Prolamovače hesel

Chránit si důvěrná data heslem by v současnosti mělo být nepsaným pravidlem. Smůla ovšem je, když si na heslo později nemůžete vzpomenout. Jedinou nadějí mohou být v takovém případě nástroje pro rekonstrukci hesel (password recovery). Chip vám představí ty nejlepší!

Nepamatuji si heslo! Aby nikdo nemohl nahlédnout do vašeho důvěrného dokumentu ve Wordu, opatřili jste ho heslem a teď ho nemůžete otevřít. To heslo začínalo na "L". Ne, nebylo to "Leica", nebylo to jméno labradora ani poznávací značka auta, nýbrž pořádné, bezpečné heslo, s písmeny, číslicemi a zvláštními znaky. Chránit dokumenty heslem patří mezi standardy bezpečnosti uvědomělého uživatele. Jen tak si může být jist, že k jeho datům nebude mít přístup žádná třetí osoba. Stupeň bezpečnosti pak závisí na druhu a délce použitého hesla.

V zásadě funguje ochrana dokumentů a jiných dat heslem takto: Při zadání třeba ve Wordu je heslo určitým algoritmem zašifrováno. Na konci tohoto procesu je kontrolní součet, který se uloží v dokumentu. Při opětovném otevření program ze zadaného hesla opět vypočítá kontrolní součet a porovná ho s uloženým. Pokud souhlasí, lze dokument dešifrovat a otevřít.

Pro každé heslo platí, že když jej zapomenete, zavřete cestu sami sobě. Právě firmy často trpí tím, že se nemohou dostat k důležitým datům bývalých zaměstnanců. Vynalézaví programátoři tento problém identifikovali a vyvinuli nástroje, které umí přečíst přístupové kódy pro nejrůznější aplikace.

Chip otestoval prolamovače hesel pro nejdůležitější programy a vybral ty, které pracují spolehlivě a jsou snadno ovladatelné. Programy, které zde představujeme, jsou určeny jen k otevírání vašich vlastních souborů. Budete-li s nimi louskat data jiných uživatelů, dopustíte se trestného činu.

Windows XP

Operačním systémem Windows XP může být na jednom počítači odděleně obslouženo více uživatelů. Jednotlivé uživatelské účty se proto dají chránit hesly. Microsoft sice při šifrování hesel používá bezpečné kryptografické algoritmy, existuje tu však jeden problém: aby byla zajištěna kompatibilita se staršími verzemi Windows, nevyužívá Microsoft schopností existujících šifrovacích metod úplně. Proto má útok hrubou silou, tedy zkoušení všech možných kombinací, poměrně velkou naději, že takto chráněné heslo během několika málo hodin odhalí. Mnoho správců a uživatelů navíc nevyužívá plný počet znaků hesla, nýbrž se většinou spokojí se čtyřmi až pěti znaky. Windows XP přihlašovací hesla standardně ukládají do souboru SAM (Security Accounts Manager). Tento soubor najdete v adresáři C:\WINDOWS\SYSTEM32\CONFIG. Tak snadno se ovšem k cíli nedostanete, neboť Windows soubor ochraňují tak, že brání jeho kopírování a čtení. Pro dobré prolamovače hesel to však není žádný problém.

@stake LC4

Pro hesla do Windows se optimálně hodí program LC4 od @stake. Jeho rozhodující výhodou oproti konkurentům je to, že tento nástroj umí přečíst soubor SAM, který obsahuje všechna důležitá hesla Windows. Jiné nástroje ztroskotají už na vlastní ochraně Windows, která zakazuje, aby soubor byl za běhu systému Windows čten. Důvod: Soubor SAM je během aktivní relace Windows uložen v operační paměti počítače - a právě tam po něm LC4 sahá. Uživatel může zvolit mezi různými metodami. Vedle útoku hrubou silou je k dispozici slovníková metoda (viz rámeček na str. 158). Kromě toho existuje zvláštní forma této metody, která ke slovníku přidává další písmena a číslice. LC4 tak může rychle najít i hesla jako "Dum99". Pro hesla Windows je LC4 v současnosti nejlepším nástrojem.

Informace www.atstake.com
Download www.atstake.com/research/lc/ download.html
Cena cca 350 eur
Verze na Chip CD 15ti denní trial

Microsoft Office XP

Všechny aplikace Office nabízejí možnost ochrany vytvořených dokumentů, tabulek a databází. Pokud jste heslo zapomněli, pomůže vám správný software.

Advanced Office XP Password Recovery

Tento nástroj od Elcomsoftu ovládá metody hrubé síly, slovníkového útoku a hrubé síly se zakrytím. Posledně jmenovaná metoda má smysl v případě, kdy si ještě vzpomínáte na část hesla, například počáteční písmeno nebo nějakou číslici. Po startu kliknete v menu "File" na "Open File" a vyberete zaheslovaný soubor Office. Potvrdíte stiskem "OK" a v menu "Recovery" zvolíte položku "Start". Nástroj začne hledat metodou hrubé síly, na přání však můžete začít i slovníkovou metodou.

TIP: Hledání vždy začínejte slovníkovou metodou, pokud ještě víte, že jste jako heslo použili skutečně existující pojem. Program umí zacházet nejen se soubory Office XP, ale ovládá také všechny starší verze Microsoft Office. Mimo to se s ním dají rozluštit také hesla e-mailových účtů Outlooku.

Informace www.elcomsoft.com
Cena cca 140 eur
Download www.elcomsoft.com/aoxppr.html
Verze na Chip CD 30denní trial

Office Password Recovery

Tento nástroj od AccentSoft Utilities je též vhodný pro Office. Podporuje Word, Excel, Access a Microsoft Money. Úrovně výbavy nástroje Elcomsoftu ovšem nedosahuje. Uživatelské okno je sice omezeno na to důležité, přesto nástroj plní svou funkci. Vedle metody hrubé síly ovládá Office Password Recovery také slovníkovou metodu. Praktické: Instalační CD již obsahuje slovníky v angličtině. Bohužel chybí odkazy na internetové stránky, které nabízejí seznamy slov v jiných jazycích. Informace a download www.denglad.com Cena cca 50 eur Verze na Chip CD max. 4 znaky hesla

Komprimované archivy

Zběhlí uživatelé často komprimují data do souborů, které chrání heslem. Většinou se k tomu používají WinZip, WinRAR, WinAce nebo poněkud zastaralý formát ARJ. Kdo zapomněl heslo, pomůže si následujícími nástroji.

Advanced Archive Password Recovery

Nástroj Elcomsoftu používá metody ‚hrubá síla' a ‚slovník'. Standardně se program spustí s hrubou silou. Oba postupy prolomily testovaná hesla (čtyři znaky) ve WinZipu 8 během několika minut. Naproti tomu skenování souboru komprimovaného pomocí WinRAR trvalo sedm hodin, což hovoří pro znatelně lepší šifrovací algoritmus ve WinRAR.

Uživatelské rozhraní je uspořádáno jasně, uživatel musí v programu pouze otevřít zaheslovaný soubor a stisknout "Start". Praktické: Kdo chce, může soubor přetáhnout na program metodou "táhni a pusť" a hned začít. Na záložce "Dictionary" je možné přidat další seznamy slov, například z www.elcomsoft.com/prs.html. Podpora formátů je slušná - vedle Zip, RAR a Ace ovládá nástroj také ARJ, tedy všechny důležité formáty.

Informace www.elcomsoft.com
Cena cca 60 eur
Verze na Chip CD 30denní trial
Download www.elcomsoft.com/archpr.html

Visual zip password recovery processor

Dalším efektivním nástrojem je Visual zip password recovery processor od firmy ZipCure. Nástroj nabízí stejné metody k prolomení hesel, stojí však o 30 eur méně. Výsledky při čtení hesel jsou srovnatelné s nástrojem Elcomsoftu. Obsluha není tak vydařená jako u konkurenta: mnoho možností nastavení je ukryto příliš hluboko v programu. Tento nástroj tak lze doporučit spíše pokročilým uživatelům s dostatkem zkušeností. Navíc program nenabízí drag & drop (táhni a pusť) a umí rozluštit jen archivy Zip.

Info www.zipcure.com
Cena cca 25 eur

RAR Password Cracker

Třetí nástroj na komprimované soubory se zcela specializoval na archivy formátu RAR. Program RAR Password Cracker od Dimitrije Nikitina nabízí jako jediný ze zde představených nástrojů pomocníka, který má začátečníkům usnadnit rozlousknutí hesel. Bohužel tak vždy nečiní, občas dokonce mate

hlášeními, která právě začátečníky znejistí. Hlášení samotná jsou sice neškodná, přesto ruší při práci. Standardně jsou integrovány metody hrubé síly a slovníku.

Informace www.rarpasswordcracker.com
Cena cca 30 eur

Soubory PDF

Také pro přečtení hesel chráněných PDF souborů existují specializované programy.

Advanced PDF Password Recovery

Tento dobře promyšlený nástroj našel testované heslo sestávající ze čtyř znaků asi za 15 minut, ačkoli nebylo uvedeno v žádném seznamu slov. Konfigurační možnosti jsou vydařené: Kdo například ještě ví, že heslo začíná na "T", nastaví toto jako počáteční hodnotu. Tím se zřetelně zkrátí doba skenování. Výsledek však často přináší rozčarování: Kdo konečně má více než rok času, aby čekal na své zapomenuté heslo? Praktické: Uživatel může program naladit na svůj procesor, čímž jej nástroj využije optimálně.

Alternativa k tomuto nástroji od Elcomsoftu, která by se dala brát vážně, v současnosti neexistuje. Různé hackerské stránky sice také nabízejí nástroje na rozlousknutí PDF souborů, od nich však Chip odrazuje: za mnohými číhají viry, dialery, spyware nebo ad-aware.

Informace www.elcomsoft.com
Cena cca 50 eur

Messengery a chat

Tomu, kdo používá více programů pro chat, například ICQ, T-Online-Messenger, AOL Instant Messenger nebo MSN Messenger, pomůže v případě, že se jeho heslo ztratí, níže uvedený nástroj.

Advanced IM Password Recovery

Tento nástroj od Elcomsoftu i zde přesvědčuje na celé čáře. Dokonce osmimístné heslo do ICQ 2003 bylo při testu po několika sekundách na obrazovce jako čitelný text. Tento výsledek ukazuje, jak je šifrování v ICQ & spol. k ničemu. Kdo se v případě messengerů cítí bezpečně, mýlí se. Doporučujeme: Advanced IM Password Recovery spolehlivě přečte hesla z 31 různých chatovacích programů.

Informace www.elcomsoft.com
Cena cca 30 eur

Uložená hesla

U některých windowsovských aplikací je možné hesla po jejich prvním zadání uložit. Pro připojení na internet například stačí sestavit spojení, aniž byste museli znovu zadávat heslo. Když ho zapomenete, pomůže následující freewarová utilita.

PantsOff

Uložená hesla, jako například to pro připojení k internetu, se zobrazují jen ve formě hvězdiček. Touto utilitou jednoduše přejedete hvězdičky lupou a už je heslo vidět.

Informace www.cbuenger.de
Cena freeware

Thomas Baur a Fabian von Keudell, autor@chip.cz

SPRÁVNÉ HESLO

Kdo chce bezpečná hesla, měl by se řídit následujícími pravidly a radami.

Zásadně nepoužívejte jména nebo data narození a vyhněte se obecně všem smysluplným slovům, jedno v jakém jazyce. Používejte také zvláštní znaky (interpunkční znaménka apod.) a střídejte malá a velká písmena. Neukládejte žádná hesla, ani když váš program tuto možnost nabízí, ale zadávejte je pokaždé znovu.

NÁVOD, JAK SI VYTVOŘIT BEZPEČNĚJŠÍ HESLO

Sestavte si nejprve větu, kterou si lehce zapamatujete. Třeba: "Ahoj! Jak vlastně zní Tvoje bezpečné heslo?" Nyní vezměte vždy první písmeno z každého slova a interpunkční znaménka. Z nich vytvoříte následující kód: A!JvzTbh?

Jelikož toto heslo nestojí v žádném lexikonu, slovníková metoda žalostně selže. Jen metoda hrubé síly by se mohla dobrat výsledku, trvalo by to ovšem extrémně dlouho. Při 9 znaků dlouhém hesle a znakové sadě obsahující 255 znaků existuje 2559 možností.

JAK DLOUHO TRVÁ PROLOMENÍ HESLA

Čím delší je heslo a čím více různých znaků se v něm nachází, tím je bezpečnější. Níže uvedené doby potřebné k prolomení hesla platí pro počítače, které umí za sekundu vypočítat okolo 25 000 000 kombinací (Pentium 4/2,5 GHz).

JEN MALÁ PÍSMENA ABECEDY (26 ZNAKŮ)		
Počet znaků	**Možnosti kombinací**	**Trvání**
4 znaky	456976	18 milisekund
8 znaků	2,08827E+11	2 hod. 30 min.
12 znaků	9,5429E+16	121 let

CELÁ ASCII TABULKA (128 ZNAKŮ)		
Počet znaků	**Možnosti kombinací**	**Trvání**
4 znaky	268435456	11 sekund
8 znaků	7,20576E+16	91 let
12 znaků	1,93428E+25	24,5 miliardy let

JAK PRACUJÍ PROLAMOVAČE HESEL

SLOVNÍKOVÁ METODA: JEDNODUŠE HLEDAT V KNIZE

Mnozí uživatelé používají jako hesla celá slova nebo jména. To je sice jednoduché, ale také málo bezpečné. Na internetu existují k bezplatnému stažení obsáhlé slovníky a seznamy jmen, které utility na zjištění hesla využívají k jeho prolomení. Postup je jednoduchý. Programy se propracovávají celými slovníky, dokud nenarazí na hledané slovo. Přitom nehraje roli, v jakém jazyce bylo heslo zadáno, protože pro všechny běžné jazyky existují odpovídající seznamy. Moderní prolamovače najdou heslo, které je uvedeno v některém slovníku, zpravidla během několika minut.

Pokud tedy hledáte slovníky, můžete se podívat například na www.elcomsoft.com/ prs.html, kde naleznete i český, nebo na www.accessdata.com/dictionaries.htm. Tyto seznamy slov obecně existují jako čisté textové soubory, které může uživatel pomocí rutiny načíst do programu a v případě potřeby i editovat.

HRUBÁ SÍLA (BRUTE-FORCE): POKUS A OMYL

Tento postup je nesrovnatelně náročnější na výpočty a běžně na něj dojde tehdy, když uživatel nemá představu o použitém hesle nebo když byl slovníkový útok bezúspěšný. Prolamovače v tomto případě postupují surově, když procházejí všechny myslitelné kombinace. Začínají u jednoho znaku (většinou "a") a řádně se prokousávají lesem znaků. Tato metoda logicky trvá mnohem déle. Když například postavíte proti devítimístnému heslu (rozšířená sada ASCII s 256 znaky) rychlý počítač (Pentium 4/2,5 GHz), zvládnete za sekundu okolo 25 milionů kombinací a máte přibližně 6 milionů let času, než prolamovač propočítá všechny kombinace. Ze statistického pohledu však už po 3 milionech let najde správné heslo. U druhé varianty, bruteforcemask (hrubá síla se zakrytím), uživatel předem zadá určitou hodnotu. To je ten případ, kdy si vzpomíná jen na jedno písmeno, jeden zvláštní znak nebo jednu číslici z hesla. Zjišťování pak běží o poznání rychleji.

PŘEPSÁNÍ HESLA: TAK SE DOSTANETE K CÍLI

Tento druh patří k nejméně ušlechtilým metodám vůbec a nefunguje vždy. Přesto se v praxi stále znovu stává, že se hesla v chráněných souborech dají bez problémů přepsat. Tímto způsobem se sice nedostaneme k heslu samotnému, k obsahu požadovaného souboru však ano. Pro tuto metodu existuje na internetu několik programů, které pracují spolehlivě.