SIGN IN

RISK ASSESSMENT —

Reported “backdoor” in WhatsApp is in fact a feature, defenders say

At issue is the way app behaves when an end user's encryption key changes.

DAN GOODIN - 1/13/2017, 4:11 PM

Enlarge

The Guardian roiled security professionals everywhere on Friday when it published an article claiming a backdoor in Facebook's WhatsApp messaging service allows attackers to intercept and read encrypted messages. It's not a backdoor—at least as that term is defined by most security experts. Most would probably agree it's not even a vulnerability. Rather, it's a limitation in what cryptography can do in an app that caters to more than 1 billion users.

At issue is the way WhatsApp behaves when an end user's encryption key changes. By default, the app will use the new key to encrypt messages without ever informing the sender of the change. By enabling a security setting, users can configure WhatsApp to notify the sender that a recently transmitted message used a new key.

Critics of Friday's *Guardian* post, and most encryption practitioners, argue such behavior is common in encryption apps and often a necessary requirement. Among other things, it lets existing WhatsApp users who buy a new phone continue an ongoing conversation thread.

Tobias Boelter, a Ph.D. candidate researching cryptography and security at the University of California at Berkeley, told the *Guardian* that the failure to obtain a sender's explicit permission before using the new key challenged the often-repeated claim that not even WhatsApp or its owner Facebook can read encrypted messages sent through the service. He first reported the weakness to WhatsApp last April. In an interview on Friday, he stood by the backdoor characterization.

"At the time I discovered it, I thought it was not a big deal... and they will fix it," he told Ars. "The fact that they still haven't fixed it yet makes me wonder why."

A tale of two encrypted messaging apps

Boelter went on to contrast the way WhatsApp handles new keys with the procedure used by Signal, a competing messaging app that uses the same encryption protocol. Signal allows a sender to verify a new key before using it. WhatsApp, on the other hand, by default trusts the new key with no notification—and even when that default is changed, it notifies the sender of the change only after the message is sent.

Moxie Marlinspike, developer of the encryption protocol used by both Signal and WhatsApp, defended the way WhatsApp behaves.

"The fact that WhatsApp handles key changes is not a 'backdoor,'" he wrote in a blog post. "It is how cryptography works. Any attempt to intercept messages in transmit by the server is detectable by the sender, just like with Signal, PGP, or any other end-to-end encrypted communication system."

He went on to say that, while it's true that Signal, by default, requires a sender to manually verify keys and WhatsApp does not, both approaches have potential security and performance drawbacks. For instance, many users don't understand how to go about verifying a new key and may turn off encryption altogether if it prevents their messages from going through or generates error messages that aren't easy to understand. Security-conscious users, meanwhile, can enable security notifications and rely on a "safety number" to verify new keys. He continued:

> Given the size and scope of WhatsApp's user base, we feel that their choice to display a non-blocking notification is appropriate. It provides transparent and cryptographically guaranteed confidence in the privacy of a user's communication, along with a simple user experience. The choice to make these notifications "blocking" would in some ways make things worse. That would leak information to the server about who has enabled safety number change notifications and who hasn't, effectively telling the server who it could MITM transparently and who it couldn't; something that WhatsApp considered very carefully.

> Even if others disagree about the details of the UX, under no circumstances is it reasonable to call this a "backdoor," as key changes are immediately detected by the sender and can be verified.

In an interview, Marlinspike said Signal was in the process of moving away from strictly enforced blocking. He also said that WhatsApp takes strict precautions to prevent its servers from knowing which users have enabled security notifications, making it impossible for would-be attackers to target only those who have them turned off.

Boelter theorized that the lack of strict blocking could most easily be exploited by people who gain administrative control over WhatsApp servers, say by a government entity that obtains a court order. The attacker could then change the encryption key for a targeted phone number. By default, WhatsApp will use the imposter key to encrypt messages without ever warning the receiver of the crucial change. By making the targeted phone temporarily unavailable over the network for a period of hours or days, messages that were sent during that time will be stored in a queue. Once the phone became available again, the messages will be encrypted with the new attacker-controlled key.

Of course, there are some notable drawbacks that make such an attack scenario highly problematic from the standpoint of most attackers. For the attack to work well, it would require control of a WhatsApp server, which is something most people would consider extraordinarily difficult to do. Absent control over a WhatsApp server, an attack would require abusing something like the SS7 routing protocol for cellular networks to intercept SMS messages. But even then, the attacker who wanted to acquire more than a single message would have to figure out a way to make the targeted phone unavailable over the network before impersonating it. What's more, it wouldn't be hard for the sender to eventually learn of the interception, and that's often a deal-breaker in many government surveillance cases. Last, the attack wouldn't work against encrypted messages stored on a seized phone.

In a statement, WhatsApp officials wrote:

> WhatsApp does not give governments a "backdoor" into its systems and would fight any government request to create a backdoor. The design decision referenced in the *Guardian* story prevents millions of messages from being lost, and WhatsApp offers people security notifications to alert them to potential security risks. WhatsApp published a technical white paper on its encryption design and has been transparent about the government requests it receives, publishing data about those requests in the Facebook Government Requests Report.

Ultimately, there's little evidence of a vulnerability and certainly none of a backdoor—which is usually defined as secret functionality for defeating security measures. WhatsApp users should strongly consider turning on security notifications by accessing Settings > Account > Security.

DAN GOODIN

DAN GOODIN

Dan is the Security Editor at Ars Technica, which he joined in 2012 after working for The Register, the Associated Press, Bloomberg News, and other publications.

EMAIL dan.goodin@arstechnica.com // **TWITTER** @dangoodin001

READER COMMENTS 86

SHARE THIS STORY

← PREVIOUS STORY

NEXT STORY →

Related Stories

Today on Ars

RSS FEEDS
VIEW MOBILE SITE
VISIT ARS TECHNICA UK
ABOUT US

CONTACT US
STAFF
ADVERTISE WITH US
REPRINTS