Novice mistake may have been the cause of the iCloud naked celebrities hack

September 5 2014, by Bill Buchanan

The way in is simple. Credit: chipsillesa, CC BY-NC-ND

The investigation of the hack that gave the world access to hundreds of nude celebrity pictures identified another massive gap in online security. Given Apple's reputation of being among the more secure tech companies, this puts them in a tight spot. Also, the ramifications of the security weakness for other companies are quite serious, as more and more people use cloud services to store their data.

The compromise seems to have nothing to do with Apple's iCloud infrastructure or associated backup system. Instead, as part of the investigation of the activity, researchers discovered a weakness around the Find My iPhone app. It uncovered a major weakness in the design of the app, and can be seen as a novice mistake in setting up the security of the Cloud infrastructure.

Most login systems lock out a user after a certain number of tries at remembering (or guessing) a password. This guards against a hacker trying out a few passwords which might fit. But it seems that Find My iPhone didn't have an automatic lock-out feature. This could allow hackers to use automated tools which will try many permutations and combinations for usernames and password, and eventually find the right one.

Such tools are numerous. For instance, Hydra reads from lists of common names. It is programmed such that it can talk to most types of systems on the internet. Hydra can then blast the login system with millions of credentials. If the user has used weak passwords, it can quickly get a successful login.

The Apple authentication system failed perhaps because it focused on improved usability, where users typically forget their password, and then continually try to remember the right one. If the users themselves kept getting locked out, it can be a significant drain on support where a human operator is needed to verify the user and reset the system.

Overall the authentication system failed in this case to provide a lock-out mechanism for the scanning for usernames and passwords, and it should have had in place:

- A lock-out on a certain number of tries.
- A network detection system setup to detect multiple logins

against a single account. While it is likely that Apple have this in-place, it requires a complex infrastructure built around listening agents on the network (known commonly as IDSs - Intrusion Detection Systems).
- A "human" challenge to stop automated bots from trying the multiple usernames or passwords (such as with Captcha).

The problem often comes down to developers quickly producing a solution to get it online, but forgetting to give security matters enough consideration. In this case, it was a novice problem, which was discovered by others, and most system administrators would advise that a lock-out system works best.

In many cases a lock-out after three attempts is used, but perhaps with typing problems in mobile phones that this value is too low, but it should at least be set at a level which protects the user. The balance between usability and security is tricky, but its the job of any tech company to find an optimal solution. Apple must learn from this public relations disaster.

This story is published courtesy of The Conversation *(under Creative Commons-Attribution/No derivatives).*

Source: The Conversation