'Zero knowledge' may answer computer security question

August 29 2013, by Bill Steele

(Phys.org) —In the age of the Internet, it's getting harder and harder to keep secrets. When you type in your password, there's no telling who might be watching it go by. New research at Cornell may offer a pathway to more secure communications.

The answer is to not send sensitive information at all. Rafael Pass, associate professor of computer science, has developed a new protocol, or set of rules, to create what computer scientists call a "zero knowledge proof."

"I think zero knowledge proofs are one of the most amazing notions in computer science," Pass said. "What we have done is to combine it with another notion – that it's easier to prove that a computation can be done correctly than it is to actually compute it."

The result is a way to prove that you know something without saying out loud what it is you know. Instead of insecurely typing the password for your bank account, you just prove to the bank that you know the password. You could pass an exam by proving that you know the answer, without actually writing the answer down so the person sitting next to you can't copy it.

Applications include password authentication, cryptography, auctions, financial transactions and online voting. "At this point it's purely theoretical," Pass cautioned, "but it is teaching us a lot more about how zero knowledge works. That's what makes me excited." Pass and

colleagues will describe their work at the 54th Annual IEEE Symposium on Foundations of Computer Science, Oct. 27-29 in Berkeley, Calif.

In its simplest form, such a proof consists of answering questions that depend on having the secret knowledge. To prove you have been in my house, I might ask you what color my cat is. The idea has been around since 1985, and there are already many ways to do it. Early versions required only a few messages being passed back and forth, but were insecure if an attacker participated in many proofs at the same time, as can easily be done on the Internet. An attacker could pick up a little bit of information from each exchange, piecing together the whole secret. Some newer methods will remain secure over many simultaneous exchanges, but instead require many messages being passed back and forth. The new protocol gets the job done with as few as 10 exchanges, Pass said, while remaining secure over many simultaneous exchanges. The researchers supply a rigorous mathematical proof that the protocol is a true zero-knowledge system, and that it works with just a small number of exchanges.

The proof that a zero-knowledge protocol works is the ability to construct a "simulator" that generates a fake conversation indistinguishable from a real one using the protocol, showing that whatever attack the intruder uses against the real conversation produces the same result as attacking the simulation. In other words, the intruder can learn nothing from the real conversation that he couldn't have learned for himself by running the simulator. But running the simulator requires a lot of computer time, especially if there are many exchanges. The new protocol instead sends a "P-certificate," certifying that the simulator has been proven to work. A computer program is just a series of logical steps; that it generates a particular output can be proven like any other mathematical statement.

The next step, Pass said, will be to apply the idea to the "man-in-the-

middle" attack, where an intruder slips in between two parties to a conversation, making them think they're talking directly to each other, not only to listen in but sometimes to change the messages as they pass through.

The idea of a zero knowledge proof was introduced by Shafi Goldwasser, Silvio Micali and Charles Rackoff at MIT. This year Goldwasser and Micali received the Turing Award (the equivalent of a Nobel Prize in computer science) for this and related discoveries.

Provided by Cornell University