EASYAUDIT WHITE PAPER

Passwords: Length Is Not Enough

Many people believe that, when it comes to passwords, greater length means greater security. So why not use a very long string that is still easy to remember? Depending on taste, it could be a line from a national anthem or the lineup of a favorite football team.

Unfortunately, a new free password cracker, ocl-Hashcat-plus, will make life harder for anyone relying too much on long but predictable combinations. The old version attacked 15-character passwords effectively but did not go beyond that. The current one reaches 55 characters and decrypts passwords once considered out of reach.

The change matters because using a phrase instead of a simple word is one of the classic suggestions for securing an account without forgetting the combination. Understanding how this new version works helps us defend ourselves more effectively.

The software builds a database of possible words by searching dictionaries, encyclopedias and even forums for common letter combinations. The secret is not simply to look for very long alphanumeric strings, but to focus on something impossible to find on the web.

A whole tercet from Dante's Divine Comedy, long but widely present online, will not keep us safe. A distorted childhood word, however, will be much harder for the software to identify without becoming difficult to remember.

Our individual lives are probably the most unreachable word store for a search engine. To assess a chosen term quickly, search it on Google and look at the number of results. Forget heroic memory efforts: a little originality is much more useful for staying safe.