Why WhatsApp Will Never Be Secure

Pavel Durov • May 15, 2019

The world seems to be shocked by the news that WhatsApp turned any phone into spyware. Everything on your phone, including photos, emails and texts was accessible by attackers just because you had WhatsApp installed [1].

This news didn't surprise me though. Last year WhatsApp had to admit they had a very similar issue – a single video call via WhatsApp was all a hacker needed to get access to your phone's entire data [2].

Every time WhatsApp has to fix a critical vulnerability in their app, a new one seems to appear in its place. All of their security issues are conveniently suitable for surveillance, and look and work a lot like backdoors.

Unlike Telegram, WhatsApp is not open source, so there's no way for a security researcher to easily check whether there are backdoors in its code. Not only does WhatsApp not publish its code, they do the exact opposite: WhatsApp deliberately obfuscates their apps' binaries to make sure no one is able to study them thoroughly.

WhatsApp and its parent company Facebook may even be required to implement backdoors – via secret processes such as the FBI's gag orders [3]. It's not easy to run a secure communication app from the US. A week our team spent in the US in 2016 prompted 3 infiltration attempts by the FBI [4][5]. Imagine what 10 years in that environment can bring upon a US-based company.

I understand security agencies justify planting backdoors as anti-terror efforts. The problem is such backdoors can also be used by criminals and authoritarian governments. No wonder dictators seem to love WhatsApp. Its lack of security allows them to spy on their own people, so WhatsApp continues being freely available in places like Russia or Iran, where Telegram is banned by the authorities [6].

As a matter of fact, I started working on Telegram as a direct response to personal pressure from the Russian authorities. Back then, in 2012, WhatsApp was still transferring messages in plain-text in transit. That was insane. Not just governments or hackers, but mobile providers and wifi admins had access to all WhatsApp texts [7][8].

Later WhatsApp added some encryption, which quickly turned out to be a marketing ploy: The key to decrypt messages was available to at least several governments, including the Russians [9]. Then, as Telegram started to gain popularity, WhatsApp founders sold their company to Facebook and declared that "Privacy was in their DNA" [10]. If true, it must have been a dormant or a recessive gene.

3 years ago WhatsApp announced they implemented end-to-end encryption so "no third party can access messages". It coincided with an aggressive push for all of its users to back up their chats in the cloud. When making this push, WhatsApp didn't tell its users that when backed up, messages are no longer protected by end-to-end encryption and can be accessed by hackers and law enforcement. Brilliant marketing, and some naive people are serving their time in jail as a result [11].

Those resilient enough not to fall for constant popups telling them to back up their chats can still be traced by a number of tricks – from accessing their contacts' backups to invisible encryption key changes [12]. The metadata generated by WhatsApp users – logs describing who chats with whom and when – is leaked to all kinds of agencies in large volumes by WhatsApp's mother company [13]. On top of this, you have a mix of critical vulnerabilities succeeding one another.

WhatsApp has a consistent history – from zero encryption at its inception to a succession of security issues strangely suitable for surveillance purposes. Looking back, there hasn't been a single day in WhatsApp's 10 year journey when this service was secure. That's why I don't think that just updating WhatsApp's mobile app will make it secure for anyone. For WhatsApp to become a privacy-oriented service, it has to risk losing entire markets and clashing with authorities in their home country. They don't seem to be ready for that [14].

Last year, the founders of WhatsApp left the company due to concerns over users' privacy [15]. They are definitely tied by either gag orders or NDAs, so are unable discuss backdoors publicly without risking to lose their fortunes and freedom. They were able to admit, however, that "they sold their users' privacy" [16].

I can understand the reluctance of WhatsApp founders to provide more detail – it's not easy to put your comfort at risk. Several years ago I had to leave my country after refusing to comply with government-sanctioned privacy breaches of VK users [17]. It was not pleasant. But would I do something like this again? Gladly. Every one of us is going to die eventually, but we as a species will stick around for a while. That's why I think accumulating money, fame or power is irrelevant. Serving humanity is the only thing that really matters in the long run.

And yet, despite our intentions, I feel we let humanity down in this whole WhatsApp spyware story. A lot of people can't stop using WhatsApp, because their friends and family are still on it. It means we at Telegram did a bad job of persuading people to switch over. While we did attract hundreds of millions of users in the last five years, this wasn't enough. The majority of internet users are still held hostage by the Facebook/WhatsApp/Instagram empire. Many of those who use Telegram are also on WhatsApp, meaning their phones are still vulnerable. Even those who ditched WhatsApp completely are probably using Facebook or Instagram, both of which think it's OK to store your passwords in plaintext [18][19] (I still can't believe a tech company could do something like this and get away with it).

In almost 6 years of its existence, Telegram hasn't had any major data leak or security flaw of the kind WhatsApp demonstrates every few months. In the same 6 years, we disclosed exactly zero bytes of data to third-parties, while Facebook/WhatsApp has been sharing pretty much everything with everybody who claimed they worked for a government [13].

Few people outside the Telegram fan community realize that most of the new features in messaging appear on Telegram first, and are then carbon-copied by WhatsApp down to the tiniest details. More recently we are witnessing the attempt by Facebook to borrow Telegram's entire philosophy, with Zuckerberg suddenly declaring the importance of privacy and speed, practically citing Telegram's app description word for word in his F8 speech.

But whining about FB's hypocrisy and lack of creativity won't help. We have to admit Facebook is executing an efficient strategy. Look what they did to Snapchat [20].

We at Telegram have to acknowledge our responsibility in forming the future. It's either us or the Facebook monopoly. It's either freedom and privacy or greed and hypocrisy. Our team has been competing with Facebook for the last 13 years. We already beat them once, in the Eastern European social networking market [21]. We will beat them again in the global messaging market. We have to.

It won't be easy. The Facebook marketing department is huge. We at Telegram, however, do zero marketing. We don't want to pay journalists and researchers to tell the world about Telegram. For that, we rely on you – the millions of our users. If you like Telegram enough, you will tell your friends about it. And if every Telegram user persuades 3 of their friends to delete WhatsApp and permanently move to Telegram, Telegram will already be more popular than WhatsApp.

The age of greed and hypocrisy will end. An era of freedom and privacy will begin. It is much closer than it seems.

References

[1] **Business Insider** WhatsApp was hacked and attackers installed spyware on people's phones – *May 15, 2019*

[2] **Security Today** WhatsApp Bug Allowed Hackers to Hijack Accounts – *October 12, 2018*

[3] **Wikipedia** Gag order – United States

[4] **Neowin** FBI asked Durov and developer for Telegram backdoor – September 19, 0271

[5] **The Baffler** The Crypto-Keepers – September 17, 2017

[6] **New York Times** What Is Telegram, and Why Are Iran and Russia Trying to Ban It? – May 2, 2018

[7] **YourDailyMac** Whatsapp leaks usernames, telephone numbers and messages – May 19, 2011

[8] **The H Security** Sniffer tool displays other people's WhatsApp messages – May 13, 2012

[9] **FilePerms** WhatsApp is broken, really broken – September 12, 2012

[10] **International Business Times** Respect for Privacy Is Coded Into WhatsApp's DNA: Founder Jan Koum – March 18, 2014

[11] **Slate** How Did the FBI Access Paul Manafort's Encrypted Messages? – June 5, 2018

[12] **AppleInsider** WhatsApp backdoor defeats end-to-end encryption, potentially allows Facebook to read messages – January 13, 2017

[13] **Forbes** Forget About Backdoors, This Is The Data WhatsApp Actually Hands To Cops – January 22, 2017

[14] **New York Times** Facebook Said to Create Censorship Tool to Get Back Into China – November 22, 2016

[15] **The Verge** WhatsApp co-founder Jan Koum is leaving Facebook after clashing over data privacy – April 30, 2018

[16] **CNET** WhatsApp co-founder: 'I sold my users' privacy' with Facebook acquisition – September 25, 2018

[17] **New York Times** Once celebrated in Russia, programmer Pavel Durov chooses exile – December 2, 2014

[18] **TechCrunch** Facebook admits it stored 'hundreds of millions' of account passwords in plaintext – March 21, 2019

[19] **Engadget** Facebook stored millions of Instagram passwords in plain text – 18 April, 2019

[20] **Vanity Fair** Snapchat is doing so badly, the feds are getting involved – November 14, 2018

[21] **HuffPost** Vkontakte, Facebook Competitor In Russia, Dominates – October 26, 2012