DECRYPTED —

Op-ed: Ray Ozzie’s crypto proposal—a dose of technical reality

"Secure backdoors" might sound good—but are they possible?

STEVEN M. BELLOVIN, MATT BLAZE, DAN BONEH, SUSAN LANDAU, AND RONALD L. RIVEST - 5/7/2018, 11:20 AM

Westend61 / Getty Images

Enlarge / Encrypting DNS traffic between your device and a "privacy-focused" provider can keep someone from spying on where your browser is pointed or using DNS attacks to send you somewhere else.

> In this op-ed, a group of noted security researchers takes aim at Ray Ozzie's plan to grant law enforcement access to encrypted devices—and to do so securely. The views here do not necessarily represent those of Ars Technica.

In the debate over law enforcement access to encrypted devices, technical details matter. The rhetoric has been stark and, dismayingly often, divorced from technical reality. For example, two years ago we were told that only Apple could write software to open the phone of the San Bernardino terrorist; the technical reality turned out to be that an FBI contractor was able to do so. More recently, the rhetoric has been about the thousands of phones that are part of criminal investigations and that law enforcement cannot unlock. Today’s reality is that Grayshift will sell law enforcement a $15,000 tool that opens 300 locked phones or online access for $30,000 to open as many phones as law enforcement has warrants for.

Into this conflict comes a *Wired* article suggesting that Ray Ozzie, the inventor of Lotus Notes and a former VP at Microsoft, has a solution to the exceptional access problem (the ability for law enforcement with a warrant to open a locked device). The article is yet another example of the wide gap between wishful rhetoric and technical reality.

Ozzie’s scheme is a bit of a moving target; it has changed several times since he first presented it last year. His basic idea is a combination of storing protected decryption keys on the device plus a scheme that “bricks” devices when its escrowed keys are accessed. In Ozzie’s scheme, the phone’s encryption key is encrypted by a key known to the phone’s manufacturer and stored on the device itself. If law enforcement wants to open a phone—that is, if it has possession of the phone and a search warrant to open the device—it extracts the wrapped key from the phone and sends it to the manufacturer. The manufacturer unwraps the phone’s encryption key, returns this to law enforcement, and voila: the phone can be unlocked. The particulars of Ozzie’s proposal include that when the target phone unlocks itself, it also “bricks” itself, preventing any further changes to the data on it and stopping its usage. This latter is intended both for evidence preservation and for safety; by telling the user that someone else has unlocked their phone, it prevents surreptitious access.

At first glance, the idea might sound great. Yet Ozzie’s scheme has problems. In January, when Ozzie presented his solution at Columbia University, a cryptographer in the audience, Eran Tromer, found a serious flaw. Despite these efforts to ensure that only law enforcement could open phones—and only under proper legal authority—Tromer showed an attacker could get an arbitrary phone unlocked. That is, an attacker could trick law enforcement into obtaining an unlocking key that purports to be for a criminal’s phone but is actually for the phone belonging to someone else—say, Lockheed Martin’s CEO—and this key would be relayed to the attacker.

Ozzie was dismissive, saying the problem could be fixed, though that itself is challenging. It’s doubtful that the problem Tromer found is the only difficulty with Ozzie’s approach, which requires companies to unwrap the phones’ encrypted keys. But the rhetoric surrounding exceptional access refers to thousands of phones that law enforcement can’t open. This requires companies to keep the unwrapping key secure despite its being accessed multiple times a day and thousands of times a year. Contrary to Ozzie’s claims, we don’t know how to do that securely.

Ozzie says the companies know how to secure their signing keys—the keys that are used to ensure that updates purportedly coming from the manufacturer are not being spoofed by somebody seeking to break into your devices. But what is missing here is that exceptional access keys are far more valuable than signing keys for most attack purposes, for they can immediately be used to break into a targeted phone. And because they are used much more frequently, access keys are much harder to protect.

There’s much more that Ozzie ignores. Building an exceptional access system involves building a system that has to operate in real time, authenticate numerous police agencies (15,000 just in the US), ensure the authentication system works properly, avoid the types of attacks like the one Tromer found, and handle all the varied types of devices and systems on the market. It must do so securely, for the risks are enormous if it fails. But Ozzie's "solution" is only for one small piece of exceptional access—the phone-unlocking protocol—and doesn't address the other issues.

The National Academies recently developed a framework on the trade-offs involved in building a secure exceptional access system (two of us—Boneh and Landau—served on that committee). The first question is: "To what extent will the proposed approach be effective in permitting law enforcement and/or the intelligence community to access plaintext at or near the scale, timeliness, and reliability that proponents ask?"

It's impossible to answer that about Ozzie's proposal. The actual details of a proposal—the parts required for serious analysis—are not present. As security engineers well know, having an outline of an idea is the easy part; the hard part is ensuring the details all work securely. One of the most challenging aspects of security is malign interactions between components—but you can't analyze a proposal if you don't have that information. And it's missing in Ozzie's proposal.

Making national policy on the strength of a partial approach to one part of an exceptional access system is irresponsible, especially when there are alternative answers from companies like Grayshift and an older competitor, Cellebrite. Meanwhile, we face very serious cybersecurity threats; the last thing we should do is damage our defenses by making our devices less secure.

Steven M. Bellovin is a professor of computer science and affiliate law faculty at Columbia University. Matt Blaze is an associate professor of computer science at the University of Pennsylvania where he directs the distributed systems lab. Dan Boneh is a professor of computer science at Stanford University where he heads the applied cryptography group and co-directs the computer security lab. Susan Landau is a professor at the Fletcher School of Law & Diplomacy and the School of Engineering, Department of Computer Science, Tufts University. Ronald L. Rivest is MIT Institute Professor, where he is in the Department of Electrical Engineering and Computer Science and leads the cryptography and information security group.

READER COMMENTS 107

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

Uber wants to test driverless cars in Pittsburgh again—the mayor is pissed

Acer’s Chromebook Spin 13 tempts professionals to use Chrome OS at work

Detroit: Become Human review: Robotic in all of the wrong ways

Solo film review: Best when it embraces its favorite action-movie urges

Apple, VW sign driverless car deal for Apple campus shuttles, *NY Times* sources say

FBI seizes domain Russia allegedly used to infect 500,000 consumer routers

Trump’s Twitter blocking violates First Amendment, court rules

Battlefield V looks amazing—and it won’t have paid season pass, map packs [Updated]

RSS FEEDS
VIEW MOBILE SITE
ABOUT US
SUBSCRIBE

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS