Ro-z-rušte heslo!

V posledních dvou letech došlo v odborné komunitě ke změně postoje vůči heslům. V prvním dílu jsme ukázali, že hesla si lze zapisovat. V druhém dílu jsme ocenili kvalitu hesel, která jsou tvořena z klíčových vět. Viděli jsme, že i delší klíčové věty obsahují méně entropie, než potřebujeme. A dříve doporučovaná metoda výběru prvních písmen z jejich slov nás o ni ještě více ošizuje. Proto jsme doporučili větu použít celou, a v tomto dílu ukážeme, jak ji dále zásadně zkvalitnit, a to jejím rozrušením.

Výpočet kvality hesla

Ještě než si představíme naši metodu, uvedeme postup, kterým se měří kvalita hesla podle doporučení NIST [2]. Použijeme-li klíčovou větu samotnou, zjistíme velikost její entropie metodou předvedenou v minulém čísle. V češtině je to odhadem 4,5 bitu za první znak, 2,67 bitu za 2.–8. znak, 2 bity za 9.–20. znak a 1,33 bitu za každý další znak.

Dvě základní pravidla na zlepšení a bonusy

První pravidlo [2] zlepšení klíčové věty je její test proti slovníku. Slovník obsahuje běžná slova a běžně používané passwordy („1234", „password" atd.) a musí mít alespoň 50 000 výrazů. Klíčová věta nesmí také obsahovat jakoukoli permutaci uživatelského jména. Jestliže jsou tyto podmínky splněny, přičítá se další bonus 6 bitů.

Další bonus 6 bitů se připočítá jen u hesel do 20 znaků, pokud obsahují alespoň jedno velké písmeno, alespoň jedno malé písmeno a alespoň jeden znak ze sady nealfabetických znaků (číslice a všechny ostatní nepísmenkové znaky na klávesnici). Klíčová věta „Kočka leze dírou, pes oknem, nebude-li pršet, nezmoknem." má entropii 79 bitů a bonus za první pravidlo 6 bitů, tj. 85 bitů. Kdo chce větší kvalitu i s kratší klíčovou větou, může číst dále.

Základní myšlenka

Základní myšlenka našeho doporučení: u klíčové věty provedeme takovou modifikaci, která je co nejvíce nestrukturovaná, nesystematická, nesmyslná, unikátní, zkrátka nepredikovatelná. Tím vlastně vybereme heslo z *„množiny všech myšlenek jak tvořit heslo"*. Taková množina je velmi velká. Pokud bychom ale volili sebeztřeštěnější myšlenku a heslo bylo krátké nebo znaková sada malá, útočník by prostě vyzkoušel všechny možnosti hesla dané délky nezávisle na tom, jak geniálně jsme ho vytvořili. Čím větší je znaková sada, tím kvalitnější je heslo. Proto je velmi efektivní do modifikace *zahrnout* nové znaky, nepoužité v klíčové větě, zvláštní znaky apod. V duchu nepredikovatelnosti však nesmíme tuto radu vzít jako úzké pravidlo „vezmi klíčovou větu a (pouze) umísti do ní nějaké zvláštní znaky". Tím bychom hrubě porušili pravidlo unikátnosti a nepredikovatelnosti své modifikace. Nepredikovatelnost nemůžeme zajistit pouhým přidáním zvláštních nebo nových znaků. Musíme ji zajistit naší unikátní myšlenkou rozbití klíčové věty. V dalším uvidíme, že nejlépe je klíčovou větu rozbít nejméně dvěma *různými metodami*.

Otevřete-li notebook, nikdy nemůžete zapomenout to, co už je před vámi napsáno. Můžete to využít jako základ pro klíčovou větu nebo její rozrušení:

IntelRinsidecentrinoTM
TravelMate45002LMi
modrocervenymotylek
IntelRPentiumRM725processor
DesignedforMicrosoftRWindowsRXP
CapsLockASDFGHJKL+!
TabulatorCapsLockShiftCtrl
Interoperable with IEEE 802.11bg

Pomůcky pro heslo přímo před očima

Příklady rozbití klíčových vět

Místo mezery vložíme poslední písmeno slova, ale s velkým písmenem: „KočkaAlezeEdírouU,pesSoknemM,nebude-liIpršetT,nezmoknem." Druhým rozbitím může být modifikace „oknem – window", takže máme „KočkaAlezeEdírouU,pesSwindowW,nebude-liIpršetT,nezmoknem." Hesla často tvoří data narození dětí, třeba „12052005". To je strašně chudé! A přesto stačí trochu rozvinutější klíčová věta „Andrea se narodila 12.5.2005" nebo „Michal má narozeniny dvanáctého května 2005". Teď bychom měli narušit její přirozený jazyk, třeba zdvojíme každé písmeno „a": „AAndreaasenaarodilaa12.5.2005". Nebo větu „Mqiwcehratlzmanarozeninydvanactehokvetna2005" obdržíme tak, že slovo Michal píšeme pravou rukou a za každým písmenem jsme levou rukou připsali písmeno ze třetího řádku klávesnice (qwertz). Tyto tzv. geometrické vzory může útočník ovšem také naprogramovat, takže ke každému slovu prostě vyzkouší jeho geometrické varianty. Může ale vyzkoušet jen ty varianty, které ho napadnou – a na vás je, abyste udělali variantu tak individuální, že stěží někoho napadne. Protože nemůžeme mít jistotu, že útočníka příslušná úprava nenapadne, je lépe rozbít klíčovou větu dvěma různými metodami. Dobrá myšlenka je použít něco na první pohled strašně komplikovaného, co si ale velmi jednoduše pamatujeme. Například německy „JZD" – landwirtschaftlicheproduktionsgenossenschaft. Kdo si nepamatuje pravopis, je na tom lépe, protože heslo použije tak, jak se to vyslovuje. Zároveň tím trochu boří jazyk: „Landvirčaftlicheprodukcionsgenosnšaft". Jaký bonus máme připočítat za „modifikaci výslovností"? Většinou se dá dané heslo vyslovit jen jedním způsobem, takže jeden bit bonusu je dobrý odhad. Jsme tedy jen o jeden bit lepší než slovo ze slovníku! Nezbývá než takové slovo rozbít další metodou. Třeba „Landvir**kšá**ftlicheprodukcionsgenosn**kšá**ft",tj. když vyslovujeme „ča/ša", píšeme „kšá", což nám může připomínat slepice v JZD. Ideální je ale v rámci rozbití zavést nové znaky, takže když už píšeme kšá místo ča/ša, můžeme tam přidat nějaký zvláštní znak, číslo nebo slovo, například „Landvir**KSA123**ftlicheprodukcionsgenosn**KSA123**ft" nebo **„www.** Landvir**KSA**ftlicheprodukcionsgenosn**KSA**ft**.de**" nebo „Landvir**KSASLEPICE**ftlicheprodukcionsgenosn**KSA**ft".

Originalitou proti útokům

Pokud budou naše rozrušení klíčové věty nepredikovatelná, útočník se k heslům nedobere „analyticky", tj. nějakým lepším postupem než jen hrubou silou. Například u posledního hesla o délce 46 znaků (malá a velká abeceda, 52 písmen) bude útočník muset vyzkoušet $46^{52} > 2^{287}$ možností. Přitom původní klíčová věta měla mizivou hodnotu, neboť to bylo vlastně jedno německé slovo. Jak jsme už předeslali, informační bohatost hesla kompenzujeme „silou myšlenky".

Závěr

Naše doporučení na zkvalitnění hesla je jednoduché: vezměte klíčovou větu a rozrušte ji nejlépe dvěma různými originálními metodami.

Vlastimil Klíma, Tomáš Rosa,
v.klima@volny.cz, trosa@ebanka.cz

LITERATURA

[1] E-archivy http://cryptography.hyperlink.cz, http://crypto.hyperlink.cz

[2] Electronic Authentication Guideline, NIST Special Publication 800-63 Ver 1.0.2, http://csrc.nist.gov/publications/nistpubs/800-63/SP800-63V1_0_2.pdf