February 14, 2012

Flaw Found in an Online Encryption Method

By JOHN MARKOFF

SAN FRANCISCO — A team of European and American mathematicians and cryptographers have discovered an unexpected weakness in the encryption system widely used worldwide for online shopping, banking, e-mail and other Internet services intended to remain private and secure.

The flaw — which involves a small but measurable number of cases — has to do with the way the system generates random numbers, which are used to make it practically impossible for an attacker to unscramble digital messages. While it can affect the transactions of individual Internet users, there is nothing an individual can do about it. The operators of large Web sites will need to make changes to ensure the security of their systems, the researchers said.

The potential danger of the flaw is that even though the number of users affected by the flaw may be small, confidence in the security of Web transactions is reduced, the authors said.

The system requires that a user first create and publish the product of two large prime numbers, in addition to another number, to generate a public “key.” The original numbers are kept secret. To encrypt a message, a second person employs a formula that contains the public number. In practice, only someone with knowledge of the original prime numbers can decode that message.

For the system to provide security, however, it is essential that the secret prime numbers be generated randomly. The researchers discovered that in a small but significant number of cases, the random number generation system failed to work correctly.

The importance in ensuring that encryption systems do not have undetected flaws cannot be overstated. The modern world’s online commerce system rests entirely on the secrecy afforded by the public key cryptographic infrastructure.

The researchers described their work in a paper that the authors have submitted for publication at a cryptography conference to be held in Santa Barbara, Calif., in August. They made their findings

public Tuesday because they believe the issue is of immediate concern to the operators of Web servers that rely on the public key cryptography system.

“This comes as an unwelcome warning that underscores the difficulty of key generation in the real world,” said James P. Hughes, an independent Silicon Valley cryptanalyst who worked with a group of researchers led by Arjen K. Lenstra, a widely respected Dutch mathematician who is a professor at the École Polytechnique Fédérale de Lausanne in Switzerland. “Some people may say that 99.8 percent security is fine,” he added. That still means that approximately as many as two out of every thousand keys would not be secure.

The researchers examined public databases of 7.1 million public keys used to secure e-mail messages, online banking transactions and other secure data exchanges. The researchers employed the Euclidean algorithm, an efficient way to find the greatest common divisor of two integers, to examine those public key numbers. They were able to produce evidence that a small percentage of those numbers were not truly random, making it possible to determine the underlying numbers, or secret keys, used to generate the public key.

They said they “stumbled upon” almost 27,000 different keys that offer no security. “Their secret keys are accessible to anyone who takes the trouble to redo our work,” they wrote.

To prevent this, one of the organizations that had collected the public keys has removed the information from the Internet and taken steps to protect it from theft.

To perform their study, the researchers used several databases of public keys, including one at the Massachusetts Institute of Technology and another created by the Electronic Frontier Foundation, a Internet privacy rights group. The foundation’s database results from a project, known as the SSL Observatory, originally intended to investigate the security of the digital certificates that are used to protect encrypted data transmitted between Internet users and Web sites.

“We were very careful: we did not intercept any traffic, we did not sniff any networks,” Mr. Hughes said. “We went to databases that contained public information and downloaded public keys.”

The researchers said they were not able to determine why the random number generators had produced imperfect results, but they noted that the problem appeared in more than the work of a single software developer.

They also stated that if they had been able to discover the flaw, it was also possible that it had been previously uncovered, perhaps by organizations or individuals with malicious intent: “The lack of

sophistication of our methods and findings make it hard for us to believe that what we have presented is new, in particular to agencies and parties that are known for their curiosity in such matters," they wrote.

While they said that the publication of results that potentially undermine the security of encryption keys was inappropriate unless the parties were notified first, the researchers noted that the way they discovered the flaw made identifying potentially vulnerable parties a challenge.

"The quagmire of vulnerabilities that we waded into makes it infeasible to properly inform everyone involved, though we made a best effort to inform the larger parties and contacted all e-mail addresses recommended or specified in still-valid affected certificates," they wrote. "The fact that most certificates do not contain adequate contact information limited our options. Our decision to make our findings public, despite our inability to directly notify everyone involved, was a judgment call."

There have been previous failures of random number generators that have undermined Internet security. For example, in 1995, two researchers at the University of California, Berkeley, discovered a flaw in the way the Netscape browser generated random numbers, making it possible for an eavesdropper to decode encrypted communications. Last year a group of computer hackers revealed that Sony had made a crucial mistake in not using a random number in the algorithm used by the security system of the PlayStation 3, making it possible to discover the secret key intended to protect digital content on the system.

The researchers whimsically titled their paper "Ron Was Wrong, Whit Is Right," a reference to two pioneers in public key cryptography, Ron Rivest and Whitfield Diffie.

Mr. Diffie was a developer of the first method for two people who had not previously physically met to share a secret message safely. However, what became known as the R.S.A. algorithm, created by and named after three mathematicians, Mr. Rivest, Adi Shamir and Leonard Adleman, ultimately became the dominant standard. (They later helped found the security company RSA.) The so-called Diffie-Hellman method, developed by Mr. Diffie, Martin Hellman and Ralph Merkle, required only a single secret number.

MORE IN TECHNOLOGY (1 OF 29 ARTICLES)
OPEN
Foxconn Plans to Lift Pay Sharply at Factories in China

Sharply at Factories in China

Read More »