Laser security for the Internet

March 23 2010

A British computer hacker equipped with a "Dummies" guide recently tapped into the Pentagon. As hackers get smarter, computers get more powerful and national security is put at risk. The same goes for your own personal and financial information transmitted by phone, on the Internet or through bank machines.

Now a new invention developed by Dr. Jacob Scheuer of Tel Aviv University's School of Electrical Engineering promises an information security system that can beat today's hackers -- and the hackers of the future -- with existing fiber optic and computer technology. Transmitting binary lock-and-key information in the form of light pulses, his device ensures that a shared key code can be unlocked by the sender and receiver, and absolutely nobody else. He will present his new findings to peers at the next laser and electro-optics conference this May at the Conference for Lasers and Electro-Optics (CLEO) in San Jose, California.

"When the RSA system for digital information security was introduced in the 1970s, the researchers who invented it predicted that their 200-bit key would take a billion years to crack," says Dr. Scheuer. "It was cracked five years ago. But it's still the most secure system for consumers to use today when shopping online or using a bank card. As computers become increasingly powerful, though, the idea of using the RSA system becomes more fragile."

Plugging a leak in a loophole

Dr. Sheuer says the solution lies in a new kind of system to keep prying eyes off secure information. "Rather than developing the lock or the key, we've developed a system which acts as a type of key bearer," he explains.

But how can a secure key be delivered over a non-secure network -- a necessary step to get a message from one user to another? If a hacker sees how a key is being sent through the system, that hacker could be in a position to take the key. Dr. Sheuer has found a way to transmit a binary code (the key bearer) in the form of 1s and 0s, but using light and lasers instead of numbers. "The trick," says Dr. Scheuer, "is for those at either end of the fiber optic link to send different laser signals they can distinguish between, but which look identical to an eavesdropper."

New laser is key

Dr. Scheuer developed his system using a special laser he invented, which can reach over 3,000 miles without any serious parts of the signal being lost. This approach makes it simpler and more reliable than quantum cryptography, a new technology that relies on the quantum properties of photons, explains Dr. Scheuer. With the right investment to test the theory, Dr. Scheuer says it is plausible and highly likely that the system he has built is not limited to any range on earth, even a round-the-world link, for international communications.

"We've already published the theoretical idea and now have developed a preliminary demonstration in my lab. Once both parties have the key they need, they could send information without any chance of detection. We were able to demonstrate that, if it's done right, the system could be absolutely secure. Even with a quantum computer of the future, a hacker couldn't decipher the key," Dr. Scheuer says.

Provided by Tel Aviv University

Citation: Laser security for the Internet (2010, March 23) retrieved 20 March 2024 from https://phys.org/news/2010-03-laser-internet.html