Ochrana soukromých dat

Moderní **ŠIFROVACÍ POSTUPY** jsou považovány za bezpečné – přesto ani ony nedokáží vždy ochránit před zloději dat. Chip vám ukáže, jak šifrování funguje a kde jsou jeho skryté problémy…

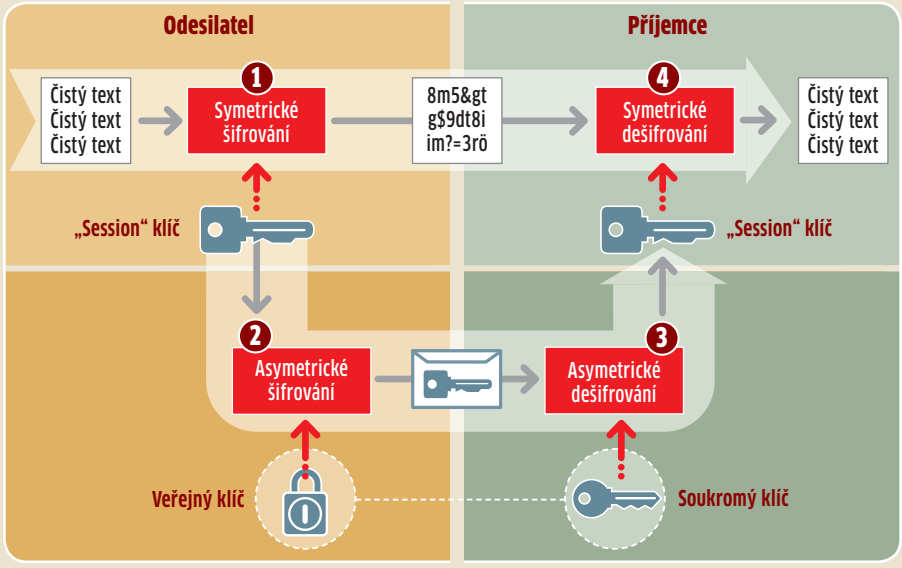
CLAUDIO MÜLLER

Krádeže dat jsou dnes na denním pořádku a neustále roste počet i význam hrozeb způsobených spywarem. Stále vyšší počet hesel, čísel kont a kreditních karet je „pod drobnohledem“ hackerů a internetové mafie. I proto se lidé bojí o bezpečnost svých osobních dat, která si ukládají na PC nebo která „prozradí“ prostřednictvím internetu nebo e-mailu.

Na to musí reagovat i bezpečnostní software. Nejnovější varianty komplexních nástrojů obvykle nechrání jen před viry a spywarem, ale pomocí šifrování zvolených informací také nabízejí ochranu před krádeží (a především zneužitím) dat, a to jak na pevném disku, tak i během komunikace na internetu. Ale stejně jako antivirové nástroje nemohou nabídnout stoprocentní ochranu před viry, nedokáží šifrovací nástroje zcela „zabezpečit“ vaše data. Obecně však platí, že čím složitější je použitá technologie, tím větší jsou nároky na úsilí vynaložené na její „cracknutí“. Zde tedy jde o souboj mezi vývojáři šifrovacích

Principy hybridního šifrování

Hybridní metody se skládají ze symetrické části pouze s jedním klíčem (session key) a asymetrické části s párem klíčů (veřejný/soukromý). ❶ Odesilatel zašifruje text „session“ klíčem ❷ a tento klíč pomocí veřejného klíče. ❸ Příjemce dešifruje pomocí soukromého klíče „session“ klíč a jeho pomocí poté i samotný text.



Ilustrace: Harald Fuchsloch

Šifrování v praxi

Když aktivně šifrujete data na disku nebo když posíláte e-mail – funguje to zcela automaticky, ať už na domácím počítači, nebo na internetu.

LOKÁLNÍ ŠIFROVÁNÍ
Programy pro zabezpečení dat na disku používají rychlé symetrické šifrování s jedním použitým klíčem, který zabezpečí přístup pouze jeho majiteli. Například oblíbený TrueCrypt (který najdete i na Chip DVD) používá tři algoritmy (AES, Twofish a Serpent), a to jak individuálně, tak pro data „kaskádovitě“. Lze také zvolit, zda nástroj zašifruje vybrané soubory, nebo celý disk.

E-MAILOVÁ KOMUNIKACE
Šifrování „poštovního provozu“ pracuje s hybridní technologií. Programy jako například GpG4win (opět i na Chip DVD) šifrují obsah e-mailu symetricky a samotný klíč asymetricky. Otevřený standard OpenPGP používá algoritmy IDEA nebo RSA.

SSL PROTOKOL
Známý SSL protokol (nebo jeho nástupce TSL) se používá k vytvoření bezpečného spojení do bank nebo internetových obchodů. Rozhodujícím činitelem je zde autentizační kontrola poskytovatele (viz rámeček na straně XX). Pokud stránka „projde“ kontrolou, protokol vytvoří hybridně šifrované spojení – data jsou šifrována symetricky (obvykle pomocí metod AES, DES a RC4) a klíče asymetricky (pomocí RSA).

WI-FI PŘIPOJENÍ
Starý standard WEP používá pro šifrování přenosu špatně implementovaný protokol RC4. Novější standard WPA2 používá vylepšený šifrovací protokol (CCMP) s bezpečným algoritmem AES, přičemž klíč je i nadále volitelný a je ukládán v konfiguraci routeru.

INTERNETOVÉ BANKOVNICTVÍ PŘES HBCI
Programy podporující HBCI (nebo jeho nástupce FinTS) šifrují zprávy pomocí symetrického klíče s využitím technologie 3DES. Samotný klíč je šifrován asymetricky s využitím RSA. Varianta s HBCI je v zahraničí používanou bezpečnější alternativou k běžnému internetovému bankovnictví.

metod a „crackery“ kódů. O tom, že tempo bitvy není malé, svědčí i skutečnost, že metody, které se před deseti lety považovaly za zcela bezpečné, jsou již překonány a v současnosti již představují riziko. Abyste se však sami mohli rozhodnout, jaké metody použijete, měli byste pochopit, jak šifrování funguje a jak se používá.

Klíč: Vodítko k textu

Neslabším místem kódování je klíč. Kerckhoffův princip, základní princip šifrování (neboli kryptografie), říká: Bezpečnost šifrovacích postupů je založena především na utajení šifrovacího algoritmu. Vývojáři tudíž v současné době své algoritmy zveřejňují, aby tyto postupy mohli analytici důkladně otestovat. Mezi známé výjimky patří například DRM (Digital Rights Management), sloužící k ochraně audiovizuálních děl: algoritmy jsou utajovány, ale ani ony nedokázaly odolat útokům hackerů.

Klíč je „nástroj“, který zašifruje originální data. Algoritmus upřesní způsob, jakým se tak stane. Existují dvě základní šifrovací metody: symetrická a asymetrická. Symetrická znamená, že ten samý klíč kóduje i dešifruje data (což lze přirovnat k zámku a odpovídajícímu klíči). V protikladu k tomu asymetrické šifrování používá rozdílné klíče pro šifrování a dešifrování.

Hybrid: Kódování ve dvou stadiích

Symetrické šifrování je bezpečné pouze do té doby, dokud uživatel ukládá kódovaná data pouze lokálně na harddisk a nikam je neposílá.

Výhoda: Běžné symetrické postupy fungují velmi rychle díky algoritmům, které jsou matematicky méně komplikované, a díky kratším délkám klíče. Nástroj TrueCrypt (na DVD) například zakóduje okolo 175 MB za sekundu.

Nevýhodou symetrických postupů je, že nejsou vhodné například pro přenos dat. Typickou ukázkou je zabezpečené internetové připojení. Ačkoliv pro každou session servery přiřadí nový, náhodný klíč (session key), komunikační partneři si klíč musí vyměnit také, aby byli schopni spojení „použít“. Pokud útočník tento klíč zachytí, dokáže komunikaci jednoduše dekódovat.

Asymetrické postupy řeší tento problém tak, že pracují s dvojicí klíčů. Odesilatel zakóduje data pomocí veřejného klíče, který příjemce již dříve se svým komunikačním partnerem sdílel. Takto se klíč určený k dekódování nedostane do špatných rukou. Na druhé straně uvolnění veřejného klíče nepředstavuje žádný problém, protože nede-

NAJDETE NA CHIP DVD

Šifrovací a bezpečnostní nástroje

CrypTool 1.4.21 ► nástroj pro analýzu zpráv

Gpg4win 1.1.4 ► šifrování nejen pro e-mail

KeePass 1.15 ► správce hesel

MegaWare Encrypter 3.0 ► výkonný šifrovací nástroj

Stegano32 ► skrývání dat do WAV a BMP souborů

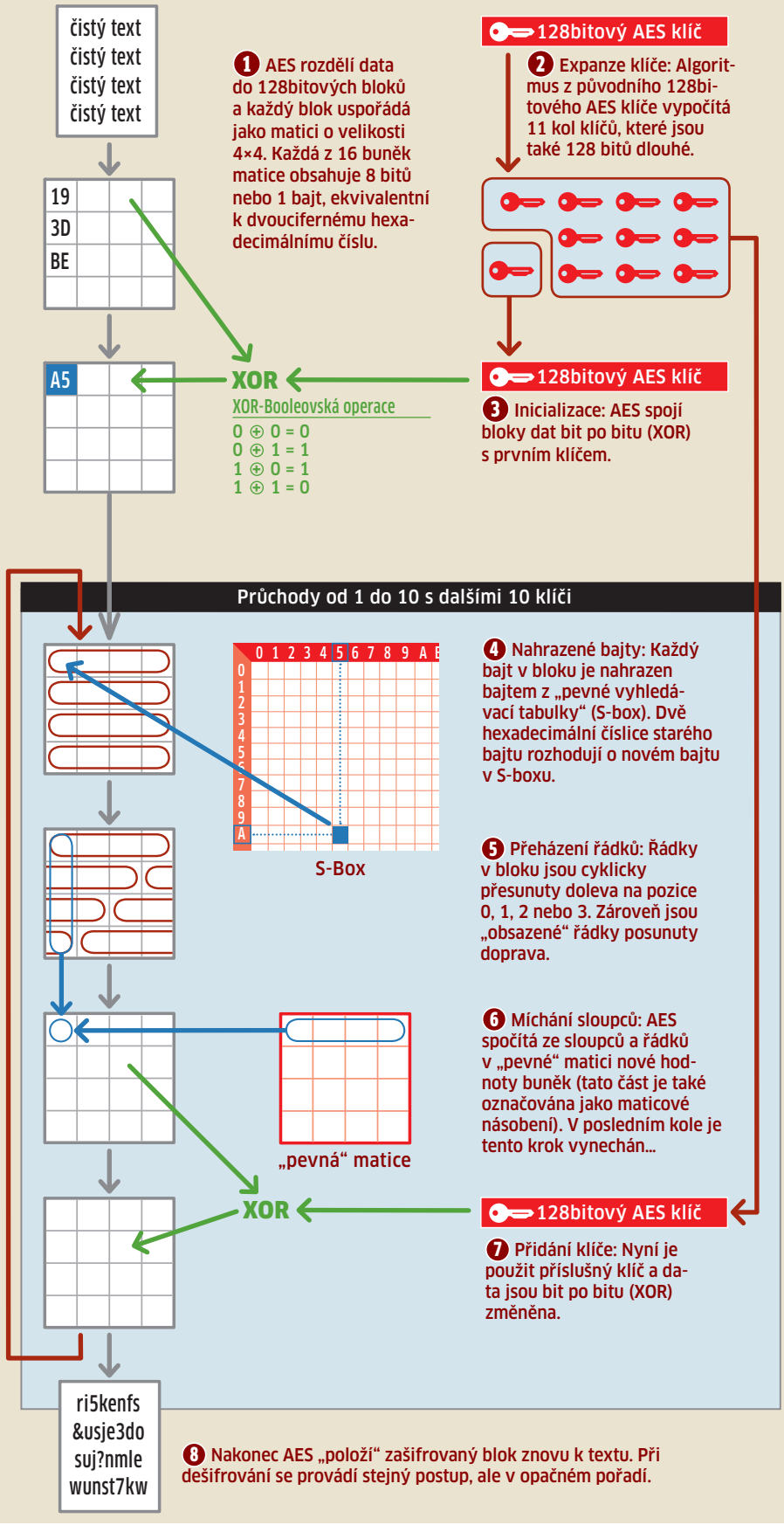
Steganos Safe One 10.0 ► zašifrování dat na disku

TrueCrypt 6.1a ► oblíbený šifrovací nástroj

► **NA DVD:** Programy k tomuto článku najdete na DVD pod indexem **ŠIFROVÁNÍ**

Jak funguje algoritmus AES

AES je posledním standardem pro symetrické šifrování. Data (levý sloupec) jsou šifrována vícestupňovým postupem, pomocí zvolných nástrojů (vpravo). V případě délky klíče 128 bitů (na obrázku) data projdou „mechanismem“ desetkrát.



kóduje žádná šifrovaná data a soukromý klíč z něho nelze odvodit. Veřejný klíč je jako visací zámek, pomocí něhož můžete zavřít dveře, ale ne je znovu otevřít. Tato metoda má však závažnou nevýhodu: asymetrické postupy šifrují asi tisíckrát pomaleji než postupy symetrické (především kvůli náročnějšímu výpočtu), proto nejsou vhodné pro větší objem dat.

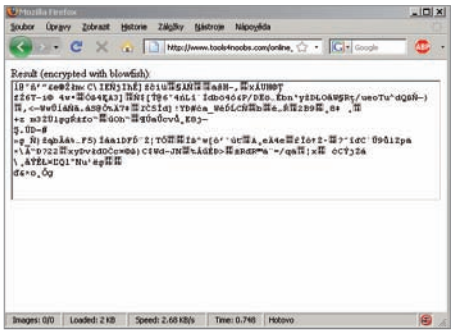
Z toho důvodu se v praxi používají hybridní (smíšené) postupy, např. pro přenos dat na webu, v e-mailovém styku či během on-line bankovnictví (viz obr. vlevo). Tato metoda kóduje skutečná data symetricky a klíč k datům asymetricky. Takový hybridní postup kombinuje bezpečnou výměnu klíčů a rychlé kódování dat.

Bit či blok: Otázka času

Další základní rozdíl v oblasti kryptologie je ten mezi šifrováním bloků či streamů. Bitové kódování dat (označované také jako streamové šifrování) je vhodné především pro přenosy v reálném čase – například v bezdrátových sítích. Výhodou je skutečnost, že šifrování začíná od prvního bitu a není nutné čekat na celý blok dat. To znamená, že tato technologie umožňuje šifrování (a přenos) bez časových ztrát. Navíc chyby neovlivní celý blok dat, ale jen jednotlivý bit. A nevýhoda? Streamové šifry nefungují s komplexním algoritmem a bezpečnost závisí především na implementaci softwarového prostředí.

Klasickou ukázkou problémů streamového šifrování může být například „starý“ Wi-Fi standard WEP (Wired Equivalent Privacy). Tento protokol řídí šifrovaný přenos ve Wi-Fi sítích a k tomuto účelu používá streamovou šifru RC4.

Princip: RC4 z klíče nejdříve vygeneruje řadu náhodných čísel mezi 0 až 255 (každé 8 bitů dlouhé). Tyto řady čísel pak spojí kousek po kousku (tedy přesněji bit po bitu) s originálními daty. Tento postup je obecně považován za relativně bezpečný, pokud klíč a jím vygenerované řady čísel použije pouze jednou. Na této podmínce ale WEP protokol vůbec nelpí. Aktuální klíč zahrnuje statický WEP klíč (uložený v konfiguraci routeru) a pseudonáhodný „session“ klíč (inicializační vektor). Problémem ale je, že při transportu dat se spolu s každým balíčkem dat přenáší i nezašifrovaný „session“ klíč. Doba výpočtu pro odvození statického klíče (většinou 40- či 104bitového) ze zakódovaného balíčku dat a ze známého inicializačního vektoru není příliš velká, dokonce i pro jednoduché počítače s patřičným nástrojem (jako je například Aircrack).



Originální a šifrovaný text: Existuje celá řada bezplatných internetových služeb, které pomocí vámi zvoleného hesla a metody zašifrují text. Příkladem mohou být weby **http://cybermachine.awardspace.com/encryption.php** nebo **www.tools4noobs.com/online_tools/encrypt/**.

Zmiňovaný nástroj potřebuje například v případě použití 40bitového klíče zachytit a analyzovat pouze okolo 5 000 „datových paketů" – což je záležitost v řádu minut.

Větší bezpečnost nabízejí šifry bloků, které se používají především pro šifrování v oblastech, které jsou méně časově „kritické" (jako jsou například data na disku nebo e-maily). Takové postupy rozdělují data do bloků a pro každý blok používají komplexní algoritmy.

DES: Inovační algoritmus

V roce 1977 zavedla americká vláda blokovou šifru DES (Data Encryption Standard), která je založena na Luciferově algoritmu, jako první veřejný standard pro symetrické šifrování. DES kóduje 64bitové bloky pomocí 56bitového klíče. Zde používaná Feistelova šifra rozděluje bloky do dvou polovin (L a R blok), každý blok po 32 bitech. Poté pomocí expanzivní permutace rozšíří R-blok na 48 bitů a spojí ho bit po bitu s 48bitovým klíčem vygenerovaným ze skutečného 56 bitového klíče. DES poté redukuje výsledný R-blok na 32 bitů a spojí ho bit po bitu s L-blokem. Tento postup se opakuje 16krát...

DES byl považován za bezpečný až do roku 1998, kdy superpočítač „Deep Crack" jako první hrubou silou „cracknul" DES klíč (důkladně přezkoušel všechny klíče) – za pouhých 56 hodin! Proto byl vyvinut 3DES (čili trojitý DES), který používá tři 56 bitové klíče a který se nyní používá například pro on-line bankovnictví nebo SSL spojení. Tyto tři klíče šifrují bloky dat jeden po druhém a navíc druhý klíč používá algoritmus obráceně (jakési dekódování). Tento postup se tedy nazývá EDE (Encrypt-Decrypt-Encrypt). Existuje ještě celá řada verzí DES, se kterými se však běžný uživatel až na výjimky nesetká (DESX v produktu pro šifrování pošty nebo crypt v unixových systémech).

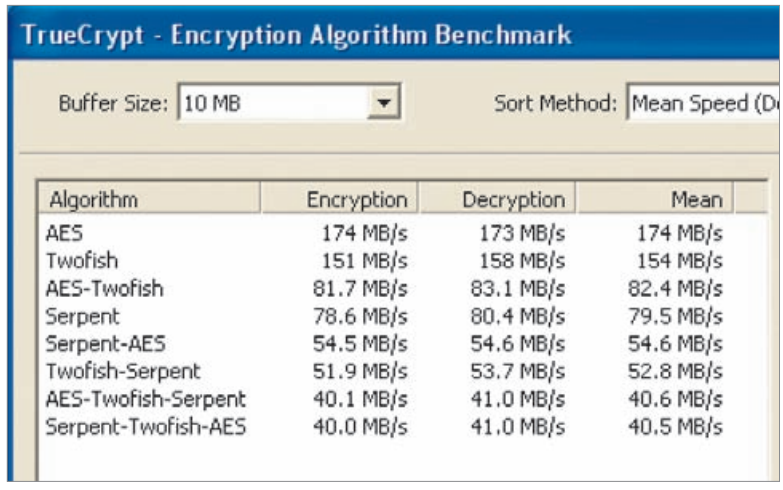
AES: Vlezlý standard

Ačkoliv je 3DES dodnes díky aktualizovanému klíči a upravenému algoritmu bezpečný, je také poměrně pomalý. A právě to byl důvod, proč AES (Advanced

Encryption Standard) nahradil v roce 2002 starší DES a stal se šifrovacím standardem.

AES je založen na Rijndaelově algoritmu a kóduje 128 bitové bloky dat pomocí klíčů s délkou 128, 192 a 256 bitů. Každý blok projde algoritmem 10, 12 či 14 kol, v závislosti na délce klíče (viz rámeček). Velkou výhodou v porovnání s technologií DES je jednoduchá implementace v softwaru i hardwaru, stejně tak i vysoká rychlost optimalizovaného algoritmu. Minimální délka klíče 128 bitů garantuje v nadcházejících letech bezpečnost před útoky hrubou silou. 128 bitů znamená, že existuje 2^{128} možných klíčů – číslo s 39 místy! A to je příliš dokonce i pro superpočítače současnosti – prakticky neexistuje možnost, aby důkladně odzkoušely všechny kombinace v reálném časovém intervalu. A právě proto je v praxi AES první volbou například při šifrování disku, SSL spojení nebo „nového" Wi-Fi standardu WPA2 – pomocí AES prý šifruje přísně tajná data dokonce i americká tajná služba NSA.

Rychle a bezpečně: Nástroj TrueCrypt zakóduje více než 170 MB za sekundu.



Algorithm	Encryption	Decryption	Mean
AES	174 MB/s	173 MB/s	174 MB/s
Twofish	151 MB/s	158 MB/s	154 MB/s
AES-Twofish	81.7 MB/s	83.1 MB/s	82.4 MB/s
Serpent	78.6 MB/s	80.4 MB/s	79.5 MB/s
Serpent-AES	54.5 MB/s	54.6 MB/s	54.6 MB/s
Twofish-Serpent	51.9 MB/s	53.7 MB/s	52.8 MB/s
AES-Twofish-Serpent	40.1 MB/s	41.0 MB/s	40.6 MB/s
Serpent-Twofish-AES	40.0 MB/s	41.0 MB/s	40.5 MB/s

RSA: Bezpečná výměna klíčů

Pouze asymetrické postupy, které používají asymetrické šifrování klíčů, dokáží zabezpečit bezpečný přenos symetricky šifrovaných dat. Standard RSA (pojmenovaný po autorech Rivest, Shamir a Adleman) zabezpečuje klíč pro výměnu dat na internetu (SSL), on-line bankovnictví nebo šifrování e-mailů. Bezpečnost RSA je založena na skutečnosti, že není znám výpočetní algoritmus, který by jednoduše dokázal velká čísla rozložit na prvočísla.

Uživatel, který chce obdržet šifrovaná data, vytvoří pár klíčů (veřejný soukromý klíč). Veřejný klíč tvoří dvojici čísel (e, N) a soukromý klíč dvojice čísel (d, N). N je součin dvou náhodně vybraných prvočísel, e (šifrovací klíč) celé číslo zvolené v určitém limitu a d (dešifrovací klíč) se počítá s využitím hlavních prvočísel e a N. Původní data jsou šifrována pomocí matematické operace na bitové úrovni. Potencionální útočník potřebuje pro dešifrování číslo „d", tedy prvočíslo z N. To ale není možné získat bez více informací. Útočník sice může použít k získání prvočísel metodu „pokus a omyl" – v případě nižších hodnot N. Například pro hodnotu N = 143 mohou být činitele 11 a 13. Ale RSA používá 1024- nebo 2048bitové číslo (309 nebo 617 míst), což zajišťuje, že jsou podobné pokusy nereálné...

Odborníci odhadují, že při současném nárůstu výpočetního výkonu počítačů bude v blízké budoucnosti možné, aby špičkové týmy luštily zprávy šifrované pomocí RSA s klíčem 512 bitů, při volbě dalšího klíče je bezpečnost zaručena ještě delší dobu. Jediným potenciálním nebezpečím budoucnosti by mohl být vývoj kvantových počítačů.

Volba RSA, AES nebo DES: Šifrovací metody nefungují jako nezávislé programy, ale jsou v programech implementovány (například pro šifrování dat na disku) nebo používány v přenosových protokolech (internet, WiFi, e-mail). Ve většině případů si tedy uživatel nemůže přímo vybrat šifrovací metodu, což ale příliš nevadí, protože používané „postupy" jsou relativně bezpečné...

Hesla: Nejslabší článek řetězu

Jaké jsou aktuální možnosti útočníků při „crackování" dat? Obecně vzato existují tři místa, na která mohou zaútočit: klíč, kterým se data šifrují, prostředí (programy, protokoly), do kterých je algoritmus integrován, a hesla, která zabezpečují klíč (například v programech pro šifrování disku). Nejjednodušší cestou je obvykle útok na heslo s použitím „hrubé síly" – při tomto typu útoku útočník jednoduše vyzkouší všechny kombinace znaků. Ve většině případů je počet možných znaků hesla omezen, a tak je možné u jednodušších aplikací touto metodou zjistit heslo během několika minut. To znamená, že pokud uživatel použije „slabé" heslo, jsou i nejlepší algoritmy k ničemu. Obzvláště snadno odhalitelná jsou hesla typu „heslo" nebo „123456". Dalším typem je „slovníkový" útok, kde hacker nezkouší náhodné shluky hesel, ale testuje jejich „pravděpodobné kombinace".

Na druhou stranu – v programech typu TrueCrypt je doporučeno používat hesla o délce 15 až 20 znaků, obsahující kombinaci čísel, písmen a speciálních znaků. Takové heslo není možné v reálném časovém horizontu odhalit „hrubou silou" ani při použití superpočítačů (viz tabulka vlevo).

Hrubá síla: Nekonečné počítání

Samotná metoda útoku „hrubou silou" na šifrovací techniky je předem odsouzena k nezdaru. Všechny moderní postupy totiž používají klíče o délce minimálně 128 bitů, kde je množství kombinací tak velké, že i pro superpočítače zvládající 80 miliard klíčů za sekundu jde o úkol na triliony let. I přesto zde ale existuje nedůvěra: metodu s použitím „hrubé síly" lze přirovnat k loterii. Ačkoliv obrovské množství kombinací prakticky vylučuje rychlé nalezení klíče, teoreticky na něj lze narazit po několika sekundách. To znamená, že ani dlouhý klíč nezaručí stoprocentní bezpečnost...

AUTOR@CHIP.CZ

BEZPEČNÉ ŠIFROVÁNÍ A DÉLKA HESLA

Bezpečnost šifrovacích algoritmů závisí na délce hesla a klíče. Například superpočítač Copacobana dokáže vyzkoušet 65 miliard kombinací za sekundu

HESLO	PROLOMENO ZA
Zjovned	0,12 sekund
Pzg1/9}gh87&gtv	33 let
ŠIFROVÁNÍ	**PROLOMENO ZA**
56 bit klíč (např. DES)	12,4 dne
128 bit klíč (např. AES)	166 000 000 000 000 000 000 let