RADEK BENEŠ MSc.
soudní znalec informačních technologií

Uživatelská hesla a hrubá síla, resp. jednoduchá matematika

Úvod

V praxi se velmi často setkávám s běžnými hesly uživatelů (ať již jako znalec zkoumající např. techniku, ke které uživatelem nebyl dodán přístup, nebo při běžném technickém zásahu, v podnikovém provozu, atp.), kdy je stále běžným zvykem používat velmi jednoduchá a zapamatovatelná hesla uživateli, nebo i tzv. PINy o délce např. 4 znaků, atp. Pro běžné uživatele je stále nepochopitelné, jak je možné, že jde takovéto heslo odhalit během několika vteřin (např. svému klientu jsem byl schopen na telefonické požádání převést finanční prostředky z lokální aplikace při absenci uživatele, který měl v držení jediný přístup) a přitom zde vládne opravdu jednoduchá matematika základní školy. Tento krátký článek věnuji jednoduchému vysvětlení, kdy běžný uživatel předpokládá pod představou útočníka jinou osobu, která se posadila za jeho klávesnici a pokouší se uhodnout jeho „bezpečné“ heslo.

Základní matematika, resp. variace

Pro náš jednoduchý příklad předpokládejme, že posuzujeme běžné heslo uživatele o pěti znacích. Jak již to tak bývá, tak se heslo bude skládat pouze z malých písmen anglické abecedy (tedy v tomto případě vynechávám českou diakritiku, kdy heslo používané z více stanic, tedy bez předpokladu nainstalovaných klávesnic, atp. se diakritika příliš nevyužívá). Pro úplnost uvádím, že počet písmen anglické abecedy je dvacet šest.

Nyní již jen jednoduše spočítáme, kolik různých hesel o délce pěti znaků, mohl uživatel z této množiny sestrojit. Budeme používat variace, jelikož nám záleží na pořadí písmen (heslo např. mé jméno „radek“, není stejné jako slovo „darek“, ačkoliv se skládá z naprosto stejných písmen). Dále musíme využít variace s opakováním, protože písmena se v heslech mohou opakovat.

Vzoreček pro práci s variacemi s opakováním vypadá $V'(k, n) = n^k$. Za n dosadíme počet písmen, ze kterých budeme vybírat – počet písmen anglické abecedy a za k, dosadíme počet písmen, ze kterých se heslo skládá, v našem případě pět. Vychází nám přibližně dvanáct milionů různých variací, včetně opakování.

Výpočetní výkon

Zde je na místě zmínit výpočetní možnosti počítačů, což je velice variabilní a na další odbornější článek, ale budeme v tomto případě počítat s naprostým základem, čili s tím, že počítač zvládne cca deset milionů porovnání a vyhodnocení za vteřinu.

Udělením této konstanty v tomto pojednání je již každému čtenáři jasné, že s jednoduchým software jsme vybrané heslo odhalili cca za 1,2s.

Běžná hesla o více znacích

Některé informační systémy neumožňují zvolit tak krátké a jednoduché heslo, jako jsme pro příklad zvolili výše. Setkávám se s tím, že heslo by nemělo být kratší, nežli osm znaků. Spočítejme tedy, kolik existuje variací pro osmimístné heslo. Stejně jako v předchozím případě budeme uvažovat pouze malá písmena anglické abecedy. Dosadíme tedy do vzorce a vychází nám 268, což je přibližně dvě stě miliard variací. Zdá se, že jde již o několik řádů větší číslo. Náš imaginární počítač by tedy všechny variace vyhodnotil za cca necelých šest hodin. Zkusme, jak by narostla síla hesla, pokud budeme využívat i velká písmena, číslice a speciální znaky jako jsou podtržítka, pomlčky apod.

Hesla se speciálními znaky

Malých písmen je tedy 26, velkých písmen je tedy také 26, to dává dohromady 52 znaků. K tomu ještě musíme přičíst 10 číslic a některé speciální znaky. Nemůžeme počítat se všemi povolenými speciálními znaky, tak pro jednoduchost budeme počítat pouze s osmi speciálními znaky. Délka hesla bude opět osm znaků, stejně jako v předchozím výpočtu. Po dosazení vychází toto číslo: 708, což je pro lepší představu přibližně $5 \cdot 1014$, slovně pět milionů miliard variací ☺. Což již je docela úctyhodné číslo. Náš imaginární počítač, resp. útočník, by všechny variace zkontroloval za cca šestnáct tisíc hodin! Což jsou necelé dva roky.

RYBNÁ 716/24, PRAHA 1 , 110 00, CZECH REPUBLIC
TEL: (+420) 725 37 37 37 • FAX: (+420) 227 203 999 • WEB: www.RADEK-BENES.cz

Závěrem
Na těchto velmi jednoduchých výpočtech jsme si předvedli, jak exponenciálně roste množina možných variant hesel, resp. doba prolomení, nebo chcete-li uhodnutí hesla, pokud používáme standardně alespoň velká i malá písmena, číslice a nejlépe i speciální znak, při rozumném počtu znaků v hesle, atp.

Dále je potřeba zmínit, že tato popsaná metoda je samozřejmě tou nejjednodušší a v některých případech (např. přerušení přihlášení uživatele na nějakou dobu při několika neplatných pokusech) také zcela nepoužitelná. I v případě možného použití této hrubé síly se však využívají nejdříve např. slovníky (zda heslo dává nějaký smysl, není kombinováno z několika slov, zkratek, běžných výrazů a často používaných hesel, atp.), nicméně pro představu čtenáře snad takto stačí.

Pro naprostou úplnost a srovnání ještě uvedu paralelu s lidským mozkem.
Dle p. Dharmendry Modhy, tedy vedoucího výzkumného týmu z IBM Almaden Research Center, který se věnuje problematice umělé inteligence a tvorby „kybernetického mozku“, je jakýkoli superpočítač stále daleko za výkonem běžného lidského mozku. Tradiční počítač by totiž musel mít cca 3 581 terabajtů paměti a výkon okolo 38 petaflops (38 biliard operací za sekundu).

RYBNÁ 716/24, PRAHA 1 , 110 00, CZECH REPUBLIC
TEL: (+420) 725 37 37 37 • FAX: (+420) 227 203 999 • WEB: www.RADEK-BENES.cz