TrueCrypt

Aby byla vaše data v bezpečí

(CD)

KAREL ŠREDL

Opět vás po pravidelné měsíční pauze vítám u dalšího Rychlokurzu. Dnes si nastavíme laťku poněkud výše než obvykle. Představovaný program bude na první pohled vypadat možná složitě, ale uvidíte, že práce s ním je vlastně jednoduchá a časem se bez něj neobejdete. Dovolte mi představit program TrueCrypt.

První důležitá informace: TrueCrypt je zcela zdarma. Co vlastně umí? Umožňuje vytvořit šifrovaný soubor, který pak připojíte do systému jako virtuální disk a pracujete s ním jako s jakýmkoli normálním diskem. Můžete dokonce zašifrovat celý diskový oddíl nebo třeba celou USB klíčenku. Pokud při připojování disku zadáte správné heslo, máte ho plně k dispozici a ani nepoznáte, že se od jiných disků na vašem počítači nějak liší. Dokonce na něm můžete spouštět třeba defragmentaci nebo v něm vytvářet další šifrované disky. Pokud však své šifrované úložiště odpojíte, rázem se k vašim datům nikdo nepovolaný nedostane. Proto je důležité zapamatovat si heslo! Jestliže jej zapomenete, vaše data budou nedostupná i pro vás!

Jak na to

Předvedeme si jedno vzorové použití. Koupili jsme si USB klíčenku a chceme na ní umístit nejen své dokumenty, ale i některé aplikace (e-mailový klient, ICQ klient, apod.). Pokud bychom snad klíčenku ztratili, rozhodně nechceme, aby se k datům dostal někdo nepovolaný. Nyní si představíme řešení, které sám dlouhou dobu používám.

Na klíčenku nahrajeme TrueCrypt a celý zbytek prostoru na klíčence vyhradíme pro zašifrovaný disk. Ke svým datům se pak dostaneme tak, že klíčenku připojíme k USB portu a v Průzkumníku TrueCrypt spustíme. S jeho pomocí připojíme zašifrovaný soubor k systému jako virtuální disk a pak už můžeme pracovat se svými daty a aplikacemi. Na konci práce pak šifrované úložiště a následně i USB klíčenku ze systému odpojíme. Naše data budou opět v bezpečí.

Jak tedy na to? Nejprve na klíčenku zkopírujeme TrueCrypt. NA NAŠEM CD najdete archiv ZIP. Ten obsahuje instalační soubor *TrueCrypt setup.exe* a dále pak adresář nazvaný *Setup Files*, v němž jsou soubory potřebné k běhu programu. Pokud tedy chcete provozovat TrueCrypt nezávisle na systému (v tzv. *Traveller modu*), stačí pouze překopírovat soubory ze zmíněného adresáře na cílové místo, v našem případě na USB klíčenku. Instalace pak není zapotřebí.

V klíčence spusťte program dvojitým kliknutím na *TrueCrypt.exe*. Objeví se hlavní okno, jež obsahuje seznam neobsazených písmen pro diskové jednotky a několik „akčních" tlačítek. Nás teď bude nejvíc zajímat tlačítko *[Create Volume]* (Vytvořit jednotku).

Vytvoření šifrovaného disku

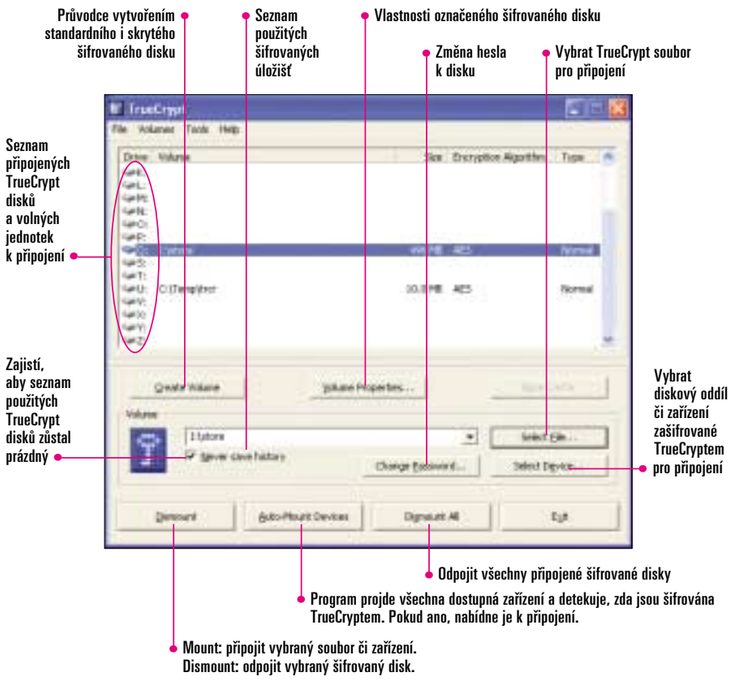
Po kliknutí na tlačítko [Create Volume] se spustí průvodce, který vás krok za krokem provede procesem vytvoření šifrovaného úložiště. V prvním okně se průvodce ptá, zda chcete vytvořit standardní TrueCrypt disk (Create a standard TrueCrypt disk), nebo tak zvaný Hidden disk. Co je Hidden disk a jaké jsou jeho výhody si povíme na konci článku. My si zvolíme první volbu – standardní disk – a stiskneme tlačítko [Next>].

V druhém kroku se nás průvodce zeptá, kam chceme disk umístit. I zde máme dvě možnosti: *[Select Device]* umožňuje zašifrovat celý diskový oddíl (nebo např. celou USB klíčenku). Pro nás se však tato volba nehodí, protože na klíčence potřebujeme mít i nešifrovaná data – vlastní program TrueCrypt. Proto zvolíme druhou možnost, a to vytvoření šifrovaného úložiště ve formě souboru. Stiskněte tedy tlačítko *[Select File]* a v dialogovém okně určete, kde chcete soubor vytvořit, a zadejte jeho jméno. Pak klikněte na tlačítko *[Otevřít]*. V průvodci se objeví námi zvolená cesta a jméno souboru. Kliknutím na *[Next>]* přejdeme k dalšímu kroku.

Nyní určíme způsob, jak budou naše data šifrována. K dispozici je celá řada šifrovacích algoritmů. Já osobně preferuji *AES* či *TwoFish* (jsou to poměrně nové a moderní šifry) nebo *BlowFish* (poněkud starší šifra z roku 1993, avšak nejrychlejší z nabízených). Při rozhodování vám může pomoci tlačítko *[Benchmark]*. Klikněte na něj a v dialogovém okně stiskněte znovu *[Benchmark]*. Po chvilce se před vámi objeví seznam šifer s rychlostmi, jakými probíhá šifrování právě na vašem systému. Okno benchmarku zavřete pomocí *[Close]*. Benchmark můžete spustit i samostatně, a to přes menu *Tools >> Benchmark*.

Dejme tomu, že použijeme šifru AES. Kliknutím na *[Next>]* se přesuneme do dalšího okna. Sem zapište velikost vašeho úložiště. V našem případě chceme využít co největší zbylý prostor na USB klíčence, a proto do vstupního pole opište hodnotu z řádku *Free\space on drive F: is* (například) *508 MB*, tedy že na úložišti (disku F) je 508 MB volného místa. Potom klikněte na *[Next>]*. (Malé upozornění – souborový systém FAT32 umí vytvořit soubor o maximální velikosti 4 GB, a proto ani vaše úložiště na takovém disku nemůže být větší. V takovém případě musíte přejít na NTFS.)

V dalším kroku zadáme do obou polí heslo. Pokud má mít šifrování nějaký smysl, musí být heslo alespoň 10 znaků dlouhé (autoři říkají 20) a mělo by obsahovat velká i malá písmena, číslice a speciální znaky. Návodům, jak vytvořit zapamatovatelné silné heslo, jsme se v Rychlokurzu věnovali již několikrát. Takové vzorové heslo je např. *Kock@L*z*D1r@u*, naopak snad nejhorší heslo je „heslo". Na to, že heslo je „slabé", vás program upozorní. Pokud se tak stane, stiskněte *[Ano]* a program vám dovolí pokračovat dál.



V dalším kroku volíte souborový systém, který chcete používat na svém šifrovaném disku. Vyberte kterýkoli – já bych doporučil NTFS. Obsah šifrovaného disku můžete později formátovat na jakýkoli jiný souborový systém. Klikněte tedy na tlačítko *[Format]*. Proběhne vytváření disku (což může nějakou dobu trvat) a na konci vám TrueCrypt oznámí výsledek. Stiskněte *[Next>]* a pokud nechcete vytvářet nějaké další úložiště, stiskněte *[Cancel]*.

Nyní je šifrované úložiště vytvořené, zbývá ho připojit jako disk a začít používat.

Připojení disku a použití

Jak tedy připojit soubor šifrovaného úložiště jako disk? V hlavním okně TrueCryptu označte písmenko, pod kterým chcete šifrovaný disk připojit (třeba W:). Kliknutím na *[Select File]* – pokud máte šifrovaný disk jako soubor, nebo *[Select Device]* – pokud je zašifrovaný celý disk, vyberte šifrovaný soubor či diskový oddíl. V našem případě to bude soubor na USB klíčence. Potom klikněte na *[MOUNT]* (Připojit). Budete dotázáni na heslo. Zadejte jej a klikněte na *[OK]*. Pakliže vše proběhlo v pořádku, objeví se v systému nový virtuální disk W:. Od této chvíle ho můžete používat jako jakýkoli jiný disk. Uložte na něj své dokumenty či oblíbené aplikace (takové, které nepotřebují instalaci a neukládají svá data do registru). Seznam vhodných aplikací najdete na konci článku.

Po připojení disku můžete hlavní okno TrueCryptu zavřít. Vaše šifrované disky zůstanou stále připojeny. Program spustíte, až když budete chtít disky zase odpojit.

Odpojení disku

Až budete chtít práci s diskem ukončit a svá data opět znepřístupnit, stačí spustit TrueCrypt, kliknout na písmeno disku a pak na *[DISMOUNT]* (Odpojit). Více disků najednou odpojíte kliknutím na *[DISMOUNT ALL]* (Odpojit vše). Pokud se při této činnosti objeví hlášení Volume contains files being used by application or system, znamená to, že nějaká aplikace data z disku stále používá. Prověřte tedy, zda na disku nemáte spuštěnou nějakou aplikaci či nemáte otevřený dokument. Pokud ne, pak na otázku *Force dismount* odpovězte *[Ano]*.

Důležité!

Vzhledem k tomu, že data jsou na zašifrovaném disku vzájemně provázána, jakákoli chyba na disku způsobí nejen nečitelnost postiženého sektoru, ale i nečitelnost všech sektorů na něm závislých. V nejhorším případě (při poškození sektoru v hlavičce) bude nečitelný celý disk. Proto si zapamatujte dvě zásady, které jsou více než důležité:

1. Vždy odpojujte šifrovaný disk korektně (přes aplikaci TrueCrypt). Máte-li třeba zašifrovaný USB disk, nikdy jej za běhu nevytahujte. Nejprve softwarově odpojte zašifrovaný disk a následně odpojte USB disk přes volbu systému Windows *Bezpečně odebrat zařízení*.
2. Zálohujte! Zálohujte vždy a co nejčastěji. Není to jen fráze – z vlastní zkušenosti mohu potvrdit, že ztráta několika gigabytů důležitých dat opravdu bolí.

Tipy a triky

Chcete pracovat s TrueCryptem efektivněji? Pak vám nabídnu několik triků:

1. **Rychlé připojení disku** pomocí parametrů předaných TrueCryptu prostřednictvím příkazové řádky.

Vytvořte zástupce souboru *TrueCrypt.exe* (klikněte na něj pravým tlačítkem a zvolte *Vytvořit zástupce*). Na zástupce opět klikněte pravým tlačítkem a zvolte *Vlastnosti*. V políčku *Cíl*, kde vidíte cestu k programu, vepište např. následující parametry:

F:\TrueCrypt.exe /v <<cesta_k_šifr_ulozisti>> /letter <<pismeno_jednotky>> /beep /cache n /mountoption rm /a /q

kde <<cesta_k_šifr_ulozisti>> bude kompletní cesta k souboru se šifrovaným úložištěm (např. *F:\uloziste*) a <<pismeno_jednotky>> bude pismeno, pod kterým chcete disk připojit (např. *Q*). Výsledek tedy může vypadat takto:

F:\TrueCrypt.exe /v F:\uloziste /letter Q /beep /cache n /mountoption rm /a /q

Stiskněte *[OK]* a nakonec tohoto zástupce přejmenujte – např. na *Připojit Q.lnk*. Pokud takovéhoto zástupce spustíte, budete pouze vyzváni k zadání hesla a soubor se automaticky připojí jako disk Q.

2. **Rychlé odpojení disku.** Stejným způsobem lze vytvořit zkratku pro rychlé odpojení šifrovaného disku Q. Postupujte jako v předchozím případě, ale do kolonky *Cíl* vepište **F:\TrueCrypt.exe /d Q /q**. Po spuštění tohoto zástupce bude disk Q automaticky odpojen.

Další informace

- Jak již jsme se zmínili, TrueCrypt umí pracovat ve dvou modech. V prvním (námi popisovaný případ) jsou šifrovaná data umístěna na disku jako obyčejný soubor a vztahují se na ně veškerá omezení použitého souborového systému (např. u FAT32 je to omezení velikosti souboru na 4 GB). Ve druhém modu TrueCrypt dokáže zašifrovat celý diskový oddíl či disk (ale také disketu, USB klíčenku, ZIP disk, apod.). V tomto modu nás omezují pouze vlastnosti systému Windows XP.
- Pokud stále ještě používáte Windows 98/ME, pak vězte, že poslední verze TrueCryptu, schopná pod těmito systémy pracovat, je TrueCrypt 1.0. Osobně jsem jej pod Windows 98/ME nikdy neprovozoval a tudíž se nemohu podělit o jakékoli zkušenosti.
- Program pamatuje i na situaci, kdy vás někdo může násilím donutit k prozrazení hesla. Pro takový případ vám TrueCrypt nabízí možnost vytvořit tzv. *Hidden disk* (něco jako tajná zásuvka v tajné zásuvce). Ve vašem šifrovaném úložišti použije část volného prostoru k vytvoření „skrytého" disku s vlastním přístupovým heslem. Podle toho, jaké při připojení zadáte heslo, se buď objeví data ze standardního úložiště nebo ze skrytého. Do standardního úložiště lze tedy umístit nějaká bezvýznamná data, do skrytého pak data přísně tajná. Způsob, jak zjistit, zda se v šifrovaném úložišti nachází další skrytý disk, neexistuje.

Koncept skrytého disku má však jednu zásadní „vadu": protože skrytý disk používá pro svá data volné místo z disku standardního, může se stát, že pokud standardní šifrovaný disk zcela zaplníte, data z disku skrytého zničíte! Vyplývá to z principu fungování skrytého disku. Pamatujte na to a ponechte si vždy dostatek volného místa. A kromě toho zálohujte, zálohujte, zálohujte.

Skrytý disk vytvoříte obdobným způsobem jako obyčejný, jen na první otázku průvodce odpovíte, že chcete *Create hidden True Crypt Volume*. V dalším okně pak uvidíte dvě volby: *Create a TrueCrypt volume and then a hidden volume within it* (Vytvořit TrueCrypt disk a následně v něm vytvořit skrytý disk) a *Create a hidden volume within a existing TrueCrypt volume* (Vytvořit skrytý disk v již existujícím TrueCrypt disku). Překlad myslím dostatečně vystihuje, kdy kterou volbu použít. Pozor! Hidden disk lze (myslím prozatím) vytvořit pouze v standardním TrueCrypt disku se souborovým systémem FAT.

Aplikace vhodné pro přenosný disk

Nakonec ještě slíbený krátký seznam aplikací, které můžete používat na vašem kryptovaném USB disku. Nevyžadují instalaci a pokud možno nepoužívají pro ukládání dat registr. Některé potřebují, aby byl šifrovaný disk připojen pod určitým písmenem – což lze většinou snadno zaručit (já používám písmeno P:, protože je málokdy obsazené).

- **Souborový manager:** Total Commander (shareware).
- **E-mailový klient:** FoxMail, Portable Mozilla Thunderbird, PopCorn (vše free).
- **Browser:** Portable Mozilla FireFox (free), Opera (adware, obsahuje i e-mailového klienta a spoustu dalších specialit).
- **Instant messaging klient:** Miranda (free, protokoly ICQ, MSN, Jabber a mnoho dalšího)
- **Textový editor:** SciTe, PSPad (free).
- **FTP server:** EFTP (free).

Závěr

Tentokrát jsem vám odhalil jedno ze svých soukromých es (domnívám se, že to z článku bylo dostatečně cítit). Ačkoli TrueCrypt vypadá na první pohled složitě, nic složitého na něm není. Věřím, že si ho oblíbíte stejně jako já.

URL: ruecrypt.sourceforge.net 5 0245/0K ❑