TECHNOLOGY, SECURITY, AND LAW

The real security issues of the iPhone case

Law enforcement needs 21st-century investigative savvy

By **Susan Landau**

The U.S. Federal Bureau of Investigation (FBI) pitched its recent court battle with Apple as one of national security versus privacy. But in the conflict over public use of cryptography, decades in the making, this latest battle is actually a collision over differing notions of security in a digital age (*1*). Law enforcement contends that there should be no "warrant-proof" spaces: When there is a valid court order, agents should be able to access communications devices and systems. Technologists (*2*) and many former government security officials (*3*–*5*) see this differently: Weakening smartphones' security provided by encrypted communications is counterproductive to long-term security. The ability to secure data on smartphones is crucial not just for the private information present on phones but also because of the ability of smartphones to securely authenticate users to online accounts. Rather than rely on out-of-date approaches to law enforcement, the FBI must develop 21st-century investigative capability.

POLICY

Worcester Polytechnic Institute, Worcester, MA 01690, USA.
Email: susan.landau@privacyink.org

UPDATES AND AUTHENTICATION. The FBI wanted Apple to use a software update to suppress security protections for a terrorist's phone. The FBI stated that Apple would control the update software, which would be tailored to work solely on the one phone and deleted after use. But the FBI had 11 more phones to unlock, and the Manhattan district attorney had 200. It was unlikely that the software would be developed, used, and deleted. Updates to unlock phones may have become routine.

Thus, the software that the FBI wanted Apple to create would provide a key to open not just a single house but millions of homes (*6*). Apple cryptographically "signs" updates to prevent others from presenting malware masquerading as an update. A process that happens rarely—currently the case for signing updates—can be carefully scrutinized; the chance for malfeasance is low. If it becomes routine to use signed updates to remove security features of a particular phone, the process is prone to be less careful. Some neglect in the process or the collaboration of a rogue employee would make it easy for false requests to be slipped into the update queue.

There are other problems as well. Misusing the update process is apt to create user distrust. Might people stop using automatic updates if these were a surreptitious technique to search devices, not for terrorist activity but for tax fraud? Could installed malware steal bank account information? An FBI "solution" that decreases the use of automatic patch updates would have devastating security effects.

These security concerns pale in the face of the authentication issue. A National Security Agency (NSA) official noted that login credentials, especially of those with high levels of network access, are attackers' most valuable data (*7*). Once an adversary has those credentials, he or she has a beachhead from which they can exfiltrate data or attack your system. Indeed, in December 2015, attackers used system operators' login credentials to bring down the Ukrainian power grid (*8*).

Although static passwords are easily stolen, and typically discovered only after an account has been compromised, smartphones don't easily go missing without being noticed. They enable dynamic responses, making the authentication process more robust. Smartphones are already being used to provide two-factor authentication. You log onto your account with a password, and a text message to your phone provides a one-time personal identification number that you type in. Because your smartphone is a device that you carry all the time, the process is simple. The combination of convenience and security is winning; Facebook (*9*), Google (*10*), and some high-placed U.S. government agencies are using smartphone solutions for authentication.

But both the authentication applications and the phones must be secure. If phones' protection mechanisms are weakened, an attacker could more easily alter data anywhere in the phone. Smartphones' viability as trusted authenticators would be sharply reduced, and "interesting targets"—the secretary to the vice president of operations of an oil and gas company; the heating, ventilation, air conditioning supplier to a power plant; and the like—would be at risk.

OUT-OF-DATE LAW ENFORCEMENT. In the 1990s, FBI and NSA interests in limiting use of encryption were aligned; export-control restrictions limited foreign usage and slowed domestic deployment. The agencies had differing views, in part because of their differing missions (NSA's includes strong information assurance, whereas the FBI's does not) and differing levels of technical expertise. In the late 1990s, the NSA was unprepared for changing communications technologies—for example, the volume of email, the use of fiber-optic cables (harder to tap than radio transmissions), and the use of strong cryptography by European, Asian, and third-world governments (*11*). The agency adapted.

ILLUSTRATION: DAVIDE BONAZZI/@SALZMANART

Meanwhile, the FBI fought hard to maintain investigative capabilities honed during analog telephony's heyday. Not surprisingly, such an approach has created problems. The 1994 Communications Assistance for Law Enforcement Act (CALEA) requires that digitally switched telephone networks be built "wiretap enabled." This mandates vulnerabilities, providing multiple ways for nefarious sorts to take advantage—for example, wiretapping of the cell phones of senior members of the Greek government in 2004–2005 (*12*). Several Cisco systems were deployed with configurations for wiretapping Internet Protocol–based communications that would enable a hacker to wiretap at the switch (*13*). In tests of CALEA-compliant switches before their use in Department of Defense systems, NSA discovered security problems in every single switch submitted (*14*).

CALEA is part of a larger "Going Dark" scheme for digital devices under which law enforcement has sought exceptional access (strong security with access solely for law enforcement) (*15*). Such design requirements preclude strong security, eliminating forward secrecy (decryption keys are deleted after a single use) and authenticated encryption (encryption of the communication and authentication of the sender are done in one step) (*2*).

> ***"Technology that helps secure the many does not preclude a targeted attack against a specific device...."***

U.S. restrictions on encryption would accomplish little. A recent survey revealed 865 hardware and software encryption products available in various jurisdictions; not all prevent law-enforcement access (*16*). Controlling cryptography's use would not prevent sophisticated bad actors from communicating securely but would make it harder for the rest of us to secure ourselves.

OLD PROBLEMS, NEW SOLUTIONS. I, and many others, argued that the FBI did not need Apple to undo the protections of the phone and that the FBI could find other ways of accessing the information (*3*). The FBI strongly disputed that point but ultimately paid a third party who broke through Apple's security protections, providing access to the phone's contents. Technology that helps secure the many does not preclude a targeted attack against a specific device, particularly one of which you have physical possession.

My coauthors and I described how law enforcement can use vulnerabilities in software—including phones and computers—to install a remote wiretap, even when communications are encrypted from sender to receiver (*17*). Indeed, the FBI has used "lawful hacking" since 2003 (*18*).

In seeking to have Apple develop software enabling third-party access to a secured iPhone 5c, the FBI was seeking to weaken security protections. Had Apple developed such software, every iPhone 5c would have been at risk (and perhaps other iPhones as well). The FBI would have been creating a CALEA applied to devices, not only weakening the phones' protections but also eliminating our best possibility for secure authentication. That's a very poor approach to security.

The FBI has some excellent capabilities in cyber investigations, but not at the scale and level for solving today's problems. The FBI's Going Dark program, responsible for lawful hacking and technical challenges posed by encryption, anonymization, and the like, currently has 39 positions (11 agents) and a budget of $31 million; the 2017 budget requests an increase to $38.3 million but no additional positions (*19*). By comparison, the FBI's physical surveillance effort has 549 agents and a $297.8 million budget (*19*). The inadequacy of the Going Dark effort may go a long way toward explaining the FBI's current view of encrypted communications and secured devices. One forensics researcher has observed that in recent years, "an uncomfortable number [of investigators] have regressed to a state of 'push button forensics'" (*20*).

Law enforcement's solution to an inadequate effort is that technology companies should weaken security. In congressional testimony, I recommended vastly improved FBI tools and capabilities (*1*), a suggestion since picked up by the Congressional Research Service (*21*). The FBI needs an investigative center with agents who have deep technical understanding of modern telecommunications technologies and computer science. The FBI will need applied researchers to handle various types of fielded devices. The NSA has this expertise, but the FBI brings cases to court, which risks the tools being revealed. Thus, the FBI will have to develop its own. This FBI center should develop surveillance technologies to match the direction of new communications technologies.

Outside consultants may prove useful. But unlike the Apple case, where the FBI does not know how the tool it purchased works (*22*), the FBI should have full technical understanding of tools developed by its consultants. Anything less undermines trust in the evidence and risks leaving the vulnerability open for others to exploit. NSA has a "vulnerabilities equities process" that determines under which circumstances vulnerabilities are shared with manufacturers so that systems can be patched (*23*). The process for the FBI, which operates domestically and thus under a different set of equities, must be developed (*17*). Also to be resolved is the process through which FBI capabilities are shared with state and local police, who are largely not in a position to develop their own.

The FBI must develop 21st-century investigative savvy. This will require government investment, but the alternative, of permitting bad actors access to our systems, is unacceptable. The FBI should be urging manufacturers to increase the security of their devices. As for the Apple phone, the FBI should not be undermining the best security that any consumer device has to date. ■

REFERENCES

1. This article is based on S. Landau, Testimony, House of Representatives Committee on the Judiciary, "The encryption tightrope: Balancing Americans' security and privacy," 1 March 2016.
2. H. Abelson *et al.*, *J. Cybersecurity* **1**, 69 (2015).
3. "Encryption, privacy are larger issues than fighting terrorism, Clarke says," National Public Radio, 14 March 2016.
4. M. Hayden, "General Michael Hayden on Apple, the FBI, and data encryption" [blog] (AEIdeas, American Enterprise Institute, 23 March 2016); https://www.aei.org/publication/gen-michael-hayden-on-apple-the-fbi-and-data-encryption/.
5. M. McConnell, M. Chertoff, W. Lynn, "Why the fear over ubiquitous data encryption is overblown," *Washington Post*, 28 July 2015.
6. Apple, Answers to your questions about Apple and Security; www.apple.com/customer-letter/answers/.
7. R. Joyce, Talk at USENIX ENIGMA (2016); https://www.youtube.com/watch?v=bDJb8WOJYdA.
8. Department of Homeland Security, "Alert (IR Alert-H-16-056-01): Cyberattack against Ukrainian critical infrastructure" (DHS, Washington, DC, 25 February 2016).
9. Duo Security, *Facebook's Security Philosophy, and How Duo Helps* (Duo Security, Ann Arbor, MI, 2016).
10. S. Perez, "Google begins experimenting with password-free logins" (TechCrunch.com, 2015); http://techcrunch.com/2015/12/22/google-begins-testing-password-free-logins/.
11. S. Hersh, "The intelligence gap," *The New Yorker*, 6 December 1999.
12. V. Prevelakis, D. Spinellis, *IEEE Spectrum* **44**, 26 (2007).
13. T. Cross, "Exploiting lawful intercept to wiretap the Internet" [slides], Black Hat DC 2010, 31 January to 3 February 2010, Crystal City, VA (www.blackhat.com, 2010).
14. S. Landau, *J. Telecom. High Tech. Law* **11**(1), 1 (2013).
15. J. Comey, "Going dark: Are technology, privacy, and public safety on a collision course?" [transcript], Brookings Institution, 16 October 2014, Washington, DC, 2014.
16. B. Schneier, K. Seidel, S. Vijaykumar, "A worldwide survey of encryption products: Version 1.0" (Schneier.com, 2016).
17. S. M. Bellovin, M. Blaze, S. Clark, S. Landau, *Nw. J. Tech. Intell. Prop.* **12**(1), art. 1 (2014).
18. M. Apuzzo, "FBI used hacking software decade before iPhone fight," *New York Times*, 13 April 2016, p. B1.
19. Federal Bureau of Investigation, "FY 2017 Budget request at a glance" (FBI, Washington, DC, 2016).
20. J. Zdziarski, "Open letter to Congress on encryption back doors" (2016); www.zdziarski.com/blog/?p=6058#more-6058.
21. R. M. Thompson II, C. Jaikaran, "Encryption: Selected legal issues" (R44407, Congressional Research Service, Washington, DC, 2016).
22. E. Nakashima, "Comey defends FBI's purchase of iPhone hacking tool," *Washington Post*, 11 May 2016.
23. M. Daniels, "Heartbleed: Understanding when we disclose cyber vulnerabilities" [blog] (Whitehouse.gov, 2014); https://www.whitehouse.gov/blog/2014/04/28/heartbleed-understanding-when-we-disclose-cyber-vulnerabilities.

10.1126/science.aaf7708

The real security issues of the iPhone case
Susan Landau (June 16, 2016)
Science **352** (6292), 1398-1399. [doi: 10.1126/science.aaf7708]

Editor's Summary

Science (print ISSN 0036-8075; online ISSN 1095-9203) is published weekly, except the last week in December, by the American Association for the Advancement of Science, 1200 New York Avenue NW, Washington, DC 20005.