Researchers crack unassailable encryption algorithm in two hours

May 20 2014, by Emmanuel Barraud

Credit: thinkstockphotos

(Phys.org) —A protocol based on "discrete logarithms", deemed as one of the candidates for the Internet's future security systems, was decrypted by EPFL researchers. Allegedly tamper-proof, it could only stand up to the school machines' decryption attempts for two hours.

Without cryptography, no one would dare to type their credit card number on the Internet. Security systems developed to protect the communication privacy between the seller and the buyer are the prime targets for hackers of all kinds, hence making it necessary for encryption algorithms to be regularly strengthened. In universities, research in hacking aim mostly at testing their robustness.

Most of them rely on "discrete logarithm problems" – very complex mathematical operations – to secure data transmissions. "There are several variants, based for example on prime numbers or other mathematical formulas, explains Arjen Lenstra, director of the Laboratory for Cryptologic Algorithms (LACAL) at EPFL . "Their complexity is such that they are deemed as impossible to solve." Due to their effectiveness, the industry, especially banks, makes use of them for encoding their transactions. "The danger lies in the fact that these systems are based on principles that we do not fully understand, states Arjen Lenstra. If someone were to find out how to solve them all, the entire system would collapse."

In fact, a little over a year ago, cracks began to appear. Robert Granger, then at University College Dublin but who has since joined LACAL, showed that surprisingly the problem's first phase can be solved very easily. Antoine Joux, a French Scientist, independently had similar insights, and together with a French team then showed how to make the second and final phase `very nearly' easy. Then, many other cryptographers stepped in.

However, these methods only managed to overcome a very particular type of discrete logarithm. Nothing suggested that they could crack the industrial variants.

Therefore, an EPFL team, together with Jens Zumbragel from TU Dresden, focused on a "family" of algorithms presented as candidates for the next generation of encryption keys, which made use of "supersingular curves. "We proved that it would only take two hours for EPFL computers to solve a problem of this kind. Whereas it was believed that it would take 40'000 times the age of the universe for all computers on the planet to do it!" explains Thorsten Kleinjung, post-doctoral fellow at LACAL.

However, we need not panic; this system has not yet been deployed. EPFL researchers' success is not likely to be misused. "Basically, we just excluded this option from the search for a successor to current algorithms," said Arjen Lenstra, whose team will present its findings this August at the Crypto 2014 conference, which announced today that it accepted their submission to participate.

More information: Robert Granger, Thorsten Kleinjung, Jens Zumbrägel. "Breaking `128-bit Secure' Supersingular Binary Curves (or how to solve discrete logarithms in $F_2$4·1223 and $F_2$12·367)." arXiv:1402.3668. arxiv.org/abs/1402.3668

Provided by Ecole Polytechnique Federale de Lausanne