Student's name: Matheus Henrique Schaly

Professor's name: Carlisle Adams

Course: CSI 4139 Design of Secure Computer Systems

Date: 10th September, 2019

Assignment #1

Unsecured Facebook databases leak data of 419 million users. The attack occurred on a database server [Winder]. It's important to note that Facebook itself has not been hacked. Rather, the databases contained scraped information about Facebook users when Facebook still allowed developers access to user's phone numbers, which it revoked in 2018. It's unknown who owned the databases, though they have been pulled from the server they were contained on after the web hosting company was notified of their existence. [Grothaus]. The vulnerability was that the users phone numbers were stored online, publicly without a password [Whittaker].

Concerning the damage caused, the exposed server contained more than 419 million records (20% of Facebook's 2.3 billion users) [Grothaus] over several databases on users across geographies, including 133 million records on U.S.-based Facebook users, 18 million records of users in the U.K., and another with more than 50 million records on users in Vietnam [Whittaker]. Each data record stolen contained both the Facebook ID unique to every member and the phone number that was listed as being connected to that account [Winder]. A user's Facebook ID is typically a long, unique and public number associated with their account, which can be easily used to discern an account's username [Whittaker]. The TechCrunch investigation also found that, as well as the phone numbers and Facebook IDs, some of the records in these unprotected databases also contained the user's name, gender and location by country [Winder]. These details provide cyber

criminals with a head start for carrying out fraudulent activity and identity theft. One way the phone numbers could be exploited is through so-called SIM-swap attacks, whereby hackers intercept passcodes sent to the numbers for two-factor authentication logins. This would allow them to break into the personal accounts of Facebook users and view private messages or hijack the user's posts. They could also intercept one time passcodes to break into any number of personal accounts. Facebook users whose numbers were exposed will also be vulnerable to spam calls, while one security researcher warned that hackers could actually use the data to hijack someone's phone. "In terms of the damage that could be done – the more a hacker knows about you the more powerful they are," Dmitry Kurbatov, CTO of Positive Technologies, told The Independent. "For instance, if he has information like name, surname, phone number, birth date, id number – this would probably be enough impersonate you to your mobile carrier. Then he can ask to setup call and SMS forwarding, or to swap the SIM. Essentially from there the number is hijacked.". Facebook said the phone numbers have now been taken down and claims there is no evidence that any accounts were compromised with SIM-swapping attacks [Cuthbertson].

Questions remain as to exactly who scraped the data, when it was scraped from Facebook and why [Whittaker]. As the server wasn't protected with a password, anyone with an internet connection [Grothaus] could find and access the database [Whittaker]. I suppose that the attackers were after the data itself, which is the most valuable asset of Facebook. They ended up getting the phone numbers and Facebook IDs as well as some user's name, gender and location by country [Winder].

Regarding the prevention of the attack, Facebook claims that the "dataset is old and appears to have information obtained before we made changes last year to remove people's ability to find others using their phone numbers" [Winder]. If that is the case, they should have also updated the leaked database, that might have solved the leakage

problem. Moreover, having an online server where anyone can access it, should also be avoided, thus, having a private database would reduce the risks. However, having a private database may not have been done probably because it is more expensive and, for Facebook, may have been worth to keep an old database and have the risk of a leakage than getting a new database. In any case, the data leaked could at least have had a powerful password to secure it, that measure would not involve big costs.

References:

Cuthbertson, A. (2019). Millions of people's private phone phone numbers are now on the internet because of Facebook. [online] The Independent. Available at: https://www.independent.co.uk/life-style/gadgets-and-tech/news/facebook-phone-numbers-data-breach-privacy-a9092641.html [Accessed 7 Sep. 2019].

Grothaus, M. (2019). The phone numbers of 419 million Facebook accounts have been leaked. [online] Fast Company. Available at: https://www.fastcompany.com/90399734/the-phone-numbers-of-419-million-facebook-accounts-have-been-leaked [Accessed 7 Sep. 2019].

Whittaker, Z. (2019). A huge database of Facebook users' phone numbers found online – TechCrunch. [online] TechCrunch. Available at: https://techcrunch.com/2019/09/04/facebook-phone-numbers-exposed/ [Accessed 7 Sep. 2019].

Winder, D. (2019). Unsecured Facebook Databases Leak Data Of 419 Million Users. [online] Forbes.com. Available at: https://www.forbes.com/sites/daveywinder/2019/09/05/facebook-security-snafu-exposes-419-million-user-phone-numbers/#2e5ce9c51ab7 [Accessed 7 Sep. 2019].