Jak skonstruować dobre hasło?

Przemysław Jaroszewski
CERT Polska

Przede wszystkim należy uzmysłowić sobie, co oznacza dobre hasło. Najprostszym i najpowszechniej stosowanym sposobem przełamywania haseł jest tzw. metoda słownikowa, polegająca na próbowaniu kolejnych słów z różnych słowników lub metoda nazywana *brute*-force, polegająca na generowaniu kolejnych ciągów znaków. Obecne rozwiązania są na tyle zaawansowane, że potrafią poradzić sobie także z prostymi „dekoracjami" haseł, np. przez dodanie na końcu jednej czy kilku cyfr. Wynika z tego prosty wniosek, że dobre hasło, to niekoniecznie hasło bardzo długie, ale na pewno dostatecznie skomplikowane. Wystarczy uzmysłowić sobie, że kod ASCII zawiera 256 znaków, z czego ponad 200 może być użyte w haśle. Ograniczając się do małych liter łacińskich, używamy zaledwie 26 z nich. Używając kombinacji małych i wielkich liter oraz cyfr mamy już 62 znaki. Przy ośmioliterowym haśle daje to ponadtysiąckrotnie więcej kombinacji, a zatem potrzeba ponad tysiąc razy więcej czasu, by odgadnąć je wspomnianymi metodami. Jeżeli dołożymy do tego kilka znaków specjalnych, np. *$, !* czy +, dostajemy w efekcie naprawdę mocne hasło.

Hasło składające się z małych i wielkich liter, cyfr oraz znaków specjalnych można wygenerować w sposób losowy. Problemem staje się jednak jego zapamiętanie. Wielu użytkowników trzyma zapisane hasła na karteczkach przy klawiaturze czy w notesie. W ten sposób oczywiście hasło staje się tylko tak bezpieczne jak trudny jest fizyczny dostęp do notatek. Z drugiej strony, kto zapamięta kilka czy kilkanaście haseł typu „b%7^(L0>"? Na szczęście, istnieją dobre metody, pozwalające na wybór haseł jednocześnie skomplikowanych i… łatwych do zapamiętania!

Zacznijmy od ułożenia lub wybrania zdania, które na pewno zapamiętamy. Może to być nasze ulubione powiedzonko, puenta dowcipu, cytat. Choćby:

„Litwo! Ojczyzno moja! ty jesteś jak zdrowie;"

Zapiszmy pierwsze litery cytatu. Dodając znaki interpunkcyjne, od razu wzbogacamy hasło:

L!Om!tjjz;

Całkiem nieźle. Możemy jeszcze zastąpić literę „O” cyfrą zero „0” (pamiętajmy, im szerzej korzystamy z zestawu znaków, tym lepiej).

L!0m!tjjz;

I mamy bardzo dobre, dziesięcioznakowe hasło, którego zapamiętanie powinno przyjść bez trudu.

Jeżeli musimy często zmieniać hasła, można posłużyć się techniką podobną, jak przy hasłach jednorazowych – użyć części stałej i zmiennej. Na przykład, jeśli hasło ma być zmieniane co tydzień, wprowadźmy jako cztery czy sześć dodatkowych znaków na końcu datę przypadającą we środę poprzedniego tygodnia. Jeszcze lepiej, jeśli nieco ją zmodyfikujemy, na przykład zapisując cyfry od końca albo zamieniając niektóre cyfry na kojarzące się z nimi litery (0=O, 4=A, 5=S itp.), albo odpowiadające im znaki specjalne, uzyskiwane jako Shift+cyfra (1=!, 4=$ itp.). Dla daty 14/08 mamy więc:

L!0m,tjjz;!$/)*

Pamiętaj! Nie wykorzystuj bezpośrednio przykładowych haseł czy systemów podanych w tym dokumencie. Zmodyfikuj je nieco. Pole dla wyobraźni jest ogromne. Powodzenia.