Engineers devise new method for securing location-sensitive data by using quantum mechanics

July 26 2010, By Matthew Chin and Wileen Wong Kromhout

(PhysOrg.com) -- A research group led by computer scientists at the UCLA Henry Samueli School of Engineering and Applied Science has proved that cryptography -- the practice and study of hiding information -- that is based solely on physical location is possible by using quantum mechanics.

Such a method, the researchers say, allows one to encrypt and decrypt data at a secure location without pre-sharing any cryptographic keys that can be used to lock or unlock sensitive information.

The idea behind location-based cryptography is that only a recipient at a precise geographic location can receive an encrypted message — the location itself acts as the credential required for generating an encryption key.

This type of cryptography could be useful in several settings. For example, one could communicate with a military base with a guarantee that only someone physically present at the base will have access to the information. Furthermore, the location-based method eliminates the need for distributing and storing keys, one of the most difficult tasks in cryptography.

A central tool in location-based cryptography is secure location verification, which is a method for verifying the geographical position of

a device in a secure manner, according to Rafail Ostrovsky, a UCLA professor of computer science and mathematics.

"Securely proving a location where such a proof cannot be spoofed, and securely communicating only to a device in a particular location and nowhere else is extremely important," Ostrovsky said. "Often, the location of a device determines its credentials. Our recent paper shows how our method allows one to securely communicate to a device only in a particular location and without any other assumptions regarding prior interaction with the device at this location."

The strategy, outlined in a new research paper currently available at http://arxiv.org/abs/1005.1750, was recently accepted to the highest-rated theoretical computer science peer-review conference, the 2010 IEEE Symposium on Foundations of Computer Science.

According to Ostrovsky, the problem of secure positioning has been widely studied by the wireless security community. It was assumed that the classical approach, based on triangulation, offered a secure solution. However, last year, a research group led by Ostrovsky proved that this approach cannot offer security against a coalition of dishonest persons that actively try to break the scheme, thereby breaking all known classical location verification systems.

Surprisingly, with the help of quantum mechanics, the task of location verification can be done in a secure way, even in the presence of colluding adversaries, the researchers say.

The research group has recently shown that if one sends quantum bits — the quantum equivalent of a bit — instead of only classical bits, a secure protocol can be obtained such that the location of a device cannot be spoofed. This, in turn, leads to a key-exchange protocol based solely on location.

The core idea behind the protocol is the "no-cloning" principle of quantum mechanics. By making a device give the responses of random challenges to several verifiers, the protocol ensures that multiple colluding devices cannot falsely prove any location. This is because an adversarial device can either store the quantum state of the challenge or send it to a colluding adversary, but not both.

The proposed method does not require any involved quantum computation other than creating and measuring quantum bits, which could be implemented with existing technology.

Provided by University of California - Los Angeles