Quantum Physics: Secure, Single-Use Computer Memories may be Possible

NIST

Computer security systems may one day get a boost from quantum physics, as a result of recent research from the National Institute of Standards and Technology (NIST). Computer scientist Yi-Kai Liu has devised a way to make a security device that has proved notoriously difficult to build — a "one-shot" memory unit, whose contents can be read only a single time.

The research, which Liu is presenting at the Innovations in Theoretical Computer Science conference, shows in theory how the laws of quantum physics could allow for the construction of such memory devices. One-shot memories would have a wide range of possible applications such as protecting the transfer of large sums of money electronically. A one-shot memory might contain two authorization codes: one that credits the recipient's bank account and one that credits the sender's bank account, in case the transfer is canceled. Crucially, the memory could only be read once, so only one of the codes can be retrieved, and hence, only one of the two actions can be performed — not both.

"When an adversary has physical control of a device — such as a stolen cell phone — software defenses alone aren't enough; we need to use tamper-resistant hardware to provide security," Liu says. "Moreover, to protect critical systems, we don't want to rely too much on complex defenses that might still get hacked. It's better if we can rely on fundamental laws of nature, which are unassailable."

Unfortunately, there is no fundamental solution to the problem of building tamper-resistant chips, at least not using classical physics alone. So scientists have tried involving quantum mechanics as well, because information that is encoded into a quantum system behaves differently from a classical system.

Liu is exploring one approach, which stores data using quantum bits, or "qubits," which use quantum properties such as magnetic spin to represent digital information. Using a technique called "conjugate coding," two secret messages — such as separate authorization codes — can be encoded into the same string of qubits, so that a user can retrieve either one of the two messages. But as the qubits can only be read once, the user cannot retrieve both.

The risk in this approach stems from a more subtle quantum phenomenon: "entanglement," where two particles can affect each other even when separated by great distances. If an adversary is able to use entanglement, he can retrieve both messages at once, breaking the security of the scheme.

However, Liu has observed that in certain kinds of physical systems, it is very difficult to create and use entanglement, and shows in his paper that this obstacle turns out to be an advantage: Liu presents a mathematical proof that if an adversary is unable to use entanglement in his attack, that adversary will never be able to retrieve both messages from the qubits. Hence, if the right physical systems are used, the conjugate coding method is secure after all.

"It's fascinating how entanglement — and the lack thereof — is the key to making this work," Liu says. "From a practical point of view, these quantum devices would be more expensive to fabricate, but they would provide a higher level of security. Right now, this is still basic research. But there's been a lot of progress in this area, so I'm optimistic that this will lead to useful technologies in the real world."

Citation: Y-K Liu. "Building one-time memories from isolated qubits." Paper presented at the ITCS 20-14 Innovations in Theoretical Computer Science meeting, Princeton University, Jan. 11-14, 2014. More info at http://itcs2014.wordpress.com/program/ [1].

The National Institute of Standards and Technology (NIST) is an agency of the U.S. Department of Commerce [2].

Links:
[1] http://itcs2014.wordpress.com/program/
[2] http://www.commerce.gov