Securing data from tomorrow's supercomputers

August 18 2015, by Rose Trapnell

For the powerful quantum computers that will be developed in the future, cracking online bank account details and credit cards number will be a cinch.

But a team of cryptographers which includes QUT's Dr Douglas Stebila is already working at future-proofing the privacy of today's Internet communications from tomorrow's powerful computers.

Dr Stebila, along with researchers Joppe Bos from chip maker NXP Semiconductors and Craig Costello and Michael Naehrig from Microsoft Research, have developed upgrades to the Internet's core encryption protocol that will prevent quantum computer users from intercepting Internet communications.

"Governments and the computing industry are working with scientists to try to build quantum computers. It's a very significant scientific challenge, but quantum computers could be reality in a few decades," Dr Stebila said.

"Quantum computers will be able to solve complex scientific problems, like simulating chemical reactions, much faster than today's most powerful supercomputers, but they'll also be able to break much of the public key cryptography that's used to protect Internet, mobile telephone, and other electronic communication."

"Though quantum computers don't exist yet, they could be used to

retroactively decrypt past transmissions," Dr Stebila explained.

"That's why it's important that we start updating our communication infrastructure. We've tested some new techniques and found some very promising first steps towards future-proofing Internet encryption."

Dr Stebila said that Internet communication was currently protected by encryption using the Transport Layer Security (TLS) standard, which ensures that web browsers can't be tricked into sending data to the wrong web server, and that eavesdroppers can't intercept passwords or other personal information.

"The TLS Internet encryption protocol uses a variety of mathematical techniques to protect information, some of which would need to be updated to be resistant to quantum computers.

"We've developed a new quantum-proof version of TLS that incorporates a mathematical technique called the 'ring learning with errors problem', a fairly recent technique that mathematicians think has the potential to resist quantum attacks.

"We've tested our new protocol to encrypt data moving between two PCs—the new techniques are a little slower than existing ones, but the confidentiality of the data is improved.

"The speed of the new protocol is now something we will work on, but this is a big step forward, demonstrating the practicality of these new techniques. We're optimistic this will provide a framework for developing effective ways of future-proofing our data in the world of quantum computers."

More information: "Post-quantum key exchange for the TLS protocol from the ring learning with errors problem." eprint.iacr.org/2014/599

Provided by Queensland University of Technology