the UCLA Henry Samueli School of Engineering and Applied Science, and his colleagues have devised a new data-protection method they hope will put Internet criminals out of business.

"We want to change the rules of the game on hackers and even out the playing field," Sahai said.

Along with co-authors Brent Waters, a UCLA computer science alumnus, and Jonathan Katz of the University of Maryland, Sahai has come up with a mathematical system — known as functional encryption — that will not only help to simplify the encryption of data in servers but will also allow access to the data in an intuitive way, making it much harder for hackers to gain access to sensitive information but much easier for programmers to secure it.

While the method is not yet available for public use, it has received close attention from the data-encryption community. The authors' study, chosen as one of the top four papers at Eurocrypt 2008 — one of two flagship international conferences in cryptography — was presented this week at the conference in Istanbul.

In it, Sahai and his colleagues suggest that the biggest problem in data security today is that the world relies on "trusted servers" to store and secure data.

"This 'trusted server' model is a simple model," Sahai said. "It's easy to implement. It's easy to put into practice. Information is placed in the server at face value and the server itself is simply given the task of deciding who to give the data to. Because of the simplicity in programming, these servers have become ubiquitous and are prime targets — everyone wants to attack them."

An additional problem with trusted servers, the authors say, is the current trend toward replicating data on a wide scale.

"To create robustness and availability, data is stored on several trusted servers as backups," said Waters, currently with the nonprofit research institute SRI. "If one server goes down, another can be accessed. There is a trade-off between data availability and security. The more replicated servers there are, the more targets there are for hackers."

The results of this lack of security speak for themselves. According to a 2007 FBI analysis, Internet crime costs U.S. businesses some $67 billion annually, including the indirect expense of repairing hacked systems. TJX, the parent company of discount clothing chains T.J. Maxx and Marshalls, revealed that during a recent 18-month period, hackers had stolen 45.6 million credit card numbers and other sensitive customer information. For every two Americans, one private record has been stolen through computer data breaches alone.

Cryptography, the practice and study of hiding information, is considered to be a branch of both mathematics and computer science and is closely tied to information theory, computer security and engineering. And while the technology of encryption has been around a

long time, encrypting data and then deciding how to allow access to hundreds or even thousands of people has been a dilemma, Sahai said.

"Imagine current encryption technology as a lock and key — the data is locked, and to allow different people access, many copies of the key need to be made," he said. "One record might need to be accessed by 10,000 people, so you make 10,000 copies of that key. With millions of documents and thousands of keys per document, you can imagine how very, very complicated it gets. It becomes much too complicated to manage. So even though we've had very strong encryption technology now for decades, it's just not used, or it is used incorrectly."

The study authors' new functional encryption method allows a programmer to simply plug in his criteria for the information. The mathematical system will then produce an encrypted record that only people matching the criteria can decrypt. The complex system of managing many keys is now simplified, and servers hold encrypted data that the servers themselves can't read. The information looks like gibberish to hackers.

In addition, the new mathematical system allows for keys to be personalized — only one key is needed to unlock all the information that is available to that person.

"This is the key innovation in our system," Sahai said. "We have this mathematical method for randomization of personalizing keys so that your key doesn't just depend on what attributes you have, like what your name is. Further, there is some mathematical hardening that is personalized to you, so that you can't combine it with anyone else's keys to do anything meaningful."

The system severely restricts what a hacker can do. If he is an insider, he is limited by what access he legitimately has, and since keys are

personalized, it becomes much easier to trace who accessed and released the information in the first place.

Sahai and Waters are considered the founders of the area of functional encryption. Sahai recently won a prestigious 2007 Okawa Research Grant Award from Japan's Okawa Foundation for his work in this area.

"Some of this work is already being implemented and is actually being incorporated into some research systems," Sahai said. "It's making its way closer to practice. Brent and I were able to apply for a patent on the very initial work we did, which was bought by a company called Voltage Security. There certainly is interest from the U.S. military and the U.S. Department of Homeland Security as well."

"Our goal is to rethink what encryption is," Waters said. "Over the years, people have taken on a somewhat rigid view of what encryption is. What we're hoping to do is show that we can build simpler and more powerful systems by changing the way we think. Eventually, we hope to get rid of complex infrastructures and do things in a simpler manner that is also more secure and cost-effective."

In addition to being presented at the Eurocrypt conference, the study, "Predicate Encryption Supporting Disjunctions, Polynomial Equations and Inner Products," will appear in a forthcoming edition of the *Journal of Cryptography.*

Source: UCLA