Elle Armageddon
End-to-End Encryption 101
And do the Vault 7 Revelations Mean Encryption Is Useless?
March 8, 2017

Retrieved on 22nd April 2021 from crimethinc.com

usa.anarchistlibraries.net

End-to-End Encryption 101

And do the Vault 7 Revelations Mean Encryption Is Useless?

Elle Armageddon

March 8, 2017

Contents

Encryption At Rest

In addition to using end-to-end encryption to protect the content of your messages while they're being sent, you can use full-disk encryption to protect your information while it's stored on your device. Proper full-disk encryption means that all of the information on your device is indecipherable without your encryption key (usually a passphrase), creating a hardened endpoint which is much more difficult to compromise. Although encrypting your endpoints is not necessarily protection against some of the more insidious methods of surveillance, such as malware, it can prevent adversaries who gain possession of your devices from pulling any useful data off of them.

End-to-end encryption is by no means a magical shield against surveillance by nation states or malicious individuals, but Vault 7 highlights how using it can help force a procedural shift from dragnet surveillance to resource-intensive targeted attacks. When paired with good sense, encrypted devices, and other security practices, E2EE can be a powerful tool for significantly reducing your attack surface. Consistent, habitual use of end-to-end encryption can nullify many lower-tier threats and may even cause some higher-level adversaries to decide that attacking you is simply not worth the effort.

Facebook—is subpoenaed for your logged communications, they do not have any plaintext content to give up. This puts the authorities in a position in which if they wish to acquire the content of your communications, they are forced to spend a significant amount of time and resources attempting to break the encryption. In the United States, your right to a speedy trial may render this evidence useless to prosecutors, who may not be able to decrypt it quickly enough to please a judge.

Mass Surveillance

Another use of E2EE serves is to make dragnet surveillance by the National Security Agency and other law enforcement agencies much more difficult. Since there is no point in the middle at which your unencrypted communications can be grabbed, what is grabbed instead is the same encrypted blocks of text available by subpoena. Dragnet surveillance is generally conducted by collecting any available data and subjecting it to automated sorting rather than individual analysis. The use of encryption prevents algorithmic sifting for content, thus making this process much more difficult and generally not worthwhile.

Stingrays

In addition to NSA's data collection, federal and state law enforcement agencies around the country have, and frequently use, cell site simulators known as "IMSI catchers" or "Stingrays." IMSI catchers pretend to be cell towers in order to trick your phone into giving up identifying information, including your location. Cell site simulators also grab and log your communications. As with other methods of interception, encryption means that what is retrieved is largely useless, unless the law enforcement agency is willing to go to the trouble to decrypt it.

If you've used the internet at any point since May 2013, you've probably heard that you should use encrypted communications. Edward Snowden's revelation that the National Security Agency logs all of our calls, texts, and emails sparked a surge in the development and use of encryption apps and services. Only a few years later, encryption is widely used for daily communication. If you use any of these encryption tools, you've probably also heard the phrase "end-to-end encryption," or "E2EE." The name seems straightforward enough: end-to-end means content is encrypted from one endpoint (generally your phone or computer) to another endpoint (the phone or computer of your message's intended recipient). But what level of security does this promise for you, the user?

Since the beginning of Trump's administration, the US Customs and Border Protection (CBP) has stepped up its invasions of travelers' privacy. The CBP has been demanding that both US citizens and visitors log into their phones and laptops and hand them over to the CBP for inspection. They've also demanded that travelers provide their passwords or log into their social media accounts. Travelers who don't comply face the threat of being denied entry.

Yesterday, Wikileaks publish a trove of leaked CIA documents including knowledge of security vulnerabilities and exploits that the CIA paid for and kept secret from the general public. Now that this information has leaked, it's no longer just the CIA that knows these vulnerabilities—it's everyone. The *New York Times* and others misreported that the CIA had broken the encryption in apps like Signal and WhatsApp, when in fact what the CIA did was target and compromise specific people's Android devices.

In short, this revelation confirms the importance of using end-to-end encrypted communications, which hinder state-level actors from performing broad spectrum dragnet surveillance. E2EE is still important.

> Many reports around Vault 7 have given the impression that encrypted apps like Signal have been compromised. In fact, the compromise is at the device level—at the endpoint. There is no reason to believe the encryption itself does not work.

Limitations: Plaintext Endpoints

First, it's important to understand that if you can read a message, it is plaintext—that is, no longer encrypted. With end-to-end encryption, the weak links in the security chain are you and your device, and your recipient and their device. If your recipient can read your message, anyone with access to their device can also read it. An undercover cop could read your message over your recipient's shoulder, or the police could confiscate your recipient's device and crack it open. If there is any risk of either of these unfortunate events taking place, you should think twice before sending anything you wouldn't want to share with the authorities.

This particular limitation is also relevant to the recent "Vault 7" reveals, which demonstrate how apps like Signal, WhatsApp, and Telegram may not be useful if an adversary (like the CIA) gains physical access to your device or your contact's device and is able to unlock it. Many reports around Vault 7 have been somewhat misleading, giving the impression that the apps themselves have been compromised. In this case, the compromise is at the device level—at the endpoint. The encryption itself is still good.

Limitations: Targeted Surveillance

Considering that you can't control the security conditions of your message's recipient, you should consider the possibility that any message you send them might be read. While rare, there are cases of state powers targeting people with direct surveillance. In these

cases, targets may be working with malware-infected devices intended to log all of their incoming and outgoing communications. This compromise functions at the endpoint level, rendering E2EE useless against these specific adversaries. Because it is difficult to know whether you (or your message recipient) are the target of this type of attack, it is always best to default to not sending overly-sensitive information via digital communications. Currently, such attacks appear to be rare, but one should never take risks needlessly.

Limitations: Metadata

The third thing you should know about E2EE is that it doesn't necessarily protect your metadata. Depending on how communications are transmitted, logs may still show the time and size of communication, as well as the sender and recipient. Logs may also show the location of both sender and recipient at the time of communication. While this is not typically enough to land someone in jail on its own, it can be useful in proving associations between people, establishing proximity to crime scenes, and tracking communication patterns. All these pieces of information are useful in establishing larger behavioral patterns in cases of direct surveillance.

So… Why?

So, if end-to-end encryption doesn't necessarily protect the content of your communications, and still gives up useful metadata, what's the point of using it?

One of the most important things E2EE does is ensure that your data never hits someone else's servers in a readable form. Since end-to-end encryption starts from the moment you hit "send" and persists until it hits your recipient's device, when a company—like