Brute Force Attack

Alan Kubit

June 17, 2019

Co to jest "Brute-force attack"?

Atak Brute-Force nazywamy metode łamania haseł testujac kombinacje wszystkich możliwych znaków. Stad też wywodzi sie nazwa - atak ten nie polega na wyszukanych algorytmach, lecz na czystej, brutalnej sile ataku (która jednak nie jest taka potężna w przypadku dłuższych haseł).

Brute Force Attack

Teoretycznie metoda ta jest w stanie odgadnać każde możliwe hasło (a zarazem każda możliwa informacje, z samej definicji działania ataku), jednakże jest to **bardzo** czasochłonne.

Najgorszy wróg - długie hasła

Jak wcześniej wspominałem w przypadku dłuższych haseł metoda ta jest bardzo nieopłacalna pod wzgledem czasu, jak i potrzebnej energii, oraz mocy obliczeniowej. Znacznie lepiej jest zastosować wtedy metode **słownika**.

Metoda słownika

Metoda ataku słownika polega na złamaniu hasła używajac przy tym kombinacji wcześniej przygotowanej bazy ciagów znaków pochodzacej z listy możliwych słów (a wiec słownika). Metoda ta testuje również wszelkie przerwy w słowach, wklejone w środku znaki, uciete słowa itp. itd.. Metoda ta ma duże szanse powodzenia ze wzgledu na fakt, iż duża cześć ludzi używa w swoich hasłach właśnie pełnych słów (ewentualnie dodatkowego ciagu znaków jeśli logowanie tego wymaga) - na przykład Rabarbar123.

Limity metody Brute Force

Zasoby potrzebne do zastosowania ataku nie rosna liniowo wraz ze wzrostem długości hasła, lecz eksponencjalnie. Praktycznie złamanie hasła 128-bitowego ta metoda jest bliskie zeru.

Limity metody Brute Force

Tak zwany limit Landauer ustanawia dolny limit energii potrzebnej na obliczenie kT · ln 2 na bit . Z założenia nie da sie wykonać obliczenia zużywajac mniej energii. A wiec żeby obliczyć 128-bitowy klucz potrzeba ok. 263 TWh (samo obliczenie, bez sprawdzania klucza).

GPU i FPGA

Dwie technologie wioda prym przy użyciu ataku brute force - sa to procesory graficzne (GPU), oraz bezpośrednio programowalna macierz bramek (FPGA). Dla przykładu COPACOBANA w technologii FPGA zużywa tyle samo energii co zwykły komputer, jednak wykonuje prace tak jak 2500 zwykłych PC (przy obliczania odpowiednich algorytmów).

Rynek wtórny haseł

Dla czesto "odgadnietych" haseł stosuje sie ich recykling - używanie ich celem sprawdzenia, czy jest ono poprawne, zanim zastosuje sie metode brute force.

Reverse Brute Force

Pewna modyfikacja tego ataku jest odwrotny atak brute force - zamiast atakować jednego użytkownika milionami haseł, atakuje sie milionów użytkowników jednym hasłem.

Ochrona przed Brute Force i Dictionary Attack

Najprostszym sposobem ochrony przed atakiem Brute Force jest używanie długich haseł.
Najprostszym sposobem ochrony przeciwko Dictionary Attack natomiast jest stosowanie niezrozumiałych ciagów znaków.
A wiec żeby obronić sie przed oboma atakami najlepiej stosować długie ciagi znaków.

Ochrona przed Brute Force i Dictionary Attack

Kolejnymi metodami ochrony może być możliwość wpisywania hasła tylko co określona jednostke czasu (np. 10 sekund czekania przed wpisaniem hasła), badź zablokowanie logowania na **t** czasu po **n** nieudanych próbach logowania (na przykład po 3 nieudanych próbach blokada na 5 minut). Administrator może zablokować dane IP po zauważeniu wielokrotnej ilości błednego logowania. Kolejnymi sposobami jest na przykład CAPTCHA przy każdym logowaniu, badź potwierdzenie telefoniczne/mailowe.