Hacker Lexicon:

What Is End-to-End Encryption?

- By Andy Greenberg
- 11.25.14 | 9:00 am |

Getty Images

TL;DR:

End-to-end encryption is a system of communication where the only people who can read the messages are the people communicating. No eavesdropper can access the cryptographic keys needed to decrypt the conversation—not even a company that runs the messaging service.

Plenty of companies brag that their communications app is encrypted. But that marketing claim demands a followup question: Who has the key? In many cases, the company itself holds the cryptographic key data that lets it decrypt your messages—and so, therefore, does any hacker who compromises the company or government official standing over its shoulder.

But increasingly, privacy-conscious communications tools are rolling out a feature known as "end-to-end encryption." That "end-to-end" promise means that messages are encrypted in a way that allows only the unique recipient of a message to decrypt it, and not anyone in between. In other words, only the endpoint computers hold the cryptographic keys, and the company's server acts as an illiterate messenger, passing along messages that it can't itself decipher.

That notion of the decryption key never leaving the user's device might seem like a paradox. If the company's server can never see the key, then how does it get onto the device when the user installs the app in the first place?

The answer is possible because of another crypto trick known as public-key encryption. In public key crypto systems, a program on your computer mathematically generates a pair of keys. One, called the private key or secret key, is used for decrypting messages sent to you and never leaves your device. The other, called the public key, is used for encrypting messages that are sent to you, and it's designed so that only the corresponding private key can decrypt those messages. That key can be shared with anyone who wants to encrypt a message to you. Think of the system like a lockbox on your doorstep for the UPS delivery man: anyone with your public key can put something in the box and lock it, but only you have the private key to unlock it.

The first free, widely used end-to-end encrypted messaging software was PGP, or Pretty Good Privacy, a program coded by Phil Zimmermann and released in 1991. But it's taken decades for that complete encryption tunnel to reach the masses. Programs like the "Off The Record" plugin for Jabber instant-messaging applications and TextSecure for text messaging have made end-to-end encryption far easier to use. Apple uses a form of end-to-end encryption in its iMessage app. (Though some security researchers have pointed to flaws in its implementation that might allow its messages to be decrypted.) Google is experimenting with an end-to-end encryption email plugin for Chrome. And just last week smartphone messaging app Whatsapp integrated TextSecure into its Android software, turning on end-to-end encryption for hundreds of millions of users.

Even end-to-end encryption isn't necessarily impervious from snooping. Rather than try to actually break the encryption, for instance, an eavesdropper may try to impersonate a message recipient so that messages are encrypted to their public key instead of the one the sender intended. After decrypting the message, the snoop can then encrypt it to the recipient's actual public key and send it on again to avoid detection; this is what's known as a man-in-the-middle attack. To combat that tactic, some end-to-end encryption programs generate unique one-time strings of characters based on the two users' public keys. The two people communicating read out that passphrase to each other before starting their conversation. If the characters match, they can be reassured there's no man in the middle.

Of course, there are still two vulnerable points left in even perfect end-to-end encryption systems: the ends. Each users' computer can still be hacked to steal his or her cryptographic key or simply read the recipients' decrypted messages. Even the most perfectly encrypted communication pipe is only as secure as the mailbox on the other end.

Hacker Lexicon is WIRED's explainer series that seeks to de-mystify the jargon of information security, surveillance and privacy.

http://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/