Bypassing popular passwords

May 7 2019, by David Bradley

Credit: CC0 Public Domain

Every year computer security companies share their findings regarding passwords and data breaches. Again and again, they warn computer users to use complex passwords and not to use the same passwords for different accounts. And, yet, data breaches and other sources show that too many people use the same simple passwords repeatedly and that

some of those passwords are ludicrously simple, the word "password" or the number "123456" really isn't a password at all given even the least-sophisticated hacking and cracking software available to malicious third parties these days.

Inertia is one important problem: it is difficult to get users, set in their ways, to change their old, easily remembered passwords to complex, difficult to remember codes. It is even harder to get such users to use password managers or multifactor authentication, which would add another layer of security to their logins.

Now, writing in the International Journal of Information and Computer Security, Jaryn Shen and Qingkai Zeng of the State Key Laboratory for Novel Software Technology, and Department of Computer Science and Technology, at Nanjing University, China, have proposed a new paradigm for password protection. Their approach addresses online and offline attacks to passwords without increasing the effort required of a user to choose and memorise their passwords.

"Passwords are the first security barrier for online web services. As long as attackers steal and crack users' passwords, they gain and control users' personal information. It is not just an invasion of privacy. It can also lead to more serious consequences such as data damages, economic loss and criminal activities," the team writes.

Their approach involves having a login system based on two servers instead of one. The user has a short, memorable password to access their longer, computer-generated "hashed" passwords on another server, the key to "de-hashing" those longer passwords are stored on the second server, but the actual password is stored on the user's device too and so the memorable password acts as a token for two-factor authentication. The approach means that attackers with even the most sophisticated hacking tools cannot apply an offline dictionary and brute-force attacks

effectively.

More information: Jaryn Shen et al. CSPS: catchy short passwords making offline and online attacks impossible, *International Journal of Information and Computer Security* (2019). DOI: 10.1504/IJICS.2019.099434

Provided by Inderscience