UC San Diego
UC San Diego News Center

December 04, 2019 | By Ioana Patringenaru

New Record Set for Cracking Encryption Keys

An international team of computer scientists had set a new record for two of the most important computational problems that are the basis for nearly all of the public-key cryptography that is currently used in the real world.

Nadia Heninger is an associate professor in the Department of Computer Science and Engineering at the Jacobs School at UC San Diego.

Public-key cryptography is used in a number of applications including encrypting sensitive and confidential data and digital signatures. In public-key cryptography, keys come in pairs, one public, and one private, and the security of the encryption or digital signature scheme relies on the fact that it is believed to be computationally intractable to compute the private key from the public key. Factoring and discrete logarithm are two of these fundamental problems that are believed to be difficult to solve.

The team factored the largest key yet, a 795-bit integer, and also computed a discrete logarithm of a 795-bit integer. In total, this took them around 35 million hours of computation time.

The key sizes broken by this record computation are not typically used in practice by modern cryptographic applications. However, achieving regular computational records is necessary to update cryptographic security parameters and key size recommendations.

Thanks to algorithmic advances, these calculations have been achieved using much less computational power than had been estimated based on previous records or Moore's law.

The previous records were 768 bits in both cases. The previous factorization record dated from 2010, and the previous discrete logarithm record dated from 2016.

Since both the computational records for factoring and discrete log were achieved simultaneously for the same size integers and on the same computational hardware, this work influences the understanding of the scientific community on the relative difficulty of these two problems. It was commonly believed that the discrete logarithm problem was at least 10 times more difficult than factoring. This work shows that the difference is much less, on the order of a factor of three.

The team was composed of Aurore Guillevic, Paul Zimmermann, and Emmanuel Thome of Inria Nancy, France, Pierrick Gaudry of CNRS Nancy, France, Nadia Heninger of the University of California San Diego, and Fabrice Boudot of the University of Limoges, France.

The researchers carried out this computation using CADO-NFS, which is free software developed by the team at INRIA Nancy. They used a number of computer clusters, including university and national research clusters in France and Germany, and computing equipment managed by Heninger that is now located at UC San Diego.

MEDIA CONTACT

Ioana Patringenaru, 858-822-0899, ipatrin@ucsd.edu