PAPER ID: 17-02-0133

An Analysis on Vulnerabilities of Password Retrying

M. S. A. Noman Ranak[1], Saiful Azad[1,2,*], Safwan Fathi Bin Mohammad[1], Kamal Z. Zamli[1,2], Mohammed Mostafizur Rahman[3]

[1]Faculty of Computer Systems & Software Engineering, University Malaysia Pahang, Gambang, Kuantan, Malaysia.
[2]IBM Center of Excellence, UMP, Gambang, Kuantan, Malaysia.
[3]American International University Bangladesh, 58/b Rd No 21, Dhaka 1213, Bangladesh.

Recently, due to security concerns, most of the computing systems have employed authentication based access control mechanisms. Again, in general, a considerable number of such systems we use in our day-to-day life. Hence, we also have to memorize a considerably large number of passwords, which incurs the issue of memorability. Mostly, a user retries password due to memorability problem. However, password retrying leads to several vulnerabilities. The main objective of this paper is to unveil these vulnerabilities with appropriate evidences. In this process, we discover and report an attack, named retry attack, which is discussed elaborately. An experiment has been performed and a survey has been conducted to examine the impact of such attack on *27* participants—where the experiment has been designed in such a way that it does not violate the ethical regulations of the university and preserves the secrecy of the participants' passwords. The results evidently demonstrate the impact of such attack. At the end, some suggestions are noted that would assist a user to tackle this kind of attack.

Keywords: Password, authentication scheme, credential, password retrying.