Can You Trust NIST?

Lily Hay Newman ⋮ 7-9 minutes ⋮ 10/9/2013

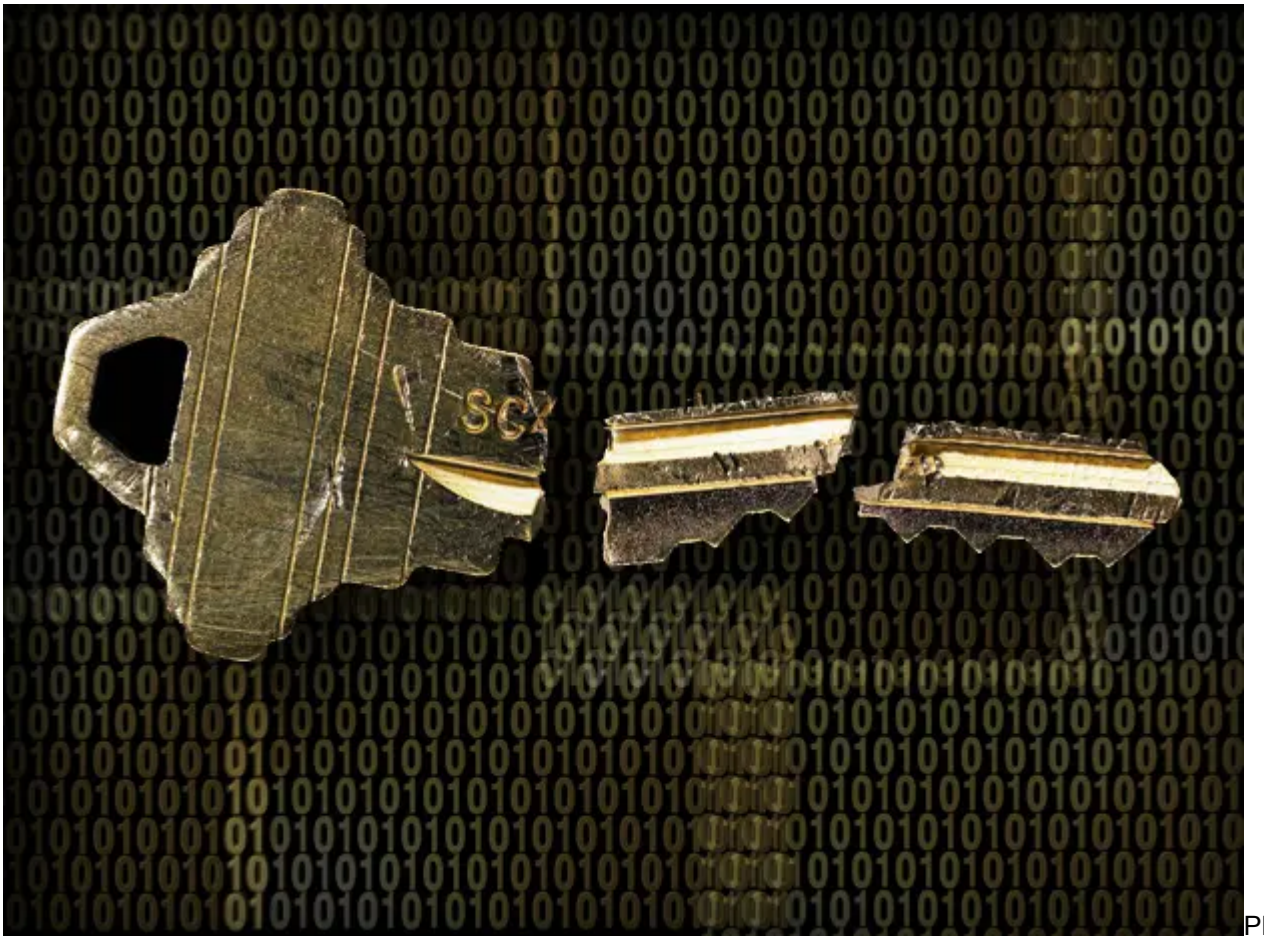

Photo-illustration: Randi Silberman Klett

The National Institute of Standards and Technology (NIST) has an image problem. Last month, revelations surfaced indicating that the National Security Agency (NSA) may have planted a vulnerability in a widely used NIST-approved encryption algorithm to facilitate its spying activities. And cryptographers are also questioning subtle changes that might weaken a new security algorithm called Secure Hash Algorithm-3, or SHA-3. Encryption experts say NIST's reputation has been seriously undermined but that the security community would like to continue using it as a standards body if it can show that it has reformed.

NIST, which sets U.S. federal standards for a number of things, including measurement instruments and the length of a second, also works in cryptography to release standards for functions that protect data. These algorithms must be present in any relevant hardware used by government agencies and contractors. Therefore, although NIST has no jurisdiction over academic or commercial security, the enormous purchasing power of the U.S. government and NIST's funding resources have made it a big player in the global cryptography community.

Noted cryptographer Bruce Schneier says that the security community has relied on NIST to develop agreed-upon standards because "they were a really good, honest broker, and they were perceived to be fair and unbiased." But recent events have dealt a blow to that perception, he says.

The algorithm at the center of the biggest controversy, Dual Elliptic Curve Deterministic Random Bit Generation (Dual EC DRBG), has been suspect since the NSA proposed its inclusion as a random-number generator in a 2006 NIST release. But documents leaked by ex-NSA contractor Edward

Snowden and excerpted by *The New York Times* suggest that the NSA deliberately introduced a vulnerability into it.

The disclosure prompted leading security firm RSA to announce that Dual EC DRBG was the default random-number generator in one of its encryption services and to recommend that customers use a different generator from the company's library.

Dual EC DRBG immediately raised red flags because it was orders of magnitude slower than the other number generators proposed alongside it, and also because it wasn't very random. Random-number generators are crucial for encryption because they prevent a security system from being predictable and therefore vulnerable to attack.

Critics of Dual EC DRBG demonstrated ways that an attacker could anticipate the numbers the generator would put out, such as by knowing one variable—*e*—in the curve equation.

Microsoft security employees Dan Shumow and Niels Ferguson presented this weakness [PDF] at the Crypto security conference in 2007. "If an attacker knows *e*, then they can determine a small number of possibilities for the internal state of the Dual Ec PRNG and predict future outputs," they wrote in their presentation.

Furthermore, there was a set of constants NIST had released for use in implementing the algorithm, but it is unclear how that group of numbers was agreed upon. Most likely, the NSA created them when it produced Dual EC DRBG, and the agency could have simultaneously generated a second set, enabling it to later decrypt data protected by Dual EC DRBG.

Despite far-reaching concerns about Dual EC DRBG, NIST still approved it as a standard number generator. And as vendors worked to comply with their government contracts, or scored new ones, they were forced to add support for it even if they did not make it their default number generator. But now, in light of the leaked NSA documents, NIST is reevaluating the cohort of random-number generators that includes Dual EC DRBG, and it has opened a public forum on its website where the cryptography community can raise concerns.

"Reopening these for comments is a good idea," says Steven Bellovin, a network security researcher at Columbia University who won the 2007 NIST/NSA National Computer Systems Security Award. As for the results, he says, "there will be consensus on Dual EC: Get rid of it."

It appears that the only way for NIST to remain a credible standards body is through total transparency in its review process. And from the start of this recent controversy, NIST has apparently been aware of this imperative. The agency could not be reached for comment because of the U.S. federal government shutdown, but it said in a statement in early September that "NIST use[s] a transparent, public process to rigorously vet our recommended standards. If vulnerabilities are found, we work with the cryptographic community to address them as quickly as possible."

Dual EC DRBG isn't the only fishy thing cryptographers are concerned about, however. Schneier and Bellovin also flagged changes that NIST made recently to a new hash function, a mathematical operation that produces a kind of digital fingerprint of a set of data.

The new function, SHA-3, was the result of a multiyear international competition overseen by NIST. The standards body ran a contest from 2007 to 2012 to find a new hash function that would complement and back up the previously approved SHA-2 in case it was ever cracked. Almost all phases and aspects of the competition were open to the public via extensive online documentation, but the NIST committee's deliberations were not public, so it was unclear exactly how it determined which teams would advance through the various rounds. And recently NIST made minor but suspicious changes to the winning SHA-3 hash function, known as Keccak. A new draft of the standard is due out later this month, although it may be delayed by the shutdown. The standard will incorporate two rather than the proposed four versions of the hash and some internal changes to the Keccak algorithm that experts fear will reduce SHA-3's security.

Yevgeniy Dodis, a cryptography professor at New York University, says that NIST's proposed changes seem innocuous but are counterproductive, because they reduce the relevance of the community's testing during the competition. If the hash function that becomes SHA-3 is different from the one vetted by the community, then the process is less valuable, he says.

There are certainly other standards bodies that the cryptography community could turn to, including those in Russia, Japan, and Europe. (ENISA, the European Union Agency for Network and Information Security, declined to comment.) But NIST has the broadest reach of them all and is considered the most prestigious. So, in spite of concerns about the NSA's influence, it appears that NIST still has a strong ability to generate quality research internally and through its international competitions. "In terms of people who are there, in terms of the resources they have, the power, the popularity, outreach, it's really the central body," Dodis says.

Going forward, openness will be crucial, but the nature of NIST's relationship with the NSA remains unclear. Bellovin, Dodis, and Schneier all say they have positive professional relationships with the researchers in the security group at NIST and would like NIST to get past its problems and continue in its role.

"NIST was, as best I can tell, blindsided by what the NSA apparently did to the Dual EC generator," Bellovin says. "That revelation has badly hurt them. They've compounded it by suggesting an apparent weakening of Keccak. I believe that NIST realizes the problem and will backpedal, but that remains to be seen. They certainly need to."

Previous Chapter Next Chapter