Highlights from Making Sense of Snowden, Part II:

What's Significant in the NSA Revelations

Susan Landau | Google

In the July/August 2013 issue of *IEEE Security & Privacy*, we published Susan Landau's analysis of the impact of Edward Snowden's initial leak of documents. As more files are revealed, we want to provide up-to-date analysis of what they mean to you, our readers. Accordingly, we're posting an in-depth follow-up to Landau's original article (http://doi.ieeecomputersociety.org/10.1109/MSP.2013.90), which we'll revise periodically as new information becomes public. Landau's in-depth analysis not only summarizes what we know but also offers references that might prove useful in helping you come to your own conclusions about the leaks' import and impact.

—Shari Lawrence Pfleeger, editor in chief

In June 2013, the English newspaper *The Guardian* began publishing a series of secret documents leaked from the National Security Agency (NSA). Each day brought startling news, from the NSA's collection of metadata records of all calls made within the US[1] to programs that collected and stored data of "non-US" persons[2] to the UK Government Communications Headquarters' (GCHQ) interception of 200 transatlantic fiberoptic cables at the point where they reached Britain.[3] I summarized these initial revelations in the July/August issue of *IEEE Security & Privacy*.[4] Writing in mid-December, I provde highlights of what the last few months have revealed; a detailed discussion appears online at http://doi.ieeecomputersociety.org/10.1109/MSP.2013.161. Meanwhile, in late December, in a different district court case, the NSA metadata collection was ruled legal (http://online.wsj.com/public/resources/documents/clapper.pdf).

What We've Learned

By early July, the torrent of leaks had slowed; it seemed as if the most important secrets had been revealed. But in early September, *The Guardian* reported NSA compromises of internationally used cryptographic standards.[5] Additional documents showed NSA efforts to break other secure communication systems.[6,7] Later leaks showed the NSA had directly targeted German Chancellor Angela Merkel, a close US ally.[8] Other documents showed Australia, a partner of the "Five Eyes"—the intelligence alliance consisting of Australia, Canada, New Zealand, the US, and the UK—had been targeting Indonesian president Susilo Bambang Yudhoyono, a close Australian ally.[9] Yet another shoe dropped when *The Washington Post* revealed that the NSA was targeting both Google and Yahoo's inter-datacenter communications;[10,11] there were indications Microsoft's inter-datacenter communications were also being accessed.[12] The US-based companies expressed outrage.

For the US public, one issue was the bulk collection of stored metadata. The Foreign Intelligence Surveillance Court (FISC) had permitted this under a secret interpretation of the 2001 USA PATRIOT Act. That the decision was secret wasn't unusual; the court operates in secret and without anyone to argue against the government's position.

During the initial set of NSA leaks, the US government tried to downplay this metadata collection, with the president noting that the NSA wasn't listening to anyone's domestic calls without a warrant.[13] But transactional information—the who, when, how long, and where of a call or email—is remarkably revelatory.[14–18] As former NSA

Copublished by the IEEE Computer and Reliability Societies
1540-7993/14/$31.00 © 2014 IEEE

General Counsel Stewart Baker noted, "Metadata absolutely tells you everything about somebody's life. If you have enough metadata, you don't really need content."[19]

The rest of the world doesn't have the same protections against warrantless searches that US persons enjoy; instead, their concerns centered on content collection, specifically about the massive collection of communications and content of non-US persons and the targeting of foreign leaders.

The June leaks showed that the GCHQ was tapping transatlantic fiberoptic cables—in fact, since July 2009, the British agency had been able to collect 2.5 Gbits per second of data flowing through transatlantic fiberoptic cables (http://apps.washingtonpost.com/g/page/world/the-nsas-three-types-of-cable-interception-programs/553). Access was 10 Gbits per second in 2010 and has been steadily increasing ever since. The collected data is shared with the NSA.[3]

The October leaks showed that the NSA was collecting inter-datacenter traffic at both Google and Yahoo. (Disclaimer: I work for Google, but the opinions expressed in this article are mine and not those of my employer. Material presented here comes solely from public sources.) This wasn't front-end access with a warrant; it was back end, apparently done without the companies' knowledge. Future foreign avoidance of US-based datacenters may ultimately result in US companies losing tens of billions of dollars because of the NSA interception activities.[20]

In addition to Chancellor Merkel's cell phone, the NSA was apparently tapping Mexican leader Enrique Pena Nieto's email[21] and Brazilian President Dilma Rousseff's cell phone.[22] While it's normal for nations to spy on one another, such targeted spying on allied leaders is not. The international outcry was strong and angry.

How does the NSA conduct such massive surveillance? Access was enabled through fiberoptic cables—and the fact that the 2008 US Foreign Intelligence Surveillance Amendments Act loosened the rules for wiretapping if one end of a communication is outside the US. There were also various network exploitation tools used; some of these also worked against the specific targets. The ability to read encrypted communications was another matter, and the source of one of the most disturbing revelations of the whole affair.

Cybersecurity and cyberexploitation issues won't be going away, and how all this will play out in the long term remains to be seen.

The Ultimate Cost of NSA Surveillance

While it has long been suspected that the NSA has attempted to compromise cryptographic implementations in deployed systems, the September leaks showed that the signals-intelligence agency had gone a major step further, compromising a National Institute of Standards and Technology (NIST) cryptographic standard.[23] The apparent standard in question, Dual EC-DRBG, was a random-bit generator that was both remarkably slow and appeared to have a back door inserted. NIST immediately deprecated the standard.[24]

The NSA's actions caused great damage. Although NIST's official role is to develop standards for use in US federal civilian agencies, the agency's reputation for fairness and honesty in the standardization process means that its standards are often widely adopted, including internationally. It will take time and much effort for NIST to regain that trust—if it can. The NSA sabotage of a cryptography standard harmed communications security. For example, using the compromised standard to generate the "Client Cryptographer Nonce" during an SSL connection enables the NSA to decrypt encrypted transmissions.[25] The sabotage also hurt industry. This includes those reliant on RSA Security's BSAFE toolkit, which used Dual EC-DRBG as the default random-bit generator. RSA quickly recommended switching to a different generator (the standard had three alternatives). But given concerns raised in 2007 about Dual EC-DRBG's security, it's RSA Security's integrity that is very much on the line.[26]

Where was the oversight? The FISC was supposed to provide it, but examination of court opinions released by the government in the wake of the leaks shows repeated instances where problems arose because of lack of clarity, policy, and understanding. Congressional oversight was hampered for many reasons, including incomplete and misleading statements by the intelligence agency (www.dni.gov/files/documents/2013-06-21%20DNI%20Ltr%20to%20Sen.%20Feinstein.pdf). There are now several efforts in play, from proposed bills to a presidentially ordered review board report that made strong recommendations on limiting surveillance of non-US persons to exclusively national security interests of the US and its allies, and that the government shouldn't collect and store "mass, undigested non-public personal information about US persons for ... future queries and data mining" for foreign intelligence purposes.[27] The government's response remains to be seen.

For more than a decade, the US government has been expressing increasing concern over the inability of US industry and critical infrastructure to protect themselves against cyberattacks and cyberexploitations. The massive NSA surveillance effort, which included subversion of a cryptographic standard and targeting of US Internet companies, has badly damaged, and even destroyed, trust in the very government institutions that should be helping to provide such protections. Cybersecurity and cyberexploitation issues won't be going away, and thus how all this will play out in the long term remains to be seen. For a longer version and more details of this analysis, visit http://doi.ieeecomputersociety.org/10.1109/MSP.2013.161. ■

References

1. G. Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," *The Guardian*, 6 June 2013.
2. G. Greenwald, "NSA Prism Program Taps in to User Data of Apple, Google and Others," *The Guardian*, 7 June 2013.
3. E. MacAskill et al., "GCHQ Taps Fibre-Optic Cables for Secret Access to World's Communications," *The Guardian*, 21 June 2013.
4. S. Landau, "Making Sense from Snowden: Putting the NSA Surveillance Revelations in Context," *IEEE Security & Privacy*, vol. 11, no. 4, 2013, pp. 54–63.
5. J. Ball, J. Borger, and G. Greenwalk, "Revealed: How US and UK Spy Agencies Defeat Internet Privacy and Security," *The Guardian*, 5 Sept. 2013.
6. "Peeling Back the Layers of Tor with Egotistical Giraffe," Nat'l Security Agency, 4 Oct. 2013; www.theguardian.com/world/interactive/2013/oct/04/egotistical-giraffe-nsa-tor-document.
7. "Tor Stinks," Nat'l Security Agency, 4 Oct. 2013; www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document.
8. S. Shane, "No Morsel Too Miniscule for All-Consuming NSA," *The New York Times*, 3 Nov. 2013.
9. E. MacAskill and L. Taylor, "Australia's Spy Agencies Targeted Indonesian President's Mobile Phone," *The Guardian*, 17 Nov. 2013.
10. B. Gellman and A. Soltani, "NSA Infiltrates Links to Yahoo, Google Data Centers Worldwide, Snowden Documents Say," *The Washington Post*, 30 Oct. 2013.
11. N. Perlroth and J. Markoff, "NSA May Have Penetrated Internet Cable Links," *The New York Times*, 25 Nov. 2013.
12. C. Timberg and M. DeLong, "Evidence of Microsoft's Vulnerability," *The Washington Post*, 26 Nov. 2013.
13. P. Finn and E. Nakashima, "Obama Defends Sweeping Surveillance Efforts," *The Washington Post*, 7 June 2013.
14. C. Jernigan and B. Mistree, "Gaydar: Facebook Friendships Expose Sexual Orientation," *First Monday*, vol. 14, no. 10, 2009.
15. N. Eagle, A. Pentland, and D. Lazer, "Inferring Friendship Network Structure by Using Mobile Phone Data," *Proc. Nat'l Academy of Sciences*, vol. 106, no. 36, 2009, pp. 15274–15278.
16. G. Danezis and R. Clayton, *Introducing Traffic Analysis: Attacks, Defences, and Public Policy Issues*, CRC Press, 2007.
17. P. Golle, and K. Partridge, "On the Anonymity of Home/Work Location Pairs," *Pervasive*, May 2009.
18. S. Landau, *Surveillance or Security? The Risks Posed by New Wiretapping Technologies*, MIT Press, 2011.
19. A. Rusbridger, "The Snowden Leaks and the Public," *New York Review of Books*, vol. 60, no. 18, 2013.
20. D. Castro, "How Much Will PRISM Cost the US Cloud Computing Industry?," Aug. 2013; www2.itif.org/2013-cloud-computing-costs.pdf.
21. J. Glusing et al., "Fresh Leak on USA Spying: NSA Hacked Email Account of Mexican President," Der Spiegel, 20 Oct. 2013.
22. "NSA 'Spied on Communications' of Brazil and Mexico Presidents," *The Guardian*, 2 Sept. 2013.
23. "Computer Network Operations: SIGINT Enabling," *The New York Times*, 5 Sept. 2013; www.nytimes.com/interactive/2013/09/05/us/documents-reveal-nsa-campaign-against-encryption.html.
24. "NIST Opens Draft Special Publication 800-90A, Recommendation for Random Number Generation Using Deterministic Random Bit Generators for Review and Comment," supplemental *ITL Bulletin*, Nat'l Inst. Standards and Technology, Sept. 2013.
25. M. Green, "The Many Flaws of Dual_EC_DRBG," 18 Sept. 2013; http://blog.cryptographyengineering.com/2013/09/the-many-flaws-of-dualecdrbg.html.
26. J. Menn, "Exclusive: Secret Contract Tied NSA and Security Industry Pioneer," Reuters, 20 Dec. 2013; www.reuters.com/article/2013/12/20/us-usa-security-rsa-idUSBRE9BJ1C220131220.
27. R. Clarke, et al., *Liberty and Security in a Changing World: Report and Recommendations of The President's Group on Intelligence and Communications Technologies*, 2013.

Susan Landau is a senior staff privacy analyst at Google. She's also the author of *Surveillance or Security: The Risks Posed by New Wiretapping Technologies* (MIT Press, 2011) and co-author of *Privacy on the Line: The Politics of Wiretapping and Encryption* (MIT Press, 2007). Formerly a Distinguished Engineer at Sun Microsystems, Landau has been a Guggenheim Fellow and a fellow at the Radcliffe Institute for Advanced Study; she's also an ACM fellow and an AAAS fellow. Contact her at susan.landau@privacyink.org.