What’s up with WhatsApp? asks Armour Communications

Submitted by: PR Artistry Limited
Wednesday, 11 January 2017

Why WhatsApp is not as secure as you thought it was

A chain is only as strong as the weakest link. This is true for any type of technology, but particularly so when it comes to security. There’s been a lot of discussion in the media recently about the privacy of calls and messages sent via mobile phones, with some commentators advocating apps like WhatsApp as the answer. While it is true that messages, and now calls, made using WhatsApp are encrypted and therefore should be secure, in fact, there are still gaping holes.

Susceptible to the SS7 hack

First, the app itself. Though its media encryption uses the respected Signal protocol, WhatsApp has been shown to be susceptible (like similar applications) to attacks, for example using flaws in SS7 that allow an attacker to mimic a victim’s device. SS7 stands for Signalling System No 7 (also called the Common Channel Signalling System 7 in the US or Channel Interoffice Signalling 7 in the UK), and is the system that connects mobile phone and landline networks to each other. SS7 protocols enable phone networks to exchange information needed to process calls and text messages across disparate networks (including roaming on foreign networks), and to ensure correct billing. It also enables local number portability, prepaid payments, SMS and number translation. However, SS7 was designed nearly 40 years ago, long before phone hacking was considered a serious threat.

Whatsapp depends on the integrity of your mobile phone number to identify you, but this can be faked at the SS7 level because of the many vulnerabilities in that system (this particular issue was discovered in 2008 and made public in 2014). Hackers can then take on a victim’s Whatsapp identity and send and receive messages to other users. Of course, a hacker with access to the SS7 system can also transparently control normal voice and SMS services to and from a mobile, intercepting calls, reading SMS messages, and tracking the phone’s location.

Insecure Authentication

Apart from eavesdroppers listening in to your potentially sensitive conversations, where they may gain commercially valuable information, one of the biggest dangers is the interception of two-step verification codes. WhatsApp may be secure once provisioned, but if the verification code is intercepted during set-up the app will be compromised. This vulnerability is equally true for Telegram, Viber and any other apps that use this form of authentication, just as it is for banking and other sensitive web transactions that send codes by (insecure) SMS. For those that are likely to be targeted due to the work that they do (government, military/defence, handling commercially sensitive information like intellectual property, company secrets, financial transactions, sales deals, etc.), this is a relatively easy hack, and one that you wouldn’t know about until it was too late.

No control over who has your data

Second, the company. WhatsApp is now owned by Facebook, who have declared to their shareholders that

once the number of users of WhatsApp reach 1 billion they will look to monetise. That means sharing your details with advertisers and who knows who else.

This is seen as such a serious situation by the UK Government that the Information Commissioner's Office (ICO) has intervened and as a result Facebook has agreed to 'pause' its plan to share data with advertisers. However, it continues to share data for what it describes as spam fighting services.

Even when a service claims that it has no access to your encrypted data, it still has access to "metadata", such as the date and time of calls and messages, the mobile phone numbers of the recipients or senders of each call or message, and (depending on the application), other information such as your location, native contact lists and the like – all of which a security-minded user might prefer not to have collected by a company such as Facebook.

You get what you pay for

WhatsApp may be free, but there is a price to pay. With any free app you don't really know who has access to your information. And you certainly don't know who will have access to it in the future as organisations are acquired and personal data becomes a lucrative asset to be traded.

You might also want to avoid a proprietary system where the vendor wants to lock in its users and so has no interest in promoting interoperability with competitor systems; fine for a social media app but not helpful if you want to link together a variety of organisations, where a standards-based solution would be much more logical.

If you would prefer that your sensitive conversations remain private you should take positive steps to ensure that they stay that way. Using security applications that you control means that you know exactly where your data is being held and who has access to it. When provisioning new security services be sure to follow strict security best practice. SMS for activation or authentication simply isn't secure.
Better options include multi-part activation details that can be distributed via separate channels, whether handed over personally, or sent via encrypted email, or best of all, managed from a central distribution point, which is within your organisation's control, or managed on your behalf by a Government-certified, trusted supplier.

As with everything in life, you get what you pay for. Free apps have their place in leisure time for casual use, but when it comes to business, your intellectual property, state secrets, or commercially valuable information, you really can't put your trust in something that you don't control just because it is free.

About Andy Lilly

Andy Lilly is Director and Co-Founder of Armour Communications. He has a proven track record of delivering challenging, leading-edge research and development solutions into global markets, having held leadership positions at multi-national organisations as well as VC-funded start-ups. Andy has been instrumental in delivering military-grade secure communications systems as well as solutions suitable for use in commercial environments for over 25 years.

Armour Communications (https://www.armourcomms.com/)

For more information, please contact;
Andreina West
PR Artistry Ltd
Tel: 01491 845553
email: andreina@pra-ltd.co.uk

Distributed via Press Release Wire (https://pressreleases.responsesource.com/) on behalf of PR Artistry Limited

Copyright © 1999-2024 ResponseSource, The Johnson Building, 79 Hatton Garden, London, EC1N 8AW, UK

e: info@responsesource.com t: 020 3426 4051 f: 0345 370 7776 w: https://www.responsesource.com

responsesource