Vulnerability in commercial quantum cryptography

August 29 2010

A security researcher (Ph.D. student Lars Lydersen) is testing a commercial quantum cryptography system in a laboratory, to confirm the security vulnerability. Credit: NTNU

The Norwegian University of Science and Technology (NTNU) and the University of Erlangen-Nurnberg together with the Max Planck Institute for the Science of Light in Erlangen have recently developed and tested a technique exploiting imperfections in quantum cryptography systems to implement an attack.

Countermeasures were also implemented within an ongoing collaboration with leading manufacturer ID Quantique.

Quantum cryptography is a technology that allows one to distribute a cryptographic key across an optical network and to exploit the laws of quantum physics to guarantee its secrecy. It makes use of the Heisenberg uncertainty principle - observation causes perturbation - to reveal

eavesdropping on an optical fiber.

The technology was invented in the mid-eighties, with first demonstration less than a decade later and the launch of commercial products during the first years of the century.

Although the security of quantum cryptography relies in principle only on the laws of quantum physics, it is also dependent on the lack of loopholes in specific implementations, just like any other security technology.

"The security of quantum cryptography relies on quantum physics but not only... It must also be properly implemented. This fact was often overlooked in the past," explains Prof. Gerd Leuchs of the University of Erlangen-Nurnberg and the Max Planck Institute for the Science of Light.

Recently, NTNU in collaboration with the team in Erlangen has found a technique to remotely control a key component of most of today's quantum cryptography systems, the photon detector, which is reported today in Nature Photonics advance online publication.

"Unlike previously published attempts, this attack is imple-mentable with current off-the-shelf components," says Dr. Vadim Makarov, a researcher in the Quantum Hacking group at NTNU, who adds: "Our eavesdropping method worked both against MagiQ Technology's QPN 5505 and ID Quantique Clavis2 systems."

In the framework of a collaboration initiated with ID Quantique, the researchers shared their results with the company prior to publication. ID Quantique has then, with a help of NTNU, developed and tested a countermeasure.

Academic researchers of the two laboratories will continue testing security aspects of quantum cryptography solutions from ID Quantique. "Testing is a necessary step to validate a new security technology and the fact that this proc-ess is applied today to quantum cryptography is a sign of maturity for this technology," ex-plains Grégoire Ribordy, CEO of ID Quantique.

More information: Paper: doi:10.1038/nphoton.2010.214
"How we did it": www.iet.ntnu.no/groups/optics/ … m-cryptography-2010/

Provided by Norwegian University of Science and Technology