THE GLOBE AND MAIL

DATA SECURITY

The strange connection between the NSA and an Ontario tech firm

OMAR EL AKKAD - TECHNOLOGY REPORTER
The Globe and Mail

Published Monday, Jan. 20 2014, 5:00 AM EST
Last updated Monday, Jan. 20 2014, 7:49 AM EST

At the heart of digital security is the concept of encryption – making information indecipherable to anyone who doesn't have the right passcode.

And since 1995, any software developer building encryption for technology they intended to sell to the American or Canadian government has had to consult something called the Cryptographic Module Validation Program. It's a list of algorithms blessed by the CMVP that are, according to the government agencies that publish it, "accepted by the Federal Agencies of both countries for the protection of sensitive information."

More Related to this Story

- Cybercrime firm uncovers six active attacks on U.S. merchants
- NSA researches quantum computers in quest to crack private encryption: report
- Obama announces ban on spying on dozens of foreign leader allies

There's only one problem. For more than six years, one of the central items listed in the CMVP – an algorithm for generating the random numbers that form the foundations of an encryption scheme – has had a glaring and well-known backdoor, a means of rendering the encryption totally ineffective.

"This has been known since 2006," said Steve Marquess, co-founder of the OpenSSL Software Foundation. "Why the heck was this officially blessed? A lot of my colleagues and a lot of people in the cryptography community are asking that question."

Today, many of those people are coming to the conclusion that the flaws in the algorithm were not the product of sloppy work, but deliberately inserted to make it easy for at least one spy agency – the National Security Agency – to break the encryption.

Because the algorithm in question made it onto the CMVP, it was used by dozens of technology companies looking to make their products government-approved.

Such companies include BlackBerry Ltd. – which not only uses the algorithm, but also owns the patent on the concepts that form its foundations.

In addition to BlackBerry, companies such as RSA Security LLC, Cisco Systems Inc., Samsung Electronics Co. Ltd., Symantec Corp. are all known to have implemented the algorithm in some of their products.

And the revelation that American and Canadian agencies (the CMVP is a joint venture between the U.S. National Institute of Standards and Technology and the Communications Security Establishment Canada) gave its blessing to a compromised encryption scheme has erupted into a major scandal within the cryptography community, the roots of which can be traced back to a Mississauga computer security firm.

In early 2005, two employees at Mississauga-based Certicom Corp. began filing a patent application for a type of random number generator using a mathematical concept called elliptic curves. The patent also described another functionality – a set of keys that could be used, for example, by “trusted law enforcement agents” to do an end-run around the encryption. (Dan Brown, one of the Certicom employees who filed the patent, did not respond to a request for comment.)

At the time, the patent generated relatively little interest. But in 2007, the NIST released its new list of approved encryption algorithms. There were four items on the list, one of which was called Dual Elliptic Curve Deterministic Random Bit Generator, or Dual_EC_DRBG for short.

From the very beginning, cryptographic researchers noticed something strange about

Dual_EC. In 2007, two Microsoft researchers showed that the algorithm contained a set of constants that, when combined with a secret key, could essentially break the encryption generated by Dual_EC. In effect, Dual_EC implemented in the real world a version of the backdoor described in the Certicom patent.

Nobody could say for certain who had the secret key. But the very existence of such a backdoor caused security researchers to strongly urge a boycott of Dual_EC.

“While we were saying don’t use it, don’t use it, government contractors were demanding it,” security researcher Bruce Schneier said.

For years, many wondered why the NIST in America and CSEC in Canada would continue to give their official blessing to a compromised algorithm. Last year, a potential answer to that question emerged, when documents leaked by Edward Snowden revealed the NSA to be a holder of the Dual_EC secret keys – essentially, allowing the spy agency to crack the encryption at will. In addition, a Reuters report in December revealed that the NSA had paid RSA Security LLC $10-million to continue making Dual_EC the default form of encryption on its products.

In BlackBerry's case, an NIST fact sheet shows the company implemented the algorithm as part of its cryptography toolkit for its BlackBerry 10 Enterprise service, among other products. But BlackBerry's relationship with Dual_EC is even closer than other companies. In 2009, the company purchased Certicom – in the process acquiring the patent that forms the basis for the Dual_EC algorithm.

Given the company's adamant denials in recent years that it offers backdoor access to intelligence agencies, critics argue BlackBerry owes its customers and shareholders an explanation.

"While it is true that many engineers and others were aware of this compromised algorithm, and the engineering security community as a whole is now dealing with this apparent lack of integrity among its members, in the case of BlackBerry's knowledge of the backdoors the implications are far more serious," said Ronald Deibert, director of the Citizen Lab at the University of Toronto's Munk School of Global Affairs. "Users of BlackBerry the world over … must now assume without evidence to the contrary that all of their communications are shared with security services, and possibly industry competitors as well."

BlackBerry did not respond to a request for comment for this story.

A CSEC spokesperson would not say whether the Canadian agency had any say in including Dual_EC in the list of approved algorithms. "Guidance approved by NIST and CSE recommends several different algorithms which commercial developers can choose to implement in their products," the spokesperson said. "CSE continually reviews its guidance on algorithm use. Accordingly, we will update our guidance once our latest review, currently under way, is complete."

In September, the NIST began urging users not to use Dual_EC any more. A spokesperson said "community concerns" prompted the change. "NIST takes seriously the concerns of the cryptographic community, which plays an integral role in the development of cryptographic standards," the spokesperson said.

But researchers are now questioning what other backdoors have yet to be discovered, and whether the NSA made similar payments to other companies to keep flawed algorithms in use. "This is the poison of NSA action, they taint everything," Mr. Schneier said. "You have no idea what has been tainted, so you think everything is tainted."

More Related to this Story

- Globe editorial The NSA has too many eyes, still prying

Topics:

- Technology

- National Security Agency
- National Institute of Standards and Technology
- Certicom Inc.
- BlackBerry Ltd.
- RSA Security Inc.