Prelamovanie hesiel

Keywords: kombinatorika, pravdepodobnosť a štatistika, kombinatorika, pravidlo súčinu

S rozvojom internetu a komunikácie na diaľku išla ruka v ruke potreba overiť si, či osoba na druhej strane monitora je skutočne človek, s ktorým komunikujeme, alebo len niekto, kto sa vydáva za známeho. Podobne ako v situácii, keď sa predstavujú dvaja spriatelení špióni na cudzom území, ponúka sa možnosť použiť heslo. Dnes sa s heslami v kybernetickom priestore stretávame denne pri prihlasovaní do elektronickej pošty, školských alebo pracovných účtov či internetového bankovníctva.

Je však samotná existencia hesiel zárukou bezpečného overovania užívateľov? Priebežné správy o nových hackerských útokoch a ukradnutých účtoch hovoria, že nie. Metódy, ktorými sa útočníci dostanú k používateľskému heslu, možno v zásade rozdeliť do dvoch skupín podľa toho, či je heslo ukradnuté alebo uhádnuté. Keďže nasledujúci problém sa zaoberá druhým prípadom, pozrime sa naň bližšie.

Útok hrubou silou (po anglicky *brute force attack*), o ktorom sa dozvieme v tejto úlohe, spočíva vo vyskúšaní všetkých možných hesiel. V závislosti od výpočtového výkonu počítača a použitého softvéru sa rýchlosť testovania môže pohybovať od niekoľkých tisíc až po niekoľko stoviek miliárd hesiel za sekundu. Veľmi krátke heslá tak môže počítač uhádnuť v relatívne krátkom čase (t. j. okamžite alebo v priebehu niekoľkých hodín).

Sofistikovanejšou formou útoku hrubou silou je *slovníkový útok* (anglicky *dictionary attack*), pri ktorom počítač neskúša heslá náhodne, ale vyberá ich zo slovníka pripravených slov. Okrem skutočných slov obsahuje aj bežne používané heslá, ako napríklad `heslo1234` alebo `password`. Ak sa heslo obete nachádza v slovníku útočníka, čas prelomenia sa v porovnaní s bežným útokom hrubou silou výrazne skráti.

Základnou ochranou proti obom typom útokov je používanie dostatočne dlhých hesiel (aspoň 12 znakov) zložených z veľkých a malých písmen, číslic a iných špeciálnych znakov.

Obr. 1: Hacking

Zadanie

Hackerský program pri útoku hrubou silou zaručene prelomí osemznakové heslo zložené z veľkých a malých písmen anglickej abecedy približne za 22 minút (Predpokladajme, že sa v nastaveniach programu dá nastaviť množina testovaných znakov klávesnice).

Úloha 1. Koľko hesiel vyskúša program za 1 sekundu?

Riešenie. Keďže anglická abeceda má 26 znakov, na každej pozícii osemznakového hesla môže byť 52 možností (veľké a malé písmená). Pomocou kombinatorického pravidla súčinu môžeme odvodiť, že celkový počet možných hesiel sa rovná 52^8.

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

Počet hesiel, ktoré program vyskúša za jednu sekundu je celkovo

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

Úloha 2. Ako dlho by programu trvalo prelomiť osemznakové heslo, ak by sme povolili aj používanie číslic?

Riešenie. Pridaním desiatich nových znakov môže byť na každej pozícii 62 rôznych znakov. Podľa kombinatorického pravidla súčinu je počet možných hesiel 62^8; využitím výsledku predchádzajúcej úlohy dostaneme čas t, za ktorý program vyskúša všetky heslá ako

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

Úloha 3. Koľko znakov by muselo mať heslo zložené z čísel a malých alebo veľkých písmen anglickej abecedy, aby bolo dostatočne silné, t. j. aby jeho prelomenie trvalo aspoň 100 rokov? Ako sa výsledok zmení, ak pripustíme možnosť použitia ďalších 40 špeciálnych znakov klávesnice?

Riešenie. Predpokladáme, že každý rok má 365 dní, t. j. 31 536 000 sekúnd. Označme n požadovaný počet znakov a dosaďme ich ako v predchádzajúcej úlohe. Teraz však dostaneme exponenciálnu rovnicu s neznámou n, ktorú vyriešime:

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

Heslo s požadovaným zabezpečením by muselo mať aspoň 12 znakov.

Ak povolíme ďalších 40 znakov na klávesnici, dostaneme podobným výpočtom výsledok v tvare

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

Heslo s požadovaným zabezpečením musí mať teraz aspoň 11 znakov.

Odkazy a literatúra

Literatúra

- Raza, Mudassar & Iqbal, Muhammad & Sharif, Muhammad & Haider, Waqas. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal*. 19. 439–444.

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

- Národní ústav pro kybernetickou a informační bezpečnost. *Bezpečný pohyb v kybersvětě* [online]. Dostupné z `https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/verejnost/` [cit. 30. 6. 2023].

Zdroje obrázkov

- Hacking password, Santeri Viinamäki, CC BY-SA 4.0, dostupné 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