Air Force grant to tighten online encryption

December 14 2009, By Bill Steele

(PhysOrg.com) -- Computer scientist Rafael Pass is seeking new approaches to cryptographic security with a $600,000, five-year grant from the Air Force Office of Scientific Research.

Computers have changed the rules for keeping secrets. Confidential information can now be encrypted with keys so long that it would take a supercomputer until the end of the universe to break the code. But at the same time, with thousands of secret messages flying across the Internet, breaking security actually becomes easier.

To keep cyber secrets secure, Rafael Pass, assistant professor of computer science, is seeking new approaches to cryptographic security with a $600,000, five-year grant from the Young Investigator Program of the Air Force Office of Scientific Research (AFOSR).

When many transactions occur simultaneously, say in a banking system, air traffic control network or online auction, attackers can reap information by comparing one message with another.

"An adversary controlling many computers all over the Internet can get a little information here and there," Pass explained. "Cryptographic protocols -- the rules for encryption -- have traditionally been designed to work when only one thing is happening at a time."

A simple example is the "man in the middle" attack. The attacker sits between two parties, appearing to the sender to be the receiver and vice versa. As each message passes the attacker may learn something about

how it is encoded. It's not even necessary to break the entire code, Pass says, if the attacker can learn enough to make subtle changes. Now suppose a hacker can deploy thousands of automated men in the middle reading thousands of messages at once and comparing notes.

One approach to foil this attack, Pass said, is to make messages "non-malleable," giving them a complex structure that is inseparable from its content so they are impossible to open or change without leaving a trace. Imagine a jigsaw puzzle with one word on each piece; change a word and the piece might need to shrink or grow, and the puzzle no longer fits together. Such a message could even be constructed so that the receiver couldn't read all of it -- just the needed information. Two parties could carry out a financial transaction or exchange passwords without meeting face-to-face or using a trusted third party.

"I will encrypt my input, and the other party will have a way to compute an answer," explained Pass, who has already developed ways to do this with simple transactions. The next challenge, he says, is to extend it to multiple concurrent messages.

Another security method is to communicate on an agreed schedule. The man in the middle would reveal his presence by the delay in retransmitting the message, even by a few milliseconds.

New security protocols, Pass said, also must protect against "side-channel attacks," where attackers gain some information by a method other than breaking encryption, such as simply reading a password pasted to a computer monitor or intercepting radio-frequency signals radiated by a computer from outside a building.

Finally, a security system must give users an incentive to be trustworthy, Pass noted. If there is a cost to the computation needed to make communication secure, not everyone will pay it.

The ultimate goal, Pass said, is to create a mathematical proof that a security protocol can't be broken. "There are many systems that we can't break, but we can't prove they are secure," he said. "We don't know what the attacker is going to do, so the only secure way is a mathematical proof."

Pass said this may not be possible with current security models. "We may have to find new models for defining what it means to be secure."

The AFOSR Young Investigator awards support scientists and engineers "who show exceptional ability and promise for conducting basic research." Pass won one of only 38 awards out of 202 proposals.

Provided by Cornell University (news : web)