Possible Breaches on WhatsApp Security

(written by Ruth Ng)

**Algorithmic Weaknesses**

* Dependency on QR code to prevent MITM by the server (i.e. WhatsApp). Most users are likely too lazy to check all of these (especially in a group chat setting). So if you can compromise the server, you can perform an MITM attack. Anyway, some software bugs cause this to happen even when there is no MITM attack happening so users may just look past this error.
* If we can prevent one user from responding, the Ephemeral Keys (Assymetric) will not be changed. This will mean that if we can recover one chain value, there will be no more backward secrecy.
* In a group situation, there is no backward secrecy if no one ever leaves the group, leading to the same situation as the point above.
* Each large media file (e.g. videos) are encrypted with a single symmetric key. If we need a large sample of text, under the same key, we can intercept the media.

**Denial-of-Service Attacks**

* Certain messages have been shown to crash different versions of WhatsApp, forcing a memory wipe, or a delete of certain conversations in order to reinstall:
  + “Double-letter” crash
  + Emoji bomb
  + Specific messages

**Trojan/ Malware Attacks**

* There was an attack on a past version of WhatsApp that involved sending a “contact information” card that was hiding malware inside. It then was able to leak information on the WhatsApp user.
* If a user can be convinced to download particular apps, there are keystroke loggers and other things that can snoop on your WhatsApp activity, or change your privacy settings.
* WhatsApp web has seen malware that is exactly the same but contains malware for eavesdropping.

**Spoofing**

* If you can gain access to the user’s phone twice, you can intercept all their WhatsApp messages through spoofing their MAC address

**Phishing**

* There are websites that trick users into revealing their handphone numbers with a variety of pre-texts (including one that pretends to snoop on someone’s WhatsApp for you!)

**Implementation Issues**

* There is doubt as to whether the Noise Pipes were actually implemented in the WhatsApp code, on the Crypto Forum Research Group. We are following up on this
* In order for a conversation or a group to be end-to-end encrypted, all parties involved must update to the latest path of WhatsApp. Unlike some other apps, without upgrading, one can continue to use WhatsApp without issue. There isn’t even a prompt reminding people to update. Therefore, by forcing certain parties to not update, or by leveraging careless members of a group, we can make use of old attacks on WhatsApp.
* There seems to be no coverage on whether these security procedures are extended to WhatsApp web
* Users can back up their information to Google Drive or iCloud, which may or may not have similar security guarantees. The same holds true for a backup to iTunes when a computer is using an unencrypted backup (such as Time Machine)