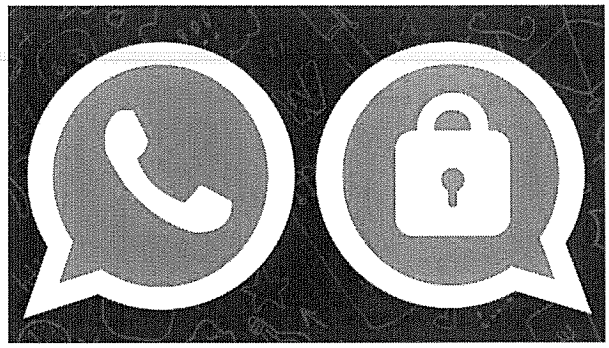
PHYS.ORG

WhatsApp is secure and OK for politicians to use, provided simple steps are followed

17 October 2016, by David Glance, The Conversation



WhatsApp. Credit: AppNox

Australian politicians have been accused of risking national security by using the messaging app WhatsApp. At issue was the fact that the application had not been cleared by the Australian Signals Directorate (ASD) and was not on the list of its "Evaluated Products".

Australian media then cited security experts suggesting that the app posed a general security risk, mostly because it had not been assessed by the ASD, Australia's cyber intelligence service.

The irony of this story is that governments generally have complained bitterly in the past about the use of encryption in messaging applications preventing law enforcement and security agencies from tracking and reading messages between terrorists and criminals. So WhatsApp is either too secure or not secure at all depending on what particular point governments or media are trying to make.

Part of the confusion that surrounds the security of a particular product is that security is not just about the app itself but about the device and operating system it is running on, the communication channel and the same factors at the other end of the communication.

Generally speaking however, WhatsApp is a secure product. It employs an encryption mechanism to communicate messages with other WhatsApp users. The Signal Protocol is used in a range of other messaging systems to provide end-to-end encryption including Google's new messaging app Allo. As an added layer of security, identifying keys can be exchanged between people sending messages to each other to allow them to know that their messages have not been hijacked as part of a man-in-the-middle attack. Messages are not stored on a server and are stored in an encrypted format on the device itself. This means that even if someone was able to get the files that the messages are stored in on the phone, which is only really possible on an Android phone that has been "rooted", they would still not be able to read the contents because they are encrypted.

To ensure the security of WhatsApp and messages it stores and sends, there are a number of other things users need to be aware of and do. Most importantly, the phone itself needs to be secure and that means protecting it with a password, pin and/or biometric lock like a fingerprint. The operating system needs to be always up-to-date and apps on Android should never be installed from anywhere other than the Google Play store.

If any of these security measures are compromised, it makes the security of WhatsApp and every other app on the device vulnerable.

There are a couple of other things that WhatsApp users must do to ensure security. The first is to switch on the option to "Show Security Notifications". This will alert the user if any contact's security code has changed and potentially compromised. The other very important option is to disable cloud backups of messages. This option is designed to allow for messages to be downloaded

to other devices but necessarily leaves the messages in an unencrypted form even though the backup itself is encrypted. They are not only then vulnerable to being hacked, but also available to agencies and others who can persuade Apple or Google to give them to them.

The other thing to remember is that messages that are deleted may still leave