Math4You

2023–2025

Prolamování hesel

S rozvojem internetu a dálkové komunikace šla ruku v ruce potřeba ověřit, zda se na druhé straně monitoru nachází skutečně člověk, s nímž komunikujeme, nebo jen někdo, kdo se za známého vydává. Podobně jako při seznamování dvou spřátelených špionů na cizím území se nabízí možnost použití hesla. Dnes se s hesly člověk setkává v kyberprostoru každodenně, při přihlašování k e-mailu, školnímu či pracovnímu účtu nebo k internetovému bankovnictví.

Zaručuje však samotná existence hesel bezpečné ověřování uživatele? Průběžné zprávy o nových hackerských útocích a ukradených účtech nám říkají, že nikoliv. Metody, kterými se útočníci dostanou k heslu uživatele, se v podstatě dají rozdělit na dvě skupiny podle toho, zda dojde ke krádeži nebo k uhádnutí hesla. Protože se následující úloha zabývá druhým případem, podívejme se na něj blíže.

Útok hrubou silou (anglicky *brute force attack*), se kterým se v úloze seznámíme, spočívá ve vyzkoušení všech možných hesel. V závislosti na výpočetní síle počítače a použitém softwaru se rychlost zkoušení může pohybovat od několika tisíc po několik set miliard hesel za sekundu. Velmi krátká hesla tak mohou být počítačem uhádnuta v poměrně krátkém čase (tj. okamžitě nebo v řádech hodin).

Dokonalejší forma útoku hrubou silou je tzv. *slovníkový útok* (anglicky *dictionary attack*), kde počítač nezkouší hesla náhodně, ale vybírá je ze slovníku připravených slov. Ten kromě skutečných slov obsahuje také typicky užívaná hesla typu `heslo1234` nebo `password`. Jestliže se heslo oběti nachází ve slovníku útočníka, doba prolomení se oproti klasickému útoku hrubou silou výrazně zkrátí.

Nezbytnou ochranou proti oběma typům útoků je používání dostatečně dlouhých hesel (alespoň 12 znaků) vytvořených z malých a velkých písmen, číslic a dalších speciálních znaků.

Obrázek 1: Hacking

Co-funded by the Erasmus+ Programme of the European Union.

Zadání

Hackerský program při útoku hrubou silou zaručeně prolomí heslo o osmi znacích z malých i velkých písmen anglické abecedy nejvýše za 22 minut, což je čas, za který při daném výpočetním výkonu projde všechny možnosti. (Předpokládejme, že se v nastaveních programu dá nastavit množina zkoušených znaků klávesnice.)

Úloha 1. Kolik hesel program vyzkouší za 1 sekundu?

Řešení. Protože má anglická abeceda 26 znaků, může být na každé pozici osmiznakového hesla ze zadání 52 možností. Užitím kombinatorického pravidla součinu tak odvodíme, že je celkový počet možných hesel roven číslu 52^8.

Počet hesel, které program vyzkouší za jednu sekundu je celkem

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

Úloha 2. Jak dlouho by programu trvalo zaručené prolomení hesla o osmi znacích, pokud bychom připustili také použití číslic?

Řešení. Přidáním deseti nových znaků může být na každé pozici 62 různých znaků. Dle kombinatorického pravidla součinu je počet možných hesel 62^8; užitím výsledku z předchozí úlohy dostaneme čas t, za který program vyzkouší všechna hesla jako

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

Úloha 3. Kolik znaků by muselo mít heslo složené z číslic a malých nebo velkých písmen anglické abecedy, aby bylo dostatečně silné, tj. jeho zaručené prolomení trvalo alespoň 100 let? Jak se výsledek změní, jestliže připustíme možné použití dalších 40 speciálních znaků klávesnice?

Řešení. Předpokládáme, že každý rok má 365 dní, tedy 31 536 000 sekund. Označme n požadovaný počet znaků a dosaďme podobně jako v předchozí úloze. Nyní však dostáváme exponenciální rovnici s neznámou n, kterou vyřešíme:

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

Heslo s požadovanou bezpečností by tak muselo mít alespoň 12 znaků.

Jestliže připustíme dalších 40 znaků na klávesnici, obdobným výpočtem dostaneme výsledek ve tvaru

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

Nyní by tak heslo s požadovanou bezpečností muselo mít alespoň 11 znaků.

Odkazy a literatura

Literatura

- 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.
- 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 obrázků

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