Šifrování USB flash disků zdarma

Během několika let se flash disky staly z novinky už běžnou a přijatelně levnou záležitostí. Dokonce je už velmi vhodné uvažovat o změně zálohovacích médií z pásek na tyto disky, alespoň u malých a středních firem. Ještě před několika lety by to bylo bláznivým luxusem, dnes možná levnější varianta a v budoucnu třeba standardní médium. Zálohování na flash discích se rozmáhá u malých firem, živnostníků nebo v domácích počítačích. První z autorů například disponuje USB flash diskem na klíčence (v ceně cca 1000 Kč) s kapacitou 4 GB, kde zálohuje práci za běžný rok i archivní data. Data jsou vždy k dispozici a chráněná „vlastním tělem". Nicméně pro případ, kdy bychom klíče i s flash diskem ztratili nebo si je někdo „vypůjčil", musíme je mít ochráněna šifrou.

Tabulka 1 Výběr programů pro šifrování disků zdarma a s veřejnými zdrojovými kódy

Název	Vývojář	Rok	Operační systém
loop-AES	Jari Ruusu	2001	Linux 2.0+
CGD	Roland C. Dowdeswell	2002	NetBSD 2.0+
GBDE	Poul-Henning Kamp	2002	FreeBSD 5.0+
TrueCrypt	TrueCrypt Foundation	2004	Linux 2.6, Windows NT-based
dm-crypt/cryptsetup	Christophe Saout	2004	Linux 2.6 Windows NT-based
dm-crypt/LUKS	Clemens Fruhwirth (LUKS)	2005	Linux 2.6 Windows NT-based
FreeOTFE	Sarah Dean	2004	Windows NT-based, Pocket PC
GELI	Pawel Jakub Dawidek	2005	FreeBSD 6.0+
Scramdisk 4 Linux	Hans-Ulrich Juettner	2005	Linux 2.4–2.6

Kvalitně a bez zadních vrátek

Ochrana dat se netýká jen USB flash disků, ale pevných disků, pamětí v mobilních zařízeních a telefonech apod. Je to celá oblast, kde dnes vznikají a kam se skutečně přesouvají důležitá data. Řada ze šifrovacích programů, které šifrují flash disky, má širší záběr. Budeme hovořit o jednom mimořádném programu (TrueCrypt), který je k šifrování těchto médií určen, je zcela zdarma a byl navržen profesionálními kryptology. Navíc je přátelský a je možné ho používat intuitivně bez studia manuálu. Pro pořádek dodejme, že podobných programů je více a neměli jsme možnost je zkoumat všechny a porovnávat je, i když by to byla velmi záslužná činnost. Uvádíme jen několik z nich, které jsou zdarma a jejichž zdrojové kódy jsou veřejné. Další (včetně komerčních programů) naleznete např. v *tabulce 1* nebo v [2].

Jak program TrueCrypt šifruje

TrueCrypt může šifrovat celé partition nebo vytvářet šifrované logické disky určité velikosti na různých médiích. My jsme konkrétně měli k dispozici 4GB USB flash disk, na němž jsme vytvořili šifrovaný virtuální disk o velikosti 3 GB. K šifrování je možné si zvolit blokovou šifru AES, Twofish nebo Serpent nebo zřetězení dvou nebo tří z nich. Označme E zvolenou blokovou šifru (nebo zřetězení dvou nebo tří), její klíč K1 a přídavný klíč K2 (128 bitů). Šifrovaný disk je tvořen jedním souborem, který obsahuje hlavičkuTrue Cryptu a pak šifrované sektory logického disku, které dodává operační systém (Linux, Windows). Hodnoty K1 a K2 jsou vygenerovány pomocí generátoru náhodných znaků při vzniku disku a jsou uloženy do hlavičky tohoto souboru, hlavička je zašifrována pomocí náhodné soli a passwordu uživatele. Logický disk je šifrován po 128bitových blocích P_i, kde *i* je 128bitový index, v tzv. modu LRW odděleně a jiným klíčem (!): $C_i = E_{K1}(P_i \oplus (K2 \otimes i)) \oplus (K2 \otimes i)$. Klíč K2 je pro kaž-dý blok modifikován indexem *i*, přičemž K2 ⊗ i je násobením dvou 128bitových hodnot v jistém Galoisově tělese GF(2^{128}), viz ST 7/2007.

LRW nahradí CBC

Uvedený způsob šifrování se nazývá modus Liskov-Rivest-Wagner a byl navržen před pěti lety. LRW má vlastnost, že když útočník vymění dva bloky šifrovaného disku, rozšifrují se náhodné nesmysly, neboť každý blok je šifrován jiným klíčem. Ještě před několika lety se takové šifry nepoužívaly a útoky výměnou nebo manipulací šifrovaných bloků byly možné. I v nejrozšířenějším modu šifrování CBC jde totiž s bloky cíleně manipulovat, o heslových modech nemluvě. Proto se v moderních šifrovacích programech pro šifrování disků přechází právě na modus LRW (TrueCrypt, dm-crypt, Scramdisk).

Vše chrání password

Protože použité blokové šifry jsou kvalitní a jejich klíče náhodné a dostatečně dlouhé, nezbývá žádný jiný útok než útok hrubou silou na nejslabší místo – password. Proti útoku hrubou silou jsou password a sůl zpracovány složitou funkcí PBKDF2 podle normy PKCS#5 v.2.0, která použije dvatisícekrát opakované hašování za sebou, aby se zkoušení passwordů hodně protáhlo. Navíc je tu možnost zvolit si tzv. klíčový soubor, což je jakýkoliv běžný soubor, který se nachází na disku a který označíme. Je to sice veřejný soubor, ale podstata spočívá v tom, že modifikuje password. (Modifikace není bohužel tak silná jako modifikace solí.) Můžete si ho také nechat naplnit náhodnými znaky od TrueCryptu. Případný útok na password musí vždy kromě soli a passwordu zpracovat ještě tento přídavný soubor. Pokud máte kvalitní password, nemusíte tento klíčový soubor používat. Pokud nemáte kvalitní password, klíčový soubor vás nemusí zachránit. Proto toto opatření považujeme spíše za kosmetické a silně doporučujeme používat kvalitní password. Navíc doporučujeme si na USB flash disku nechat nějaký nešifrovaný prostor. Ten využijete pro ukládání dat v případech, kdy nemůžete zadávat cenný password (například jsou kolem další osoby apod.) a přitom potřebujete uložit či předat nějaká data.

Pozoruhodná kvalita

Cílem článku nebylo popsat všechny možnosti programu TrueCrypt, jen vypíchnout podstatné. Čtenáři, které tento program zaujme, si mohou projít manuál nebo rozsáhlé a technicky orientované diskusní fórum na internetu. Především je však třeba říci, že program vychází z prací skupiny uznávaných kryptologů, o jejichž kvalitách není pochyb. Ostatně vidíte sami, že šifrovací systém je průzračný, jednoduše popsatelný a přitom silný. Další podstatnou vlastností je dostupnost a veřejnost zdrojových kódů a dokumentace a možnost použití programu a ostatních zdrojů zcela zdarma. Na závěr ještě přece jen malý dodatek – nemůžeme vyloučit, že někde v programu není chyba nebo že nebude objevena nějaká bezpečnostní vada, jako tomu například bylo u Schneierova programu Password Safe (byla to pouze vada na kráse, nikoli devastující chyba). Avšak z návrhu a všech informací kolem máme velmi dobrý pocit důvěry ve správnost realizace všech bezpečnostních funkcí tímto programem.

Závěr

TrueCrypt je výjimečný program jak svojí kvalitou, tak uživatelsky. Navíc je zcela zdarma k dispozici všem, kdo mají zájem chránit si silnou šifrou data na přenosných médiích, například stále populárnějších a cenově dostupnějších USB flash discích.

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

LITERATURA

[1] Domácí stránka projektu TrueCrypt: http://www.truecrypt.org/

[2] Porovnání programů pro šifrování disků, http://en.wikipedia.org/wiki/Comparison_of_disk_encryption_software