A quantum leap in information security

Pioneering physicist aims to lock out data hackers with speed-of-light cryptography

DAWN WALTON
GLOBE AND MAIL UPDATE
APRIL 3, 2007 AT 8:29 AM EDT

CALGARY — Right now, somewhere in the world, hackers are trying to break into central electronic storage facilities to pilfer sensitive data such as credit card information, financial records and personal identification.

Retail giant TJX Cos., which operates Winners and HomeSense in Canada, recently fell victim to this kind of cyber theft. So did fashion retailer Club Monaco.

And down the road, thieves may be even more sophisticated -- they may be able to steal private data while it is being transmitted from the debit-card machine at your grocery store to your bank, or en route from your home computer to the Canada Revenue Agency.

"Public channels can very easily be monitored," says Wolfgang Tittel, a 37-year-old internationally recognized physicist and pioneer in information security who was recently recruited by the University of Calgary from Switzerland.

Security measures for data transmission are scant, he notes. Companies and governments are relying on the fact that computers aren't sufficiently fast enough to peek at encrypted messages as they are being sent and immediately crack the code to unscramble the information.

"But that is based on the assumption that nobody can crack it in time," explains Dr. Tittel. "There is no proof of it. You can only hope [it doesn't happen]."

The world's increasing dependence on electronic data transfers and e-mails leaves individuals, businesses and governments vulnerable, Dr. Tittel says. But we have one thing going for us even as experts beef-up security measures: hackers are essentially lazy.

"Humans try to get information as easily as possible," he says.

Still, Dr. Tittel suspects that the bad guys will one day figure out precisely how to listen in on transmissions and make use of protected material -- whether personal and financial information, medical records or military secrets -- at their whim.

That's why he's trying to stay one step ahead of the data thieves, with a $1.5-million project at UofC's Institute for Quantum Information Science that lured him from the University of Geneva, where he was a member of the prestigious Group of Applied Physics.

In January, Dr. Tittel became the iCORE/General Dynamics Canada Industrial Research Chair in Quantum Cryptography and Communication. The title is a dry mouthful, but it represents a cutting-edge project most ordinary folks would find head-spinning.

Dr. Tittel and a team of more than a dozen researchers are applying the principles of quantum physics (the study of the smallest particles of matter and energy) to information sciences -- a field known as quantum cryptography.

Quantum cryptography aims to develop systems that are completely secure. For businesses and consumers who use widespread technology such as bank cards and credit cards, it works like this:

Dr. Tittel's team is creating a "quantum key" to protect information that is being transmitted. Only this key will unlock the protected information. The key is sent before the sensitive data is transmitted.

Conventional encryption relies on a secret key, usually a string of letters and numbers, known to both parties. In quantum cryptography, this key is transmitted over optical fibre with each bit in the key represented by one photon.

If the quantum key is copied or tampered with, it will, according to the laws of quantum physics, instantly change shape. If the recipient receives an unreadable key, that is a clear tip-off that protected information should not be sent. The sender and the receiver will establish a secure key before transmitting the data to be unlocked.

The theory has already been put into practice in the lab. In Switzerland, Dr. Tittel was at the forefront in applying quantum information techniques outside the confines of the lab and over short distances.

He now hopes to have the technology working commercially in five years over distances of about 100 kilometres.

By summer, Dr. Tittel hopes to have completely transformed his new lab in Calgary, known as QC2, to match the one he left behind in Geneva.

The paint still smells fresh in the basement-level lab on the UofC campus. The windowless space is tucked away from busy streets where the vibrations of passing vehicles could affect research. The temperature is kept stable and the air is filtered so that work with fibre optic cables will not be affected.

Dr. Tittel, who also teaches physics at the university, says Calgary is an ideal setting for this field of research because it has resources unavailable in other parts of the world. On-site engineers can whip up electronics on demand, he noted, and Calgary is home to some of the brightest researchers in the fields of both quantum physics and cryptography.

Along with a $750,000 investment from iCORE (an Alberta government agency dedicated to exceptional research), Dr. Tittel's project drew an initial grant of $150,000 from the Natural Sciences and Engineering Research Council and federal and provincial funding to equip the world-class lab. As well, it has industry support from General Dynamics Canada. The company, a leading supplier of secure communication solutions to the Canadian Forces, regards quantum cryptography as a promising technology in the evolution of security solutions, according to Dr. Tittel.

"Dr. Tittel's research represents the future of information security," Doug Horner, Alberta's minister for advanced education and technology, said in a recent statement.

"With applications ranging from fibre optics to satellite communications, his work will enhance Alberta's reputation for information and communications technology expertise."

How quantum cryptography works

Alice sends a key to Bob along a photon tunnel. The dots below represent the individual photons. Along the way, Eve eavesdrops. But by the laws of

quantum physics, Eve's action alters the state of the photons - some of the teeth in Alice's original key have been discoloured by Eve's unauthorized monitoring. When the compromised key reaches Bob, he instantly knows it has been intercepted because of the discolouration. Alice and Bob discard their key and try again - only once a secure key has been transmitted do they attempt to send the sensitive information to be locked and unlocked.

Alice

(sender)

Bob

(intended

recipient)

Eve

(hacker

taps part

of signal)

SOURCE: CAMBRIDGE RESEARCH LABORATORY