Schneier on Security

← Spanish Police Foil Remote-Controlled Zeppelin Jailbreak The ATM Vulnerability You Won't Hear About →

Homomorphic Encryption Breakthrough

Last month, IBM made some pretty brash claims about homomorphic encryption and the future of security. I hate to be the one to throw cold water on the whole thing -- as cool as the new discovery is -- but it's important to separate the theoretical from the practical.

Homomorphic cryptosystems are ones where mathematical operations on the ciphertext have regular effects on the plaintext. A normal symmetric cipher -- DES, AES, or whatever -- is not homomorphic. Assume you have a plaintext P, and you encrypt it with AES to get a corresponding ciphertext C. If you multiply that ciphertext by 2, and then decrypt 2C, you get random gibberish instead of P. If you got something else, like 2P, that would imply some pretty strong nonrandomness properties of AES and no one would trust its security.

The RSA algorithm is different. Encrypt P to get C, multiply C by 2, and then decrypt 2C -- and you get 2P. That's a homomorphism: perform some mathematical operation to the ciphertext, and that operation is reflected in the plaintext. The RSA algorithm is homomorphic with respect to multiplication, something that has to be taken into account when evaluating the security of a security system that uses RSA.

This isn't anything new. RSA's homomorphism was known in the 1970s, and other algorithms that are homomorphic with respect to addition have been known since the 1980s. But what has eluded cryptographers is a fully homomorphic cryptosystem: one that is homomorphic under both addition and multiplication and yet still secure. And that's what IBM researcher Craig Gentry has discovered.

This is a bigger deal than might appear at first glance. Any computation can be expressed as a Boolean circuit: a series of additions and multiplications. Your computer consists of a zillion Boolean circuits, and you can run programs to do anything on your computer. This algorithm means you can perform arbitrary computations on homomorphically encrypted data. More concretely: if you encrypt data in a fully homomorphic cryptosystem, you can ship that encrypted data to an untrusted person and that person can perform arbitrary computations on that data without being able to decrypt the data itself. Imagine what that would mean for cloud computing, or any outsourcing infrastructure: you no longer have to trust the outsourcer with the data.

Unfortunately -- you knew that was coming, right? -- Gentry's scheme is completely impractical. It uses something called an ideal lattice as the basis for the encryption scheme, and both the size of the ciphertext and the complexity of the encryption and decryption operations grow enormously with the number of operations you need to perform on the ciphertext -- and that number needs to be fixed in advance. And converting a computer program, even a simple one, into a Boolean circuit requires an enormous number of operations. These aren't impracticalities that can be solved with some clever optimization techniques and a few turns of Moore's Law; this is an inherent limitation in the algorithm. In one article, Gentry estimates that performing a Google search with encrypted keywords -- a perfectly reasonable simple application of this algorithm -- would increase the amount of computing time by about a trillion. Moore's law calculates that it would be 40 years before that homomorphic search would be as efficient as a search today, and I think he's being optimistic with even this most simple of examples.

Despite this, IBM's PR machine has been in overdrive about the discovery. Its press release makes it sound like this new homomorphic scheme is going to rewrite the business of computing: not just cloud computing, but "enabling filters to identify spam, even in encrypted email, or protection information contained in electronic medical records." Maybe someday, but not in my lifetime.

This is not to take anything away anything from Gentry or his discovery. Visions of a fully homomorphic cryptosystem have been dancing in cryptographers' heads for thirty years. I never expected to see one. It will be years before a sufficient number of cryptographers examine the algorithm that we can have any confidence that the scheme is secure, but -- practicality be damned -- this is an amazing piece of work.

Tags: academic papers, cloud computing, cryptography, encryption, homomorphic encryption

Posted on July 9, 2009 at 6:36 AM • 55 Comments