Quantum Cryptography: Diamonds Offer New Online Security

May 15 2006

Researchers at the University of Melbourne, Australia, have found a glamorous solution to the problem of communications systems being hacked by eavesdroppers -- diamonds. The School of Physics at the university has just secured $9 million (USD7 million) in international venture funding from international communication firms to develop the diamond-based anti-eavesdropping devices. With the new technologies, IT managers should be able to detect network prying and prevent the theft of highly sensitive information.

The project is headed by Shane Huntingdon, a scientist in the university's physics department. Huntingdon is also the chief executive officer of Quantum Communications Victoria, which has a program at the school where the quantum-based technology is being developed. The driver for the technology has been the global economic problem of eavesdropping, which causes huge financial losses for security agencies -- the FBI has estimated that breaches of critical information sent via the Internet costs millions of dollars worldwide each year. "The challenge has been to completely remove all avenues of interception by eavesdroppers," Huntingdon said.

The system won't be able to prevent criminals breaking into communications networks in an attempt to steal valuable information. What it can do is let everyone involved know that an outsider is listening in on the optic fiber that the messages are being sent down, which is a vital improvement on the current system.

Huntingdon has described how currently eavesdroppers can hack into existing communications systems and extract information from optical systems without users being aware of it. With the new quantum technologies users can cut the line as soon as they realize that they're being spied on. The message can then be re-sent through an uncompromised channel.

The key to the technology is quantum cryptography -- sending messages via optic fibers, one photon at a time. The synthetic diamonds are grown to have a targeted defect that allows them to produce this single photon of light. As quantum states cannot be copied, users of the system will know immediately if anyone steals the information. As Huntingdon says, "If you're sending one photon at a time and one goes missing, you definitely know it." Although other similar commercial systems exist in the United States and Europe, they use filtered lasers to approximate single photos instead.

The target market for the system is groups who deal in extremely sensitive data and for whom any loss of information is unacceptable. These include financial institutions, security agencies and governments, and the first-generation products from the technologies are likely to be targeted towards them for the transmission of secure datasets, such as a bank's daily offsite backup. Later generations would have more widespread uses with the commodity networking market. For now, the expected date of release of the first prototype is in three years.

If the technology takes off, there may also be an unexpected side effect hitting the gems market. QCV grows the diamonds it uses on the grounds so that they're cleaner than mined gems, but increased need for artificially grown diamonds for industrial purposes could lower the market value of jewels as gem-quality diamond producers take advantage of the new demands.

Although the technology was pitched as being a way of addressing Australia's critical need to keep up with the rest of the world in Internet security, the rest of the world is keeping tabs on the project. The initial investment came from state and federal funding when QCV was awarded $3.3 million (USD2.6 million) as part of a grant from Victoria's Department of Innovation, Industry and Regional Development to develop the technology. The consortium of quantum communication and commercialization companies that the group has just signed with includes Qucor Pty. from Sydney, but also MaqiQ Technologies in Japan and the California-based Silicon Graphics Inc.

More than simply being another step on the road to increased online security, ComputerWorld reports how Huntingdon believes that the project could also kick-start the quantum-communications industry worldwide, taking quantum technology from theory to reality. "It's not a stronger form of encoding" he enthuses, "it's a new paradigm."