NETWORKWORLD

This story appeared on Network World at
http://www.networkworld.com/news/2005/0216reseafind.html

Researchers find security flaw in SHA-1 algorithm

By Paul Roberts , IDG News Service , 02/16/2005

Security experts are warning that a security flaw has been found in a popular and powerful data encryption algorithm, dubbed SHA-1, by a team of scientists from Shandong University in China. The three scientists are circulating a paper within the cryptographic research community that describes successful tests of a technique that could greatly reduce the speed with which SHA-1 could be compromised.

Although the cracking technique could not be carried out practically, it does compromise the integrity of the algorithm and could lead to more advanced attacks that would render SHA-1 useless, affecting many Internet security products that use it to generate digital signatures, according to Bruce Schneier, founder and CTO of Counterpane Internet Security.

SHA-1 is a popular encryption algorithm that was developed by the U.S. National Security Agency (NSA) in 1995 after a weakness was discovered in a predecessor algorithm, called the Secure Hash Algorithm, or "SHA." The algorithm is among those most commonly used to generate "hashes," or unique strings of values that are used to encrypt and decrypt digital signatures, Schneier said.

SHA-1 is used to create signatures by most of the popular security protocols on the Internet, including SSL and PGP (Pretty Good Privacy), he said.

Related Content

A research team of three scientists: Xiaoyun Wang, Yiqun Lisa Yin, and Hongbo Yu, is circulating a paper called *Collision Search Attacks on SHA-1* that describes methods for creating so-called "collisions" with the SHA-1 algorithm 2,000 times more quickly than had been possible before.

"It's phenomenal research," Schneier said. "There's a lot of really impressive math."

A "collision" is an occurrence in which two messages have an identical hash value. It opens the door to forging valid signatures generated using SHA-1. Cryptographers rely on "non repudiation" in algorithms, the concept that two identical hash signatures cannot be created by different signers, said Michael Szydlo, a senior research scientist at RSA Security's RSA Labs.

The results of the paper mark a significant improvement over previous methods of cracking SHA-1 but still

require a massive number of attempts to work -- a number expressed by 1 with thirty zeros after it, he said.

That number of tries could take 1,000 years for a single personal computer to execute and is not practical for all but a few government entities, such as the National Security Agency (NSA), or wealthy private corporations to try, Schneier said.

However, once an algorithm is broken, other scientists can often move quickly to refine the process and produce even better results, he said.

"There's an old (U.S. National Security Agency) maxim: Attacks always get better. They never get worse," Schneier said.

However, the approach used by the Chinese researchers is novel enough that cryptography experts aren't sure whether it can be refined, Szydlo said.

Related Content

The paper has not yet been published but will probably appear on the Web page of the International Association for Cryptographic Research, he said.

Although practical attacks that target SHA-1 are still some time off, cryptographers will have to decide on a replacement for SHA-1 within the next couple of years, and organizations that rely on secure protocols that use SHA-1 will have to evaluate whether the algorithm is adequate to use for secure transactions, experts agree.

"Do you want your online bank account vulnerable to a 1-in-1000 chance that someone could break it?" Schneier asked.

The IDG News Service is a Network World affiliate.