Phoney protection for passwords

May 4 2016

Corporate data breaches seem to be on the rise, rarely a week passes without a company revealing that its database has been hacked and regrettably usernames, passwords, credit card details and its customers' personal information has been leaked on to the open internet. A new protection, nicknamed Phoney, is reported in the *International Journal of Embedded Systems*.

Rong Wang, Hao Chen and Jianhua of Sun College of Computer Science and Electronic Engineering, Hunan University, Changsha, China, explain that once password files have been stolen, attackers can quickly crack large numbers of passwords. With their "Phoney" system which employs a threshold cryptosystem to encrypt the password hashes in the password file and honeywords to confuse attackers, even if the hackers have comprised a database, the phoney, honeywords, obfuscate and camouflage the genuine passwords. Moreover, if those honeywords are de-hashed and used in a login attempt, the hacked system will know to immediately block the fake user and lock down the account they tried to break into.

Until a secure and safe alternative is found, passwords will remain the simplest and most effective way to login to online systems, such as shopping, banking and social media sites. Passwords lists stored by the providers can be salted and hashed to make it harder for hackers to decrypt them and users can help themselves by using long, sophisticated passwords. However, the hash used to mask a password database can itself be cracked and breaches happen and data is inevitably compromised. For example, recently 6.5 million logins from a major

social networking site were stolen and within a week almost two-thirds of those passwords had been cracked making a large proportion of the user base vulnerable to further exploitation and compromise of their personal data.

The team explains that, "Phoney is helpful to existing password authentication systems and easy to deploy. It requires no modifications to the client, and just changes how the password is stored on the server, which is invisible to the client." They have carried out tests and show that the time and storage costs are acceptable. "Of course, it is impossible for Phoney to guarantee no password leak absolutely in all possible scenarios," they say. But the so-called cracking 'search space', in other words the amount of effort a hacker needs to breach the data is increased significantly.

More information: Rong Wang et al, Phoney: protecting password hashes with threshold cryptology and honeywords, *International Journal of Embedded Systems* (2016). DOI: 10.1504/IJES.2016.076108

Provided by Inderscience Publishers