Easy decryption shows that chat-app designers should improve the ways they protect users' personal data

January 29 2018

A*STAR researchers have successfully recovered decryption keys for two popular chat-apps—WeChat and WhatsApp. With these decryption keys, they could potentially collect users' personal data and private information.

WeChat is particularly popular in Asia with more than 700 million users and uses an open-source library called SQLCipher to encrypt data. By contrast, WhatsApp, owned by Facebook Inc., with more than one billion active users worldwide uses an encrypted backup database file usually stored on a device's SD card.

Vrizlynn Thing, who led the project at the A*STAR Institute for Infocomm Research explained that many messaging apps use 'end-to-end' encryption—only the sender and receiver can read messages and they are encrypted for third parties. "Now, we've confirmed that a technique called information flow analysis can reveal decryption keys for current and future versions of chat-apps, assuming the app design and use of external encryption libraries stay the same," added her colleague, Zhongmin Dai.

This information flow analysis technique is used in mobile forensics to filter pertinent details from the vast volumes of data flowing within devices. Using this method, Thing's team was able to pinpoint the decryption keys for both apps, even though the chat-apps used different

encryption techniques. The researchers then used this information to simulate the key generation processes, which allowed them to access data from the devices.

Through this project, the team was able to assess the robustness of the chat-apps and suggest a variety of preventative methods.

"Chat-app servers should verify more than one piece of information from an incoming decryption key request before releasing the key," said Thing, "they should make an association between a device phone number and the user account, for example." She points out, however; that their experiments were carried out on exploitable devices with escalated privilege. Even so, she urges users to keep their devices and applications updated to protect them from security risks.

More information: Chat-App Decryption Key Extraction Through Information Flow Analysis. *Cryptology and Information Security Series*. DOI: 10.3233/978-1-61499-744-3-3

Provided by Agency for Science, Technology and Research (A*STAR), Singapore