MIT Technology Review

Math Advances Raise the Prospect of an Internet Security Crisis

Academic advances suggest that the encryption systems that secure online communications could be undermined in just a few years.

By Tom Simonite on August 2, 2013

The encryption systems used to secure online bank accounts and keep critical communications private could be undone in just a few years, security researchers warned at the Black Hat conference in Las Vegas yesterday. Breakthroughs in math research made in the past six months could underpin practical, fast ways to decode encrypted data that's considered unbreakable today.

Alex Stamos, chief technology officer of the online security company Artemis, led a presentation describing how he and three other security researchers studied recent publications from the insular world of academic cryptopgraphy research, which covers trends in attacking common encryption schemes.

"Our conclusion is there is a small but definite chance that RSA and classic Diffie-Hellman will not be usable for encryption purposes in four to five years," said Stamos, referring to the two most commonly used encryption methods.

Any hints that those methods could be undermined must be taken seriously, said Stamos. They are used to protect banking, online commerce, and e-mail, as well as the mechanisms that ensure that updates downloaded by operating systems such as Windows and OSX are genuine. The result of the two encryption methods being broken would be, said Stamos, "a total failure of trust on the Internet."

RSA and Diffie-Hellman encryption are both underpinned by a mathematical challenge known as the discrete logarithm problem. That problem is computationally difficult to solve, ensuring that encrypted data can only be decoded quickly with knowledge of the secret key used to encode it in the first place. Breaking RSA or Diffie-Hellman encryption today requires using vast computing resources for significant periods of time.

However, it is possible that algorithms able to solve the discrete logarithm problem quickly could exist. "We rely on that efficient algorithm not being found," said Jarved Samuel, a cryptographer who works for security consultancy ISEC Partners and presented alongside Stamos. "If it is found the cryptosystem is broken."

Earlier this year, French academic Antoine Joux published two papers that suggest such an algorithm could be found before long. "This is a big deal, since there was marginal progress for 25 years," said Samuel. "This will spur researchers into looking more closely at the problem and most likely result in more progress."

One reason to believe that progress will be swift, says Samuel, is that Joux's advances weren't based on inventing completely new techniques. Rather, he applied known tricks that hadn't previously been used on this specific problem. Beating RSA encryption would take a little more additional work, Samuel notes, because it relies less directly on the discrete log problem than Diffie-Hellman encryption does.

However, Stamos believes that once a mathematician publishes a good enough technique, it would quickly be used in online attacks. "Joux or one of these guys could have a breakthrough, throw it onto the crypto mailing lists, and a practical implementation could be worked out in a day or two," he said.

Philippe Courtot, CEO of security company Qualys, singled out Stamos's presentation in a brief speech that opened the Black Hat conference on Wednesday. "The RSA protocol that is the foundation of security on the Internet is likely to be broken in the very near future," he said, noting that while the computer security industry was underpinned by just a handful of key encryption schemes, "we are very slow at adapting them."

Stamos called on the security industry to think about how to move away from Diffie-Hellman and RSA, and specifically to use an alternative known as elliptic curve cryptography (ECC), which is significantly younger but relies on more intractable mathematical challenges to secure encrypted data.

The U.S. National Security Agency has for years recommended ECC as the most reliable cryptographic protection available. In 2005 the agency released a toolkit called SuiteB featuring encryption algorithms to be used to protect government information. SuiteB makes use of ECC and eschews RSA and Diffie-Hellman. A classified encryption toolkit, SuiteA, is used internally by the NSA and is also believed to be based on ECC.

The Russian government has also moved away from RSA for sensitive data, and has declassified its own encryption toolkit that uses ECC. When Russia needed to renew the method for identifying .ru Web domains, it insisted that its ECC algorithms be used.

Implementations of ECC were pioneered and patented by a company called Certicom that is now a subsidiary of the phone manufacturer BlackBerry. Although the U.S. government has purchased licenses that allow the use of ECC by itself and its contractors, other companies that want to use ECC will need to make expensive deals with Certicom to avoid lawsuits. In 2007 Certicom sued Sony for using ECC in software for BlueRay DVDs without licensing its patents. Sony initially attempted to have some patents invalidated in court, before settling out of court in 2009.

Stamos called on BlackBerry to change its policy regarding the Certicom patents, suggesting it could allow open use of them for SuiteB-based systems using ECC, but still make significant revenue from other use cases. "There's not a company in the world that has the opportunity that BlackBerry has right now," he said, adding that if RSA and Diffie-Hellman were broken, the U.S. government would likely overturn Certicom's patents in the national interest. "If the cryptopocalypse happens, those patents are

not going to last."

Some in the security community speculate that cryptographers at the NSA may have already figured out how to break many common encryption schemes. The sophisticated Flame malware discovered last year featured a completely new mathematical technique to defeat an encryption method used to verify some software updates as originating with Microsoft, allowing Flame to masquerade as legitimate software. Flame is presumed to have been created by a government, perhaps the United States, and Stamos joked that it originated with someone who had significant computing resources "in their basement, in Maryland," the state where the NSA and many defense contractors are based.

However, Moxie Marlinspike, cofounder of Whisper Systems, which develops apps for encrypted calls and texts on smartphones, told *MIT Technology Review* in advance of Stamos's talk that he believed the leading edge of cryptographic research remains mostly out in the open. "I don't think they're ahead of us," he said, referring to the government. Federal pay scales, which are public, lag far behind those in the private sector, Marlinspike pointed out, something he believes keeps the best cryptographic talent in the private sector.

Tagged: Computing, Communications, Web, Black Hat, Black Hat security conference, RSA