Experts withdraw from Internet security conference

January 8 2014, by Jack Gillum

At least eight researchers or policy experts have withdrawn from an Internet security conference after the sponsor reportedly used flawed encryption technology deliberately in commercial software to allow the National Security Agency to spy more easily on computer users.

RSA Security, owned by data storage giant EMC Corp., has disputed claims it intentionally introduced the flawed encryption algorithm, but otherwise has declined to discuss what a published report last month described as a $10 million government contract.

The revelation supplemented documents leaked by former NSA contractor Edward Snowden showing that the NSA tried to weaken Internet encryption.

The pullouts from the highly regarded RSA Conference represent early blowback by technology researchers and policy experts who have complained that the government's surveillance efforts have, in some cases, weakened Internet security even for innocent users.

Some U.S. companies that have agreed or been compelled to turn over customer records to the government have complained that their business relationships with customers in Europe, Asia and elsewhere are increasingly becoming arduous.

It was not immediately clear whether any researchers who still intended to make presentations at the conference would discuss the subject. Hugh

Thompson, a conference organizer who works for security firm Blue Coat Systems, said the event is "an open venue where people can talk openly about security."

The researchers and experts include Mikko Hypponen, chief research officer of Finland-based antivirus provider F-Secure, and Adam Langley and Chris Palmer, who work on security practices at Google.

Christopher Soghoian, a researcher with the American Civil Liberties Union, said Tuesday on Twitter that he withdrew from the conference after having "given up waiting for RSA to fess up to the truth" regarding its development of the Dual_EC_DRBG algorithm with the NSA.

RSA issued an advisory to its customers last summer urging them not to use the algorithm, following published reports of the software's potential weaknesses. But that wasn't enough for researchers who want answers about the government's contract with RSA, which thousands of businesses use to secure their data.

RSA said in a statement last month that as a security company, it "never divulges details of customer engagements, but we also categorically state that we have never entered into any contract or engaged in any project with the intention of weakening RSA's products, or introducing potential 'backdoors' into our products for anyone's use."

The published report said RSA received the $10 million contract from the NSA to use the agency's preferred method of number generation. The report said such a flawed algorithm in RSA's Bsafe software tool generates random numbers in such a way that it creates "backdoors" into the company's encryption products.

Organizers said next month's conference in San Francisco will host 560 speakers, and they expect more participants than the 24,000 who showed

up last year.

The NSA has a history in developing encryption algorithms, with documents showing decades-old criticisms among civilian government scientists about the agency's role in developing communication standards. That includes scientists' discomfort, as early as the 1980s, over the Digital Signature Standard, a way to electronically sign documents and guarantee their authenticity. That became a federal processing standard by 1994.

In September, documents leaked by Snowden showed that the agency more recently wanted to water down Internet encryption in an effort to gather and analyze digital intelligence. In turn, the federal National Institute of Standards and Technology tried to shore up confidence in the important behind-the-scenes role it plays in setting standards that are used by consumers to make purchases online, access their bank accounts or file their income taxes electronically.

The Office of the Director of National Intelligence said that "it should hardly be surprising that our intelligence agencies seek ways to counteract our adversaries' use of encryption."