Łamanie haseł

Keywords: kombinatoryka, prawdopodobieństwo, statystyka, kombinatoryka, reguła iloczynu

Wraz z rozwojem Internetu i komunikacji na odległość pojawiła się potrzeba weryfikacji, czy osoba po drugiej stronie monitora jest faktycznie tą, z którą się komunikujemy, czy tylko kimś udającym znajomego. Analogicznie do sytuacji, w której na obcym terytorium spotyka się dwóch zaprzyjaźnionych szpiegów, oferowana jest możliwość użycia hasła. Dziś z hasłami w cyberprzestrzeni spotykamy się na co dzień, logując się do poczty elektronicznej, kont szkolnych, służbowych czy bankowości internetowej.

Ale czy samo istnienie haseł gwarantuje bezpieczne uwierzytelnianie użytkowników? Ciągłe doniesienia o nowych włamaniach i skradzionych kontach mówią nam, że nie. Metody, za pomocą których atakujący uzyskują dostęp do hasła użytkownika, można zasadniczo podzielić na dwie grupy, w zależności od tego, czy zostało ono skradzione, czy odgadnięte. Ponieważ poniższy problem dotyczy drugiego przypadku, przyjrzyjmy mu się bliżej.

Atak brute force, o którym dowiemy się w zadaniu, polega na wypróbowaniu wszystkich możliwych haseł. W zależności od mocy obliczeniowej komputera i używanego oprogramowania, szybkość testowania może wynosić od kilku tysięcy do kilkuset miliardów haseł na sekundę. W ten sposób bardzo krótkie hasła mogą zostać odgadnięte przez komputer w stosunkowo krótkim czasie (tj. natychmiast lub w ciągu kilku godzin).

Bardziej wyrafinowaną formą ataku siłowego jest *atak słownikowy*, w którym komputer nie próbuje haseł losowo, ale wybiera je ze słownika przygotowanych słów. Oprócz rzeczywistych słów, zawiera on powszechnie używane hasła, takie jak `password1234` lub `hasło`. Jeśli hasło ofiary znajduje się w słowniku atakującego, czas łamania jest znacznie krótszy w porównaniu do konwencjonalnego ataku siłowego.

Podstawowym zabezpieczeniem przed oboma rodzajami ataków jest stosowanie odpowiednio długich haseł (co najmniej 12 znaków) składających się z wielkich i małych liter, cyfr i innych znaków specjalnych.

Rysunek 1: Hakowanie

Zadanie

Program hakerski, w ataku brute force, gwarantuje złamanie ośmioznakowego hasła składającego się z dużych i małych liter alfabetu angielskiego w około 22 minuty. (Załóżmy, że zestaw znaków klawiatury do przetestowania można ustawić w ustawieniach programu).

Zadanie 1. Ile haseł wypróbowuje program w ciągu 1 sekundy?

Rozwiązanie. Ponieważ alfabet angielski składa się z 26 znaków, na każdej pozycji ośmioznakowego hasła

The portal Math4U is developed within the international projects of the Department of Applied Mathematics (VSB-Technical University of Ostrava) and other institutions in Czechia, Poland, Slovakia, and Spain.
Funded by the European Union

mogą znajdować się 52 możliwości (duże i małe litery). Korzystając z reguły iloczynu kombinatorycznego, możemy wywnioskować, że całkowita liczba możliwych haseł jest równa 52^8.

Liczba haseł wypróbowanych przez program w ciągu jednej sekundy to łączna liczba haseł.

$$\frac{52^8}{22 \cdot 60} \doteq 40\ 500\ 000\ 000.$$

Zadanie 2. Ile czasu zajęłoby programowi złamanie ośmioznakowego hasła, gdybyśmy zezwolili również na używanie cyfr?

Rozwiązanie. Dodając dziesięć nowych znaków, na każdej pozycji mogą znajdować się 62 różne znaki. Zgodnie z regułą iloczynu kombinatorycznego, liczba możliwych haseł wynosi 62^8; wykorzystując wynik poprzedniego problemu, otrzymujemy czas t, w którym program wypróbuje wszystkie hasła jako

$$t = \frac{62^8}{40\ 500\ 000\ 000} \doteq 5\ 391 \text{ s} \doteq 90 \text{ min}.$$

Zadanie 3. Ile znaków musiałoby mieć hasło składające się z cyfr i małych lub dużych liter alfabetu angielskiego, aby było wystarczająco silne, tj. gwarantowało, że jego złamanie zajmie co najmniej 100 lat? Jak zmieni się wynik, jeśli pozwolimy na użycie kolejnych 40 specjalnych znaków klawiatury?

Rozwiązanie. Zakładamy, że każdy rok ma 365 dni, czyli 31 536 000 sekund. Oznaczmy n jako wymaganą liczbę znaków i dodajmy je jak w poprzednim problemie. Teraz jednak otrzymamy równanie wykładnicze z niewiadomą n, które rozwiążemy:

$$\begin{aligned}
\frac{62^n}{40\ 500\ 000\ 000} &\geq 100 \cdot 31\ 536\ 000 \\
62^n &\geq 40\ 500\ 000\ 000 \cdot 3\ 153\ 600\ 000 \\
n \log 62 &\geq \log(40\ 500\ 000\ 000 \cdot 3\ 153\ 600\ 000) \\
n &\geq \frac{\log(40\ 500\ 000\ 000 \cdot 3\ 153\ 600\ 000)}{\log 62} \doteq 11{,}22
\end{aligned}$$

Hasło o wymaganym poziomie bezpieczeństwa musi mieć co najmniej 12 znaków.

Jeśli dopuścimy dodatkowe 40 znaków na klawiaturze, otrzymamy w wyniku podobnych obliczeń wynik w postaci

$$n' \geq \frac{\log(40\ 500\ 000\ 000 \cdot 3\ 153\ 600\ 000)}{\log 102} \doteq 10{,}01.$$

Hasło o wymaganym poziomie bezpieczeństwa musi teraz składać się z co najmniej 11 znaków.

Referencje i literatura

Literatura

- Raza, Mudassar & Iqbal, Muhammad & Sharif, Muhammad & Haider, Waqas. (2012).Przegląd ataków na hasła i analiza porównawcza metod bezpiecznego uwierzytelniania. *World Applied Scien-*

The portal Math4U is developed within the international projects of the Department of Applied Mathematics (VSB-Technical University of Ostrava) and other institutions in Czechia, Poland, Slovakia, and Spain.
Funded by the European Union

ces Journal. 19. 439–444.

Krajowa Agencja Bezpieczeństwa Cybernetycznego i Informatycznego. Bezpečný pohyb v kybersvětě* [online]. Available from https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/verejnost/ [cit. 30. 6. 2023].

Źródła obrazów

- Hacking password, Santeri Viinamäki, CC BY-SA 4.0, dostępny na https://commons.wikimedia.org/wiki/File:Hacking_password_illustration.jpg [cit. 30. 6. 2023].

The portal Math4U is developed within the international projects of the Department of Applied Mathematics (VSB-Technical University of Ostrava) and other institutions in Czechia, Poland, Slovakia, and Spain.

Funded by the European Union