Mathematicians Discuss the Snowden Revelations

This is the latest installment in the *Notices* discussion of the National Security Agency (NSA).

The previous installment, "The Mathematics Community and the NSA," by Michael Wertheimer, appeared in the February 2015 issue and includes a list of all previous articles in the discussion.

Unsolicited submissions on this topic are welcome. Inquiries and submissions may be sent to notices-snowden@ams.org. Submissions of 400 words or fewer can be considered as Letters to the Editor and should be sent to notices-letters@ams.org.

—Allyn Jackson
Notices *Deputy Editor*
axj@ams.org

Cryptographic Standards, Mass Surveillance, and the NSA

Bart Preneel

The *Notices* has hosted a lively debate on the role of mathematics in mass surveillance systems deployed by the National Security Agency (NSA). Similar debates have been held in the cryptology, security, and privacy communities. However, in most countries, the public debate and political implications of the Snowden documents have been very limited, despite the continuous stream of revelations.

I was invited to contribute to the discussion, partly because of my role as advisor to the National Institute of Standards and Technology (NIST). In early 2014, NIST requested from its Visiting Committee on Advanced Technology (VCAT) an assessment of the development of NIST cryptographic standards and guidelines, including recommendations for improvements. VCAT was assisted by a committee of technical experts on this matter, and I served as the only non-US citizen on this committee. The VCAT report can be found at [7]. In this article I focus on the undermining of cryptographic standards by NSA and on the broader topic of mass surveillance and its implications.

NSA's Conflict between Offense and Defense

An important element in this debate is the dual role of NSA: it must collect and analyze foreign communications and foreign signals intelligence, and it must protect government communications and information systems. There is an obvious potential for conflict between the roles. Moreover, such a conflict typically leads to offense trumping defense: it is much easier to demonstrate successful interception and decryption of foreign communications than to demonstrate that the US government's systems have not been breached. So while the defense part of NSA wants cryptographic standards that are as strong as possible, the offense part launches programs such as BULLRUN, which, according to internal NSA documents leaked by Edward Snowden, has as its goal to "Insert vulnerabilities into commercial encryption systems, IT systems, networks, and endpoint communications devices used by targets."

Cryptographic random number generators generate random bitstrings that are used as cryptographic keys and as unique values in protocols. Because cryptography protects data through secret keys, undermining the generation of keys means jeopardizing the security of the cryptosystem using those keys. In 2006, NIST published a standard covering four cryptographic random

Bart Preneel is a professor at the Katholieke Universiteit Leuven and heads the Computer Security and Industrial Cryptography research group that is a member of the iMinds Security Department. His email address is bart.preneel@esat.kuleuven.be.

DOI: http://dx.doi.org/10.1090/noti1237

number generators, including an algorithm based on elliptic curve cryptography, the Dual_EC_DRBG. If one knows the relation between the elliptic curve points used in this algorithm, one possesses a "trapdoor" that allows one to find the keys to the cryptosystem. The NSA designed the Dual_EC_DRBG algorithm, and there is evidence suggesting that the algorithm does in fact harbor a trapdoor. The mathematical basis for this evidence was described lucidly in the *Notices* article by Hales [5].

An open discussion of the possibility of a trapdoor in the Dual_EC_DRBG algorithm took place at a conference in 2007, but clear evidence of the potential for a trapdoor appeared already in 2005. For example, the trapdoor is mentioned in US patent 2007189527 with priority date January 21, 2005 [2]. The NSA should have withdrawn its support before the algorithm ended up in any standard. Indeed, in his article in the *Notices* [9], Michael Wertheimer, the now-retired director of Research at the NSA, expresses his regret about the agency's failure to drop its support for the Dual_EC_DRBG algorithm: "With hindsight, NSA should have ceased supporting the Dual_EC_DRBG algorithm immediately after security researchers discovered the potential for a trapdoor."

Wertheimer notes that Dual_EC_DRBG was only one of four algorithms in the NIST standard and asserts that "it is neither required nor the default." However, in practice the validation process is slow and expensive. Hence, for a product designer, it is risky to implement fewer than four algorithms: if later a customer requires a missing algorithm, a new validation process would be needed. Moreover, in 2004, the widely used cryptographic library BSAFE changed its default algorithm to Dual_EC_DRBG. *Reuters* reported in 2013 that this decision was the result of a secret US$10 million deal between RSA and the NSA [6].

Wertheimer also argues that one could use parameter values other than the ones specified in the standard; the values believed to be trapdoored were necessary for validation, but not for actual use. However, this seems to have been only a theoretical possibility. First, alternative parameter values need to be hard-wired into the source code or hardware for a cryptosystem, so only the vendor can generate them, not the user (unless the user provides the parameters before the certification process). Second, the procedure for validating additional parameter values was unclear, so validating alternative parameters would have caused substantial delays. NIST is not aware of any vendor who managed to get such values validated.

Previously, the NSA raised doubts about the feasibility of exploiting the alleged trapdoor in Dual_EC_DRBG. These doubts were laid to rest by the work of Checkoway et al. [4], which shows efficient attacks on the Transport Layer Security (TLS) protocol. This paper also points out that four proposals were made (including one explicitly motivated by a request from the Department of Defense) to modify TLS such that it would have been substantially easier to exploit the trapdoor. Fortunately, none of these extensions were adopted.

One cannot escape the conclusion that the NSA has indeed tried to subvert cryptographic standards in order to make it easier to decrypt intercepted communications. The NSA has understood that the research community considers this a breach of trust, and it promises more transparency in its standardization work. In the past the NSA has not been transparent about the cryptographic algorithms it has designed for public use (admittedly the number of such algorithms has been limited). The NSA has not provided design rationales, proof of security against specific attacks, and cryptanalysis of reduced versions—all of which are standard requirements for anyone proposing such algorithms. In view of this track record, the academic community should apply a high standard of transparency to the NSA.

Of course I do recognize the legitimate right of the US government to develop advanced cryptanalytic techniques without publishing them, and I appreciate that publishing full design documents and partial attacks might leak some information on NSA's cryptanalytic techniques. But the NSA can't have its cake and eat it too. If the NSA wants the academic and standards communities to consider its designs, it has to offer full transparency for them.

While cryptographic algorithms are of natural interest to mathematicians, I also want to cover the broader impact of mass surveillance.

The Impact of Mass Surveillance is Underestimated

The position of the intelligence agencies is that the current surveillance regime is necessary, proportionate, limited (with strong filtering), and within the boundaries of the law. On the other hand, the NSA itself describes a very different "collection posture" in its internal documents: "Collect it All," "Process it All," "Exploit it All," "Partner it All," "Sniff it All," and, ultimately, "Know it All." Devlin [3] has pointed out that this massive collection is ineffective, and so far the intelligence community has failed to produce evidence to the contrary.

Technological developments have certainly made surveillance a more complex business. But those same developments have opened up new opportunities for intelligence agencies. It is now possible to intercept and store massive quantities of data that touch every aspect of our personal lives, and this is routinely done by the private sector. With the development of personal health devices and The Internet of Things, ever more personal data will become available. Through sophisticated analysis, profiles can be derived and social networks and behavioral patterns can be exposed. A frequently debated question is: Which is the bigger threat to citizens, the private sector or the intelligence agencies? However, this seems to be the wrong question. What we have learned from the Snowden documents is that intelligence agencies have multiple programs through which they obtain access to personal data in the hands of private companies (voluntarily, or through coercion or bribery). As a consequence, it is in the agencies' interest that companies collect as much information as possible. These programs were secret, so there was no opportunity for a public debate on the broader risks of this approach. As governments try to limit excessive data collection in the private sector, the same conflict of offense versus defense emerges, but now between different branches of the government.

Another issue is that of whom the security agencies are permitted to target. Anyone considered to be a "US person," which includes citizens as well as foreigners residing in the US, is protected by the Fourth Amendment prohibiting unreasonable searches and seizures. As technology evolves, the courts need to interpret the Fourth Amendment. A major concern is the collection of metadata—that is, information about whom you are calling, which web sites you are visiting, which device(s) you are using, and where you are. In spite of claims to the contrary ("it is only metadata"), metadata is data and can be extremely sensitive. The collection of metadata on US persons (such as the collection of Verizon telephone records, as disclosed by Snowden in June 2013) is a central point of the debate in the US.

In 2006, the European Union issued the Data Retention Directive, which forced telecoms to collect metadata. The motivation was the fight against cybercrime, but there is little doubt that this information has also been used for national security purposes and is shared with other nations. In April 2014, the Court of Justice of the European Union declared the Data Retention Directive invalid, as it violates two rights listed in the Charter of Fundamental Rights of the EU, namely the fundamental right to respect for private life and the fundamental right to the protection of personal data. Interestingly, this charter applies to any person, including US citizens, wherever they reside. By contrast, the legal view held in the US is that Fourth Amendment rights do not apply to non-US citizens, unless they are on US territory. This is a serious concern, as non-US citizens increasingly depend on US technology, and their data is stored in cloud services run by US companies. Human rights are universal and should not depend on citizenship. More details on the implications of US exceptionalism can be found in Bowden's analysis [1].

In the context of the massive surveillance efforts of the NSA, encrypted communications are considered "a threat." Consequently, the NSA has applied every conceivable method to crack encryption, including mathematical cryptanalysis of cryptographic algorithms and protocols, exploiting bugs or inserting trapdoors in hardware or software implementations, and obtaining the keys through security letters or malware against user devices and routers. Malware will likely exploit new vulnerabilities (so-called 0-days) that the NSA has obtained either through research or from vendors. An article published in *Der Spiegel* in December 2014 [8] shows that the NSA intended to use these and other methods to crack ten million TLS connections a day by late 2012; other protocols that are reported as vulnerable to these techniques are IPsec (Internet Protocol Security) and SSH (Secure Shell).

The picture that emerges is worrisome: intelligence agencies go way beyond collecting communications on specific targets based on selectors. They launch active attacks on networks and end systems and take de facto control of the Internet. In order to enable this mode of operation, they exploit undiscovered vulnerabilities (rather than making sure those get patched immediately) or may even insert new vulnerabilities in systems, with or without cooperation of the vendors. Making the Internet secure without interference by intelligence agencies is a daunting task. If those agencies are spending huge budgets to hide or insert vulnerabilities and to undermine standards efforts, this task becomes a mission impossible. Moreover, one can expect that other nations might start applying the same strategy. These concerns deepen as our critical infrastructures increasingly depend on this very same Internet.

Technological developments have given intelligence agencies unprecedented power. This increases the risk of abuses. The largest concerns are not NSA employees monitoring their love interests or typing errors in telephone numbers, but the fact that highly sensitive information is available on politicians and on active members in civil society, who are typically at the core of positive changes. On the international level, there is the risk of interference with foreign governments, manipulation of electronic elections, and industrial espionage. Moreover, ubiquitous surveillance transforms society through mechanisms such as self-censorship and encourages conformity. In history it is associated with societies that are repressive and authoritarian.

Developing effective and transparent oversight mechanisms to control this power is challenging. The technological developments impose a continuous recalibration of the rules, which requires a deep understanding of technology. Secret laws and secret interpretations are clearly not acceptable, but intelligence agencies by nature cannot be fully transparent. We need broadly accepted methods that restrict surveillance to the minimum necessary and that allow independent verification without compromising sensitive information. This presents a major challenge to the research community: social and legal scholars should explore together with mathematicians and computer scientists how we can reconcile these conflicting requirements.

The stakes are very high. If we fail, we might—in the name of fighting terrorism—destroy the freedom and openness that make our societies worth living in.

References

[1] C. Bowden, *The US Surveillance Programmes and Their Impact on EU Citizen's Fundamental Rights (2013)*, www.europarl.europa.eu/meetdocs/2009_2014/documents/libe/dv/briefingnote_/briefingnote_en.pdf.

[2] D. R. L. Brown and S. A. Vanstone, *Elliptic curve random number generation*, US patent 2007189527, August 16, 2007.

[3] K. Devlin, The NSA: A Betrayal of Trust, *Notices of the AMS* **61(6)** (2014), 624–626.

[4] S. Checkoway, R. Niederhagen, A. Everspaugh, M. Green, T. Lange, T. Ristenpart, D. J. Bernstein, J. Maskiewicz, H. Shacham, and M. Fredrikson, On the Practical Exploitability of Dual EC in TLS Implementations, *USENIX Security* (2014), 319–335.

[5] T. C. Hales, The NSA Backdoor to NIST, *Notices of the AMS* **61(2)** (2014), 190–192.

[6] J. Menn, Secret contract tied NSA and security industry pioneer, December 20, 2013, www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.

[7] NIST VCAT, *NIST Cryptographic Standards and Guidelines Development Process* (2014), www.nist.gov/public_affairs/releases/upload/VCAT-Report-on-NIST-Cryptographic-Standards-and-Guidelines-Process.pdf.

[8] Der Spiegel, Prying Eyes: Inside the NSA's War on Internet Security, December 28, 2014, www.spiegel.de/international/germany/inside-the-nsa-s-war-on-internet-security-a-1010361.html.

[9] M. Wertheimer, The Mathematics Community and the NSA, *Notices of the AMS* **62(2)** (2015), 165–167.