Mitigating Effects of Database Breaches with Stronger Password Storage Strategies

Walters, Bradley

When database breaches of large companies occur, attackers swarm the leaked files, attempting to crack user passwords contained within to sell or use for identity theft. Companies employing weak password storage strategies may leave their users' information in plain sight after a breach, as has been demonstrated by multiple incidents in recent years. This project aims to find which password storage strategies will leave a database of authentication information harder to crack in the event that database files are leaked. Using an AMD R7 260x processor and the open source password cracking utility Hashcat, a variety of storage strategies including MD5 hashing, MD5 hashing with salting, and bcrypt hashing were tested over a span of 5 minutes each. Approximately 50% of the passwords hashed with the MD5 algorithm without salting were cracked within 8 seconds. Passwords hashed with the bcrypt algorithm were the most resilient to cracking, with only 0.33% cracked on a low work factor and zero cracked on a high work factor in 5 minutes. Thus, the bcrypt algorithm with a high work factor was determined to be the best choice out of several for securely storing passwords. It is recommended for all data owners currently using the MD5 algorithm to switch to the bcrypt algorithm in order to protect their users.