Dutch researchers crack Internet security of the future

October 31 2008

Researchers at Eindhoven University of Technology (TU/e) in The Netherlands have managed to crack the so-called McEliece encryption system. This system is a candidate for the security of Internet traffic in the age of the quantum computer - the predicted superpowerful computer of the future.

The attack succeeded this month by means of a large number of linked computers throughout the world, says TU/e professor Tanja Lange. Earlier this year she and her PhD student Christiane Peters, together with visiting professor Daniel Bernstein (University of Illinois, Chicago), had discovered a way to speed up attacks against the 30-year-old McEliece cryptosystem. The researchers wrote software that would decrypt a McEliece ciphertext in just 1 week on a cluster of 200 computers.

The software was run recently on several dozen computers in Eindhoven, Amsterdam, France, Ireland, Taiwan and the United States. A lucky computer in Ireland found the ciphertext.

The successful attack was announced recently at a conference in Cincinnati (US) on Post-Quantum Cryptography. The researchers said that the McEliece cryptosystem can be scaled to larger key sizes to avoid their attacks and remains a leading candidate for post-quantum cryptography.

At present, banks use the RSA code from 1977 for securing matters such

as electronic transactions. For RSA the currently used key sizes are significantly larger than initially thought: a single PC would need only 3 weeks to break the parameters from the original paper. Yet a quantum computer will have no problems cracking even the improved current version. For this reason, anticipating the introduction of the quantum computer (which Lange thinks will take at least ten more years) and to deal with long-term confidentiality such as health records, researchers are trying to find better encryption systems.

Source: Eindhoven University of Technology