



PERSBERICHT

LEUVEN, 17 August 2011

Researchers identify first flaws in the Advanced Encryption Standard

Researchers have found a weakness in the AES algorithm. They managed to come up with a clever new attack that can recover the secret key four times easier than anticipated by experts.

The attack is a result of a long-term cryptanalysis project carried out by Andrey Bogdanov (K.U.Leuven, visiting Microsoft Research at the time of obtaining the results), Dmitry Khovratovich (Microsoft Research), and Christian Rechberger (ENS Paris, visiting Microsoft Research).

The AES algorithm is used by hundreds of millions of users worldwide to protect internet banking, wireless communications, and the data on their hard disks. In 2000, the Rijndael algorithm, designed by the Belgian cryptographers Dr. Joan Daemen (STMicroelectronics) and Prof. Vincent Rijmen (K.U.Leuven), was selected as the winner of an open competition organized by the US NIST (National Institute for Standards and Technology). Today AES is used in more than 1700 NIST-validated products and thousands of others; it has been standardized by NIST, ISO, and IEEE and it has been approved by the U.S. National Security Agency (NSA) for protecting secret and even top secret information.

In the last decade, many researchers have tested the security of the AES algorithm, but no flaws were found so far. In 2009, some weaknesses were identified when AES was used to encrypt data under four keys that are related in a way controlled by an attacker; while this attack was interesting from a mathematical point of view, the attack is not relevant in any application scenario. The new attack applies to all versions of AES even if it used with a single key. The attack shows that finding the key of AES is four times easier than previously believed; in other words, AES-128 is more like AES-126. Even with the new attack, the effort to recover a key is still huge: the number of steps to find the key for AES-128 is an 8 followed by 37 zeroes. To put this into perspective: on a trillion machines, that each could test a billion keys per second, it would take more than two billion years to recover an AES-128 key. Note that large corporations are believed to have millions of machines, and current machines can only test 10 million keys per second.



Because of these huge complexities, the attack has no practical implications on the security of user data; however, it is the first significant flaw that has been found in the widely used AES algorithm and was confirmed by the designers.

For more information please contact Andrey Bogdanov, tel. +32 488 156780, email: andrey.bogdanov@esat.kuleuven.be or visit <http://homes.esat.kuleuven.be/~abogdano/>.

—

—