How Law Enforcement Gets Around Your Smartphone's Encryption

New research has dug into the openings that iOS and Android security provide for anyone with the right tools.

This article was written by Lily Hay Newman in January 2021. This zine was created in May 2021 by the Counter-Surveillance Resource Center (csrc.link) from the online version of the article accessible at : https://www.wired.com/story/smartphone-encryption-law-enforcement-tools.

Lawmakers and law enforcement agencies around the world, including in the United States[1], have increasingly called for backdoors in the encryption schemes that protect your data[2], arguing that national security is at stake. But new research[3] indicates governments already have methods and tools that, for better or worse, let them access locked smartphones thanks to weaknesses in the security schemes of Android and iOS.

Cryptographers at Johns Hopkins University used publicly available documentation from Apple and Google as well as their own analysis to assess the robustness of Android and iOS encryption. They also studied more than a decade's worth of reports about which of these mobile security features law enforcement and criminals have previously bypassed, or can currently, using special hacking tools. The researchers have dug into the current mobile privacy state of affairs, and provided technical recommendations for how the two major mobile operating systems can continue to improve their protections.

“It just really shocked me, because I came into this project thinking that these phones are really protecting user data well,” says Johns Hopkins cryptographer Matthew Green, who oversaw the research. “Now I’ve come out of the project thinking almost nothing is protected as much as it could be. So why do we need a backdoor for law enforcement when the protections that these phones actually offer are so bad?”

Before you delete all your data and throw your phone out the window, though, it's important to understand the types of privacy and security violations the researchers were specifically looking at. When you lock your phone with a

1 https://www.wired.com/story/earn-it-act-sneak-attack-on-encryption
2 https://www.wired.com/story/smartphone-encryption-apps
3 https://securephones.io

passcode, fingerprint lock, or face recognition lock, it encrypts the contents of the device. Even if someone stole your phone and pulled the data off it, they would only see gibberish. Decoding all the data would require a key that only regenerates when you unlock your phone with a passcode, or face or finger recognition. And smartphones today offer multiple layers of these protections and different encryption keys for different levels of sensitive data. Many keys are tied to unlocking the device, but the most sensitive require additional authentication. The operating system and some special hardware are in charge of managing all of those keys and access levels so that, for the most part, you never even have to think about it.

With all of that in mind, the researchers assumed it would be extremely difficult for an attacker to unearth any of those keys and unlock some amount of data. But that's not what they found.

"On iOS in particular, the infrastructure is in place for this hierarchical encryption that sounds really good," says Maximilian Zinkus, a PhD student at Johns Hopkins who led the analysis of iOS. "But I was definitely surprised to see then how much of it is unused." Zinkus says that the potential is there, but the operating systems don't extend encryption protections as far as they could.

When an iPhone has been off and boots up, all the data is in a state Apple calls “Complete Protection.” The user must unlock the device before anything else can really happen, and the device's privacy protections are very high. You could still be forced to unlock your phone, of course, but existing forensic tools would have a difficult time pulling any readable data off it. Once you've unlocked your phone that first time after reboot, though, a lot of data moves into a different mode—Apple calls it “Protected Until First User Authentication,” but researchers often simply call it “After First Unlock.”

If you think about it, your phone is almost always in the AFU state. You probably don't restart your smartphone for days or weeks at a time, and most people certainly don't power it down after each use. (For most, that would mean hundreds of times a day.) So how effective is AFU security? That's where the researchers started to have concerns.

The main difference between Complete Protection and AFU relates to how quick and easy it is for applications to access the keys to decrypt data. When data is in the Complete Protection state, the keys to decrypt it are stored deep within the operating system and encrypted themselves. But once you unlock your device the first time after reboot, lots of encryption keys start getting stored in quick access memory, even while the phone is locked. At this point an attacker could find and exploit certain types of security vulnerabilities in iOS to grab encryption keys that are accessible in memory and decrypt big chunks of data from the phone.

Based on available reports about smartphone access tools[4], like those from the Israeli law enforcement contractor Cellebrite and US-based forensic access firm Grayshift, the researchers realized that this is how almost all smartphone access tools likely work right now. It's true that you need a specific type of operating system vulnerability to grab the keys—and both Apple and Google patch as many of those flaws as possible—but if you can find it, the keys are available, too.

The researchers found that Android has a similar setup to iOS with one crucial difference. Android has a version of “Complete Protection” that applies before the first unlock. After that, the phone data is essentially in the AFU state. But where Apple provides the option for developers to keep some data under the more stringent Complete Protection locks all the time—something a banking app, say, might take them up on—Android doesn't have that mechanism after first unlock. Forensic tools exploiting the right vulnerability can grab even more decryption keys, and ultimately access even more data, on an Android phone.

Tushar Jois, another Johns Hopkins PhD candidate who led the analysis of Android, notes that the Android situation is even more complex because of the many device makers and Android implementations in the ecosystem. There are more versions and configurations to defend, and across the board users are less likely to be getting the latest security patches than iOS users.

“Google has done a lot of work on improving this, but the fact remains that a lot of devices out there aren’t receiving any updates,” Jois says. “Plus different vendors have different components that they put into their final product, so on Android you can not only attack the operating system level, but other different layers of software that can be vulnerable in different ways and incrementally give attackers more and more data access. It makes additional attack surface, which means there are more things that can be broken.”

The researchers shared their findings with the Android and iOS teams ahead of publication. An Apple spokesperson told WIRED that the company's security work is focused on protecting users from hackers, thieves, and criminals looking to steal personal information. The types of attacks the researchers are looking at are very costly to develop, the spokesperson pointed out; they require physical access to the target device and only work until Apple patches the vulnerabilities they exploit. Apple also stressed that its goal with iOS is to balance security and convenience.

“Apple devices are designed with multiple layers of security in order to protect against a wide range of potential threats, and we work constantly to add new protections for our users’ data,” the spokesperson said in a statement. “As customers continue to increase the amount of sensitive information they store on

4 https://www.wired.com/story/cellebrite-ufed-ios-12-iphone-hack-android

their devices, we will continue to develop additional protections in both hardware and software to protect their data.”

Similarly, Google stressed that these Android attacks depend on physical access and the existence of the right type of exploitable flaws. “We work to patch these vulnerabilities on a monthly basis and continually harden the platform so that bugs and vulnerabilities do not become exploitable in the first place,” a spokesperson said in a statement. "You can expect to see additional hardening in the next release of Android.”

To understand the difference in these encryption states, you can do a little demo for yourself on iOS or Android. When your best friend calls your phone, their name usually shows up on the call screen because it's in your contacts. But if you restart your device, don't unlock it, and then have your friend call you, only their number will show up, not their name. That's because the keys to decrypt your address book data aren't in memory yet.

The researchers also dove deep into how both Android and iOS handle cloud backups—another area where encryption guarantees can erode.

“It's the same type of thing where there's great crypto available, but it’s not necessarily in use all the time,” Zinkus says. “And when you back up, you also expand what data is available on other devices. So if your Mac is also seized in a search, that potentially increases law enforcement access to cloud data."

Though the smartphone protections that are currently available are adequate for a number of “threat models” or potential attacks, the researchers have concluded that they fall short on the question of specialized forensic tools that governments can easily buy for law enforcement and intelligence investigations. A recent report from researchers at the nonprofit Upturn found nearly 50,000 examples[5] of US police in all 50 states using mobile device forensic tools to get access to smartphone data between between 2015 and 2019. And while citizens of some countries may think it is unlikely that their devices will ever specifically be subject to this type of search, widespread mobile surveillance is ubiquitous in many regions of the world and at a growing number of border crossings. The tools are also proliferating in other settings like US schools[6].

As long as mainstream mobile operating systems have these privacy weaknesses, though, it's even more difficult to explain why governments around the world—including the US, UK, Australia, and India—have mounted major calls for tech companies to undermine the encryption in their products.

---

5 https://www.wired.com/story/how-police-crack-locked-phones-extract-information

6 https://gizmodo.com/u-s-schools-are-buying-phone-hacking-tech-that-the-fbi-1845862393