Researcher Discovers Method to Fully Process Encrypted Data Without Knowing its Content

June 25 2009

(PhysOrg.com) -- An IBM Researcher has solved a thorny mathematical problem that has confounded scientists since the invention of public-key encryption several decades ago. The breakthrough, called "privacy homomorphism," or "fully homomorphic encryption," makes possible the deep and unlimited analysis of encrypted information -- data that has been intentionally scrambled -- without sacrificing confidentiality.

IBM's solution, formulated by IBM Researcher Craig Gentry, uses a mathematical object called an "ideal lattice," and allows people to fully interact with encrypted data in ways previously thought impossible. With the breakthrough, computer vendors storing the confidential, electronic data of others will be able to fully analyze data on their clients' behalf without expensive interaction with the client, and without seeing any of the private data. With Gentry's technique, the analysis of encrypted information can yield the same detailed results as if the original data was fully visible to all.

Using the solution could help strengthen the business model of "cloud computing," where a computer vendor is entrusted to host the confidential data of others in a ubiquitous Internet presence. It might better enable a cloud computing vendor to perform computations on clients' data at their request, such as analyzing sales patterns, without exposing the original data.

Other potential applications include enabling filters to identify spam, even in encrypted email, or protecting information contained in electronic medical records. The breakthrough might also one day enable computer users to retrieve information from a search engine with more confidentiality.

"At IBM, as we aim to help businesses and governments operate in more intelligent ways, we are also pursuing the future of privacy and security," said Charles Lickel, vice president of Software Research at IBM. "Fully homomorphic encryption is a bit like enabling a layperson to perform flawless neurosurgery while blindfolded, and without later remembering the episode. We believe this breakthrough will enable businesses to make more informed decisions, based on more studied analysis, without compromising privacy. We also think that the lattice approach holds potential for helping to solve additional cryptography challenges in the future."

Two fathers of modern encryption -- Ron Rivest and Leonard Adleman -- together with Michael Dertouzos, introduced and struggled with the notion of fully homomorphic encryption approximately 30 years ago. Although advances through the years offered partial solutions to this problem, a full solution that achieves all the desired properties of homomorphic encryption did not exist until now.

In the past IBM made several major cryptography breakthroughs, such as the design of the Data Encryption Standard (DES); Hash Message Authentication Code (HMAC); the first lattice-based encryption with a rigorous proof-of-security; and numerous other solutions that have helped advance Internet security.

Craig Gentry conducted research on privacy homomorphism while he was a summer student at IBM Research and while working on his PhD at Stanford University.

Provided by IBM