Közösen használt fájlrendszerek titkosítása

Mick a BestCrypt nevű nyílt forrású alkalmazást fogja megvizsgálni, amely titkosított kötetek Windows- és Linux-felületek közti megosztását teszi lehetővé.

A személyi titkosítás szószólói számára az idei március fekete hónap volt. A Network Associates hivatalosan bejelentette, hogy felhagyott a PGP Desktop (minden számítógépre külön telepített titkosítási eszköz) támogatásával – egyszerűen szólva ez a manapság használatban lévő legnépszerűbb, legérettebb, és leghasználhatóbb végfelhasználói titkosítási eszköz. Kimondhatatlanul nehezen viselem, ha egy kereskedelmi termék nagyszerűségét kell elismernem egy ingyenes termékkel szemben, jelen esetben a PGP termékéét, miközben az bár távolról sem tökéletes, mégis a legjobbak az esélyei, hogy a nagy hatékonyságú titkosítást a felhasználók sokaságához eljuttassa.

A világnak jó titkosítási módszerekre van szüksége, különösen olyan jó minőségű titkosítási eszközökre, amelyeket idő- és emberi erőforrástakarékos grafikus felülettel láttak el. Senki sem húz hasznot a PGP Desktop piacának megüresedéséből, ez azonban leginkább a kötelező érvényű választási lehetőségek hiánya miatt alakult így.

Egyik program sem kívánja semmilyen módon kisebbíteni ***Werner Koch*** és a GnuPG-csapat csodálatra méltó munkáját, akiket lapunk korábbi számaiban már elárasztottam szívből jövő elismerésemmel. A GnuPG hihetetlenül rövid idő alatt megbízható és érett alkalmazássá fejlődött, és máris elfoglalta az őt megillető helyet az olyan létfontosságú eszközök körében, amelyek minden Linux-változatban szerepelnek. A Linux-hívők már megszerették a GnuPG-t, barátkozz meg vele te is! Sajnos grafikusfelület-központú világunkban a GnuPG különböző felületei igazi erejét még fel kell ismerni, mielőtt igazán azt remélhetnénk, hogy a mindennapi felhasználók is készek lesznek elfogadni a GnuPG-t. Amennyiben a nem szakmai felhasználók számára ezt az utat nem tudjuk biztosítani, akár el is felejthetjük a nagy hatékonyságú titkosítás eljuttatását a felhasználók tömegeihez, még akkor is, ha ingyenesen történik. A használhatóság szempontjából a GnuPG a Linuxszal a legtágabban vett értelemben osztozik – de ó jaj, itt jön az az átkozott levelezés!

Sőt, a GnuPG a PGP Desktop működési területének csak egy részét célozza meg. Miközben a GnuPG többek között pótolja a PGP Desktop elektronikus levelezési és állománytitkosítási szolgáltatásait, nem végez állományrendszer-titkosítást, amely a legjobb szolgáltatás volt a PGP Desktop programban. A PGPdisk – a PGP állományrendszert titkosító segédprogramja – a titkosítási folyamatot egyszerűvé, gyorssá és átláthatóvá tette.

Az egyetlen dolog, amit nélkülözni volt kénytelen, az a Linux-rendszerben használható ügyfélprogram. Jómagam is – mint hordozható számítógépén két operációs rendszert üzemeltető felhasználó – ezt mindig csalódást keltőnek tartottam: egy hordozható számítógépnek minden operációs rendszerben, amelyet csak képes betölteni, titkosítással kell rendelkeznie – nincs mese!

Természetesen Linux-rendszeremre telepíthetek egy visszacsatolt titkosított állományrendszert, csakhogy az operációs rendszerek közötti átjárhatóságot ez még mindig nem teszi lehetővé. Jobb egyetlen titkosított lemezrészt megosztani a két környezet között, mint két külön környezetet fenntartani.

Ez a felvetés, ha mégannyira közvetve is, e havi témánkhoz repít bennünket, ami már nem a PGP, de még csak nem is a GnuPG: ez a BestCrypt, a nyílt forrású kereskedelmi program, amely titkosított kötetek megosztását teszi lehetővé Windows- és Linux-rendszerek között – a PGPdisktől megszokott átláthatósággal, egyszerűséggel és gyorsasággal.

Áttekintés

A BestCrypt állományrendszer-titkosító segédprogram, amellyel „befogadóegységeket" (containers) hozhatsz létre, fűzhetsz a rendszeredhez, vagy kezelhetsz bármilyen más befűzött kötethez hasonlóan a számítógépeden, viszont használaton kívül titkosított állományként tárolhatod. Ez védi az érzékeny adatokat a számítógépes kalózoktól vagy bárki mástól, aki illetéktelenül férne hozzá rendszereden tárolt adataidhoz. Minthogy a BestCrypt befogadóegységek tulajdonképpen közönséges állományok, cserélhető adathordozókon lehet őket tárolni, archiválhatók, elektronikus levélmellékletként elküldhetők – egy szó, mint száz, bármilyen más állományhoz hasonlóan kezelhetők. A BestCrypt befogadóegységeket megoszthatjuk másokkal, és távoli ügyfelek befűzhetik. Természetesen egy adott befogadóegységet rendszeréhez egyszerre csak egyetlen ügyfél fűzhet be. Ezenkívül a szóban forgó befogadóegységet mind a windowsos, mind a linuxos BestCrypt-változat képes befűzni, az egyes irányokban bármilyen működésbeli korlátozás nélkül. Mindkét változat ugyanazt az állományformát használja.

A BestCrypt beszerzése és telepítése

A BestCryptet a finnországi székhelyű Jetico, Inc. cég webhelyéről, a ➲ http://www.jetico.com/download.htm címről lehet letölteni. A webhely gyors, a BestCrypt tömör és jól összefogott – a program linuxos változata mindössze 160 K-nyi.

A Windows-változatok kissé nagyobbak, s ez kétségkívül azért van, mert bináris változatokról van szó, ugyanakkor a linuxos változatot forráskód formájában terjesztik. Írásunkban főként a linuxos változatot fogom bemutatni, azonban a windowsos változatról is ejtek pár szót.

Mielőtt megpróbálod telepíteni a BestCryptet, győződj meg róla, hogy Linux-rendszered magjának a forráskódját a */usr/src/linux* könyvtárba telepítetted-e, amelyben a */usr/src/linux* közvetett hivatkozás, vagy éppen rendszermagod főkönyvtára. Ha Linux-változatod szabványos rendszermagját használod, nincs más tennivalód, csak telepítsd a megfelelő változatszámú csomagot – ellenőrizd, hogy a változatszám megegyezik-e rendszeredével, valamint azt, hogy a */usr/src/linux* valóban a forrás főkönyvtárra mutat-e. Ha még sohasem fordítottál rendszermagot a rendszerben, a */usr/src/linux* könyvtárban az alábbi parancsokat szükséges végrehajtani:

```
make mrproper
make menuconfig  # rendszermag-forrÆsk d
                 # itt igØny szerint
                 # beÆll thatod a
                 # rendszermagot
make dep
```

Valójában még a rendszermag újrafordítása is szükségtelen – hacsak nem akarod mindenképpen elvégezni –, ehhez használhatod a `make bzImage modules modules_install` parancsot; a lényeg csupán az, hogy a rendszermag forráskódjának függőségei úgy épüljenek fel, hogy a BestCrypt forráskódjának fordításakor a kiegészítő rendszermagmodulok is helyesen illeszkedjenek a többi rendszeralkotóhoz.
A BestCryptet első alkalommal SuSE 7.1-es rendszerrel működő hordozható számítógépre telepítettem, viszont elfelejtettem, hogy azon a gépen még sohasem fordítottam rendszermagot, emiatt a BestCrypt fordítása meghiúsult. Azonban a fenti módszert lépésről lépésre végigkövetve erőfeszítéseim végül sikerrel jártak.

Rendszergazdaként használni: előnyös vagy veszélyes?

Attól függően, hogy a rendszer biztonsági jellemzői a telepítéskor vagy például a Bastille Linuxban a telepítést követően hogyan lettek beállítva, előfordulhat, hogy hozzá kell szoknunk: bizonyos fájlrendszert érintő feladatokat csak rendszergazdaként lehet elvégezni. Ez többfelhasználós rendszerben teljesen szokványos, mert a hagyományoknak megfelelően a felhasználónak nem kell tudnia fájlrendszereket formázni vagy új köteteket létrehozni.
A BestCryptet azonban nemcsak a rendszergazdáknak szánták, hanem mindenféle rendű és rangú felhasználónak. Mindazonáltal tény, hogy nem kizárólag a rendszergazda rendelkezik érzékeny adatokkal. Az eddig elmondottakon túl azonban a józan ész is azt sugallja, hogy a mindennapi tevékenységek és a nem felügyeleti jellegű feladatok elvégzése során kerüljük a rendszergazdai azonosító használatát. A szövegszerkesztési feladatainkat védelmező titkosított kötetek rendszerbe fűzése és használata nem képez, és nem is kellene, hogy felügyeleti szolgáltatást képezzen.
A BestCrypt az alapértelmezett telepítésnek megfelelően felhasználók által is üzemeltethető. Ugyanakkor a rendszer saját `mkfs` eszközeit használja az új befogadóegységek formázására, emiatt minden BestCrypt-befogadóegységet létrehozni kívánó felhasználónak végrehajtási jogosultságokkal kell rendelkeznie a */sbin/mkfs*, */sbin/mkfs.msdos* és más helyek felett.
Abban az esetben, ha gépünkön – mondjuk egy hordozható számítógépen – mi vagyunk az egyetlen felhasználók, semmi gond sincs azzal, hogy ezek az állományok a világon bárhonnan futtathatók, hiszen jellegüknél fogva talán máris ilyenek.
Ha az állományrendszerek létrehozását nem kívánjuk minden felhasználó számára lehetővé tenni, akkor azokat a bináris állományokat, amelyekhez ezek az állományok tartoznak, tegyük egy adott csoport által végrehajthatóvá és jelöljük ki a csoportot alkotó felhasználókat. Jó megoldás lehet, ha erre a célra önálló csoportot hozunk létre.
A BestCrypt a valóságban a befogadóegységeket közvetlenül kezeli, függetlenül attól, hogy a */sbin/mount* engedélyek hogyan vannak beállítva. A felhasználó csak olyan pontokra fűzhet be befogadóegységeket, amelyek felett megfelelő jogokkal rendelkezik, így felesleges aggódni amiatt, hogy egy rendszergazdai jogokkal bíró felhasználó a */bin*-en keresztül esetleg képes lenne hozzáférni a védett adatokhoz. Mi több, a BestCrypt kifejezetten támogatja titkosított saját könyvtárak létrehozását: az erre vonatkozó részletek a ➲ http://www.jetico.com/linux.htm#tricks címen olvashatók.

A BestCrypt telepítése RPM forráskódból

Ha a rendszermag forráskódja már a helyére került, és a függőségek is helyesen épültek fel, hozzáfoghatunk a BestCrypt összeépítéséhez és telepítéséhez. Ha RPM-alapú Linux-változatot használsz, töltsd le a Világhálóról az .RPM kiterjesztésű forráscsomagot – ez a cikk megírásakor `BestCrypt-1.05b-5.src.rpm` volt –, és a `-rebuild` kapcsoló használatával végezd el a program összeépítését:

```
rpm --rebuild ./BestCrypt-1.0b-5.src.rpm
```

Ez a parancs el fogja készíteni a BestCrypt bináris csomagját – Red Hat rendszeren a */usr/src/redhat/RPMS/i386* nevű könyvtárban, illetve a */usr/src/packages/RPMS/i386* könyvtárban a SuSE Linux, és talán a többi rendszer alatt is. Ezután a program telepítését már bármilyen más csomaghoz hasonlóan végezhetjük:

```
rpm -Uvh /usr/src/packages/RPMS/i386/
    ➥BestCrypt-1.0b-5.i386.rpm
```

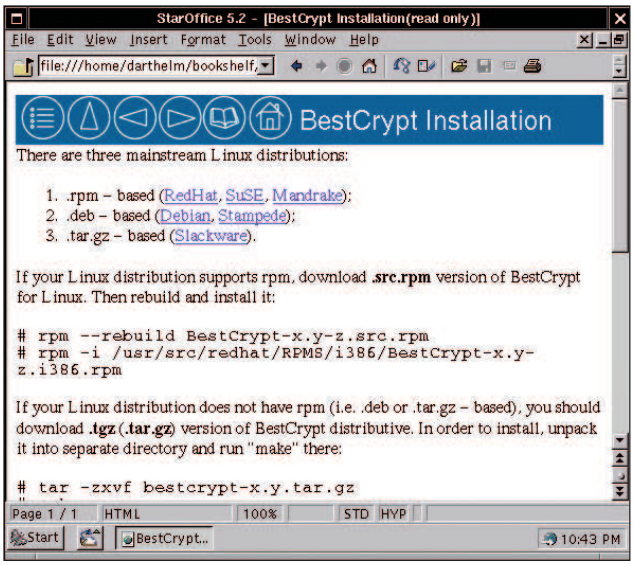
Miután minden BestCrypt bináris és `README` állomány a helyére került, a telepítés utáni héjprogram be fogja tölteni a BestCrypt rendszermagmoduljait. Ha mindezzel megvagyunk, a BestCrypt készen áll a használatra.

BestCrypt telepítése .tar állományból

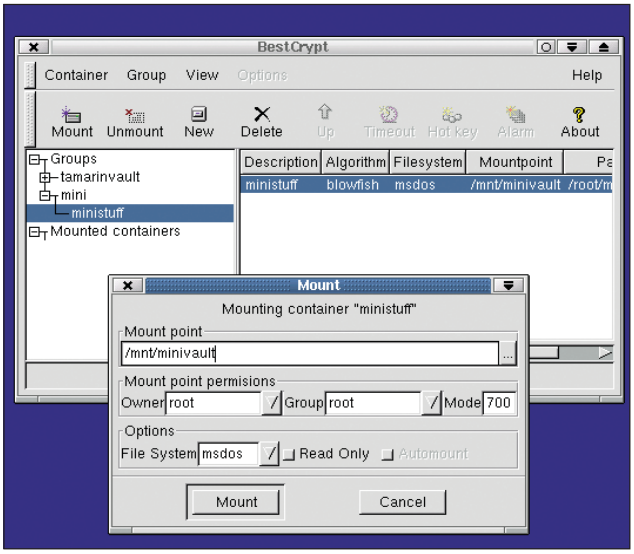
Amennyiben nem RPM-alapú Linux-változatot használsz, amilyen például a Debian vagy a Slackware, akkor az *.RPM* kiterjesztésű forráskód helyett a `tar`-állományt töltsd le – ez a cikk írásakor a `BestCrypt-1.0b-5.tar.gz` állomány volt. Csomagold ki a */usr/src* könyvtárban, tedd a */usr/src/brcypt*-et a pillanatnyi munkakönyvtárrá, és add ki a `make && make install` parancsokat. Amennyiben a rendszermag forráskódja helyesen lett telepítve, akkor a BestCrypt fordításának és telepítésének hibátlanul kell végbemennie.
A *.tar* állományban lévő `Makefile` korántsem olyan bonyolult, mint az RPM-csomag telepítő héjprogramjai. Ebben az esetben a BestCrypt első üzemszerű indítása előtt a program beállítómoduljait kézzel kell betölteni. Ennek egyszerűbb módja a BestCrypt indító héjprogramjának elindítása: `/etc/init.d/bcrypt start`

A BestCrypt leírása és vezérlőpultja

A BestCrypt programcsomagon kívül a leírást tartalmazó *.tar* csomagot is le kell tölteni, amely HTML-oldalakat tartalmazó könyvtárat rejt magában (*1. kép*).
A fentieken kívül még szükséges lehet a *BC_Panel*, azaz *BestCrypt Control Panel* (Vezérlőpult) letöltése. Ez kizárólag rpm-formátumban hozzáférhető, Debian rendszerben pedig az `alien` program segítségével telepíthető. A *BC_Panel* a BestCrypt számára grafikus felhasználói felületet biztosít, amely külsejében nagyon emlékeztet a BestCrypt windowsos változatának grafikus felhasználói felületére.
Minthogy a *BC_Panel*-t e cikk írásának idején a 0.2-1 változatszámmal látták el, valamint az a tény, hogy a parancssoros változat által nyújtott szolgáltatásokat sok tekintetben nem támogatja, arra hívják fel a figyelmet, hogy a programfejlesztési



1. kép A BestCrypt leírása



2. kép A vezérlőpult: BC_Panel v0.2b, a BestCrypt linuxos grafikus felhasználói felülete

szakasz még nem zárult le. Mindent egybevetve azonban a program számos hasznos szolgáltatást nyújt és üzembiztosnak tűnik.

A BestCrypt használata Linux-rendszerben

Egy BestCrypt befogadóegység alkalmazása nem bonyolult feladat, vessünk csak egy pillantást az alábbi példára:

```
bctool new myvault.jbc -s 150M -a twofish -d
"my test vault"
 Enter password:
 Verify password:
```

A `bctool` a BestCrypt egyetlen parancssori eszköze. Egy befogadóegység létrehozásához a `bctool` parancsnak meg kell adni a `new` (új befogadóegység) kulcsszót, az egységet jelző állomány nevét, méretét, a titkosítási algoritmust és az egység leírását. A BestCrypt ezt követően kéri a jelszót.
Használjunk könnyen megjegyezhető, de nehezen kitalálható jelszót. Annak ellenére, hogy a BestCrypt által valamennyi algoritmus támogatott – a DES-t kivéve, 128-bites vagy annál hosszabb titkosítási kulcsot használ a befogadóegységek titkosítására, és már magát az egység kulcsát is a megadott jelszóval titkosítja.
A könnyen kitalálható jelszó tulajdonképpen könnyen megfejthető objektumot jelent, függetlenül attól, hogy milyen hosszú kulccsal titkosították.
Ne felejtsük el a jelszót feljegyezni és biztonságos helyre elzárni, vagy válasszunk olyan jelszót, amelyet minden kétséget kizáróan nem fogunk elfelejteni. A Jetico cég szerint a megadott jelszavak teljes mértékben visszafejthetetlenek, helyreállíthatatlanok, és a BestCryptben semmilyen rejtett megoldás nem létezik a jelszavak korábbi titkosításának megszüntetésére. Ez alapvetően megnyugtató tény, másrészről viszont azt jelenti, hogyha jelszavunkat elfelejtjük vagy elvesztjük, adataink is visszavonhatatlanul veszendőbe mennek! Így az adatok megszerzésére törekvő számítógépes kalóz csak a találgatásban, meg a nyers erőt alkalmazó programok használatában bízhat.
A befogadóegység elkészítése után az állományrendszert is létre kell benne hozni – ez a `bctool format` paranccsal végezhető el:

```
bctool format -t msdos ./myvault.jbc
```

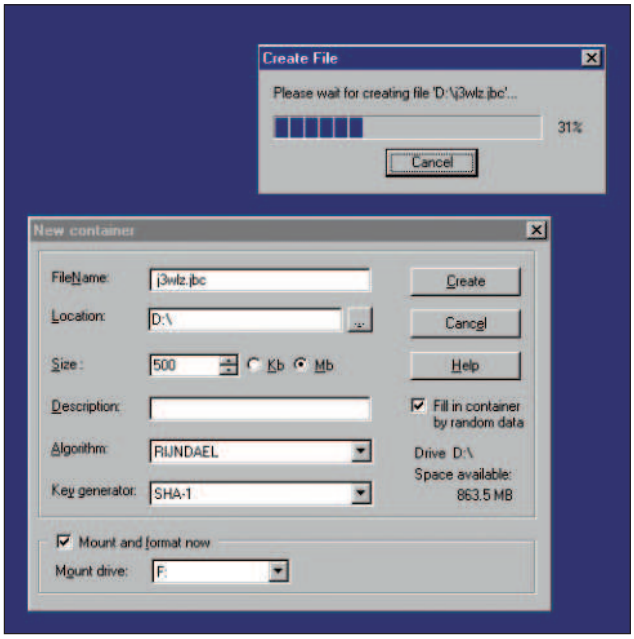
A `-t` kapcsolóval meghatározhatjuk operációs rendszerünk állományformátumát. Amennyiben ezt a befogadóegységet a BestCrypt windowsos változatával szeretnénk megosztani, típusként `msdos`-t kell megadnunk, még akkor is, ha a három karakteresnél hosszabb fájlkiterjesztést megengedő `vfat`-et, vagy a Windows 95-ben megszokott hosszú fájlneveket szeretnénk használni. Ekkor a befogadóegységet `msdos`-ként kell megformázni, de befűzésénél a `vfat` megjelölést kell használni. A BestCrypt a befogadóegység formázásakor az operációs rendszerünk által támogatott összes fájlrendszertípus használatát megengedi.
A BestCrypt befogadóegység létrehozását és formázását követően az egység befűzhető. Az ehhez szükséges `mount` utasítás nagyon hasonló a megszokott `mount` parancshoz:

```
bctool mount -t vfat ./myvault.jbc
➥./mnt/kraunj00lz
```

Innentől kezdve – egészen a leválasztásáig – a kötet ugyanúgy hozzáférhető lesz, mint bármelyik másik könyvtár. Az alapértelmezés szerint a felhasználó- és csoportváltozók annak a felhasználónak a jellemzőit veszik fel, aki a befűzést elvégezte; az engedélyeket a 0700 bájtsor jelzi, azaz `d rw- --- ---`.
Más szóval ez azt jelenti, hogy a rendszergazdától eltérő azonosítóval belépő felhasználóknak nem lesz hozzáférési joguk az egységhez, hacsak szándékosan nem más tulajdonosi jogosultságokkal és engedélyekkel végezzük el a befűzést. Természetesen a `bctool -o`, `-g` és `-m` kapcsolóival a sajátjától eltérő felhasználói azonosítót, csoportot és használati módot is kijelölhetünk. A bővebb részletek és további példák végett olvassuk át a `bctool` leírását. Amint tennivalóinkat a BestCrypt befogadóegységgel befejeztük, az egység az alább bemutatott módon kifűzhető:

```
bctool umount ./mnt/ksraunj00lz
```

Az alatt az idő alatt, amíg a BestCrypt befogadóegység nincs a rendszerbe befűzve, mentést lehet róla készíteni, vissza lehet



3. kép Új BestCrypt-befogadóegység (container) létrehozása Windows operációs rendszerben

tölteni egy korábbi állapotot, másolható vagy a többi állományhoz hasonlóan kezelhető. Ha azonban valamelyik felhasználóhoz be van fűzve, a `bctool` programon kívül mással nem módosítható vagy kezelhető.

BC_Panel: a BestCrypt linuxos grafikus felhasználói felülete

Mint fentebb már említettem, a Linux-rendszerre készített BestCrypt is rendelkezik grafikus felhasználói felülettel, e cikk írásakor azonban még csak próbaállapotú volt.
A ***BC_Panel*** (*2. kép*) a Világhálón csakis rpm-formátumban férhető hozzá. Egyrészről a ***BC_Panel*** – a bináris állománynak valójában a `bestcrypt` nevet adták, úgyhogy az egyértelműség kedvéért a továbbiakban a ***BC_Panel*** elnevezéshez fogok ragaszkodni – megbízhatóan működő, láthatóan jól megírt program, és megjelenésében nagyon is hasonlít windowsos testvérére.
A ***BC_Panel*** azonban a `bctool` szolgáltatásainak csak a töredékét tudhatja magáénak, emiatt a windowsos grafikus felhasználói felület csupán részeszköze a BestCryptnek – a másik két program fejlettségi szintjével egyáltalán nincs összhangban. Vegyük például a ***New*** (Új befogadó objektum) lehetőséget, ahol a párbeszédablak a mintegy tíz választható algoritmus-lehetőség közül csak néhányat sorol fel. Az igazi kellemetlenség azonban az, hogy a ***BC_Panel*** által felajánlott algoritmusok segítségével a befogadóegység létrehozása hibaüzenettel ér véget, hacsak nem rendszergazdaként jelentkeztünk be, és elszántuk magunkat az X-felület futtatására.
Nos, amennyiben tényleg rendszergazdaként léptünk be a rendszerbe, a BestCrypt befogadóegységeken végzett létrehozási, formázási, befűzési és leválasztási műveletek és a más algoritmussal végzett újratitkosítás egyaránt sikeresen ér véget, sőt, a BestCrypt ekkor rugalmasan képes érzékelni és felsorolni a `bctool` által befűzött egységeket, vagyis azokat a köteteket, amelyeken a felhasználó ***BC_Panelje*** olvasási engedéllyel rendelkezik.
Ezek ismeretében az ipari termelésben nem támaszkodnék e termék alkalmazására, a ***BC_Panel*** bizonyos karbantartási feladatok ellátására tűnik hasznosnak, feltéve, hogy nem törődünk azzal, hogy az X-felületet a feladat elvégzése során mindvégig rendszergazdaként kell a rendszerben használnunk. A program tevékenysége viszont mégiscsak ígéretes, és remélem, hogy a Jetico rövidesen megjelenteti a termék ipari környezetben is megbízhatóan használható változatát.

BestCrypt a Windows-rendszerben

Rendben, megállapítottam, hogy a BestCryptet könnyű Linux-rendszerben telepíteni és használni. De vajon milyen mértékig képes együttműködni a Windowszal? Milyen merevlemez-kötet-titkosítási lehetőséget tartogat a BestCrypt a Windows-felhasználók számára?
A hír mind a Windows-felhasználók, mind a Linux-hívők számára kedvező. Az elmúlt héten hordozható számítógépemen felváltva használtam Windows 98-at és SuSE Linux 7.1-et, ugyanazt a BestCrypt-egységet alkalmazva. Ez befogadóegység egy DOS/VFAT lemezterületen található, amely az írási tevékenységemhez használt operációs rendszerek munkakönyvtáraként szolgált. A BestCrypt végig hibátlanul működött, leszámítva azt a néhány ártatlan kék képernyőt, amelyet a Windows bezárásakor láttam, ugyanis a Windows gyakran arra panaszkodott, hogy a BestCrypt-kötet kifűzése után egy vagy több állomány nyitva maradt.
Adatvesztés nem fordult elő, és BestCrypt-kötet használatakor a lemez működésében sem érzékeltem lassulást. Továbbá semmiféle összeférhetetlenséget sem tapasztaltam a befogadóegységet kezelő két BestCrypt-változat között.
Mindkét program egyformán elegáns, és minden más eszköztől eltérően, amelyről mostanában írtam, gyakorlatilag nem

A program előnyei

- a program számos itt felsorolt algoritmust támogat: Blowfish, Twofish, Rijndael, IDEA, GOST, CAST, RC6, GOST, 3DES, DES. Ezenkívül ez a választék a rendszermagmodulok révén számos továbbival bővíthető
- nyílt forrású, modulrendszerű kiépítés – bárki készíthet új algoritmikus modulokat
- a Linux-változathoz tartozó forráskód – kipróbálási és tudományos célok érdekében – nyilvános
- gyors és egyszerű összeépítési és telepítési eljárás
- a jól ismert `mount` parancsot követő felépítés
- a titkosított egységeket a BestCrypt windowsos és linuxos változatai egyaránt képesek használni
- kifogástalan windowsos grafikus felület; a program linuxos grafikus felülete is hasonló elrendezésű
- a kereskedelmi termék a mérsékelt árkategóriába tartozik
- a Windows Corporate Edition (vállalati változat) tartalmazza a több távoli gépre telepített program központi kezelését végző programot
- a kereskedelmi felhasználásokhoz biztosított műszaki támogatás színvonala jó

A termék árnyoldalai

- bizonyos fokig lefordított rendszermagforrást igényel – ez elrettentheti a még kevéssé gyakorlott felhasználókat
- a linuxos grafikus felület nem támogatja az összes parancssori lehetőséget, és a windowsos grafikus felület által nyújtott lehetőségek közül sem mindet

kellett időt fektetnem a leírás hosszas böngészésébe vagy a levelezőlistákban bogarásznom, hogy a BestCryptet Windows alatt is beüzemeljem. Hogy milyen rendkívül egyszerű a BestCrypt windowsos grafikus felhasználói felületét használni, a *3. kép* mutatja be.
Már korábban megismerkedtem a nyilvános kulcsú titkosítás rejtelmeivel, és évekig más eszközöket is használtam, mint amilyen például a PGPdisk. Más szóval azt mondhatom, hogy végfelhasználóként megbízólevelem a gyanakvás – és még nagyon finoman fogalmaztam. A használhatóságot tekintve még mindig örömmel jelenthetem ki, hogy a BestCryptnek a PGPdiskkel egyenlő esélyei vannak arra, hogy a titkosítás élmezőnyébe tartozó eszközzé váljon, és a felhasználói tömegeket a kötettitkosítás és a biztonság zenszerű állapotába juttassa.
Amiben már kevésbé vagyok biztos – a fáradságos kódelemzés és titkosítás alapján –, az az, hogy a BestCrypt verhetetlen. Emberek, remélem, senki sem ragad ki részleteket a fenti mondatomból! Még szerencse, hogy a Jetico munkatársai magas elvi alapokon állnak. Minthogy sem hivatásos titkosítási szakértő, sem programozó nem vagyok, másokra kell hagynom, hogy a BestCrypt által nyújtott biztonság erejét megítéljék.

A BestCrypt nyilvánvaló biztonsága

Annyit elmondhatok, hogy a BestCrypt a közismerten jó algoritmusok lenyűgözően nagy hányadát támogatja – ahogyan talán egyes cinikusabb elmék megfogalmaznák: „crypto-kulcs-szó-megfelelő”, ideértve az Egyesült Államok kormánya által bejelentett Advanced Encryption Standard (Fejlett Titkosítási Szabvány), a Rijndael és az AES-verseny két ígéretes indulóját, ***Ron Rivest*** RC6 és ***Bruce Schneier*** Twofish algoritmusát. Ha az itt felsorolt három módszer túlságosan szokatlan lenne, a BestCrypt támogatja a 3DES-t, a több különböző kulcsmérettel a Blowfisht, az IDEA-t, a CAST-ot és az orosz szövetségi algoritmust a GOST-ot. A BestCrypt ugyan az egyszeres DES-algoritmust is támogatja, de használata nem javasolt, mivel a nyers erőt (brute force) alkalmazó programok számára a kis kulcsméret miatt könnyen feltörhető.
A Windows-felhasználók számára két további lehetőség adott: a csereállomány titkosítása, amely védelmet biztosít a jelszavak és más érzékeny adatok Windows csereállományból történő ellopása ellen, és a BCWipe, az alacsony szintű állománymegsemmisítő. E kettő közül a csereállomány-titkosító szolgáltatás még nem jelent meg linuxos változatban.
A BCWipe programot a Linux-változathoz külön kell megvásárolni, vagyis a Windows-változattól eltérően nem tartozik a BestCrypt csomagba. A BCWipe, a PGP Wipe szolgáltatásához hasonlóan a törléskor hátramaradó adatokat ismételten felülírja, ily módon téve lehetetlenné a helyreállítást szinte bármiféle lemezhelyreállító program számára, talán a legkörmönfontabbakat leszámítva, már ha azok képesek egyáltalán tenni valamit.
Megítélésem szerint a BestCrypt által nyújtott biztonság műszaki szempontból erősnek látszik: számos titkosítási és nem titkosítással kapcsolatos biztonsági módszert támogat.

Összegzés

A termék értékelése során a program által nyújtott szolgáltatásokra, a használhatóságra, a Linux-barát jellemzőkre, az általam kedvelt és hitelesnek elfogadott algoritmusok támogatására, és természetesen a küllemre összpontosítottam. Véleményem szerint a BestCrypt minden területen méltó az elismerésre, és a Jetico által képviselt magas színvonal alapján nem habozok kijelenteni, hogy titkosítási eljárásaik megvalósítása minden részletre kiterjed, és jól működik. Összességében a BestCrypt lenyűgöző programtermék. Ha a megbízhatóságból, a népszerű titkosítási algoritmusok széles kínálatának átfogó és modulrendszerű támogatásából, az általános tömörségből következtetni lehet valamire, hát akkor az az lesz, hogy nagyon biztonságos.
Lelkesedéssel ajánlhatom állományrendszerbeli szükségletek kielégítésére, különösen akkor, ha számítógépünkön Windowst is, Linuxot is használunk. E program segített felélesztени a titkosítás iránt fogékonyabb társadalomba vetett hitemet, ugyanakkor a programmal való játszadozás nagy élvezetet is jelentett számomra.

Linux Journal 2002. június, 98. szám

Mick Bauer (mick@visi.com)
hálózati biztonsággal foglalkozó szaktanácsadó. 1995 óta a Linux elkötelezett híve, 1997 óta pedig OpenBSD prófétaként tevékenykedik. Mick minden kérdést és megjegyzést szívesen fogad.

Adatok

A bemutatótermék készítője: Jetico, Inc.
A cég hivatalos honlapjának címe
➲ http://www.jetico.com

A termékek kereskedelmi ára

- Nem üzletszerű használat esetén a termék ingyenes.

A Linux-változatokhoz való programok árai

- A BestCrypt egyfelhasználós Linux-változata kereskedelmi, illetve kormányzati felhasználás esetén: 49,95 dollár.
- A BCWipe lemezterület biztonságos törlését végző segédprogram: 29,95 dollár.
- A BestCrypt egyfelhasználós változata Windows 9x/ME/NT/2K/XP rendszerekre: 89,95 dollár.
- A BestCrypt Corporate Edition Windows 9x/ME/NT/2K/XP rendszerekben használható vállalati változatának kereskedelmi, illetve kormányzati felhasználása egy felhasználóra vonatkoztatva: 149,95 dollár.

A program működésének feltételei

- Linux 2.2.0-s rendszermag, vagy ennél fejlettebb – ideértve a 2.4.x rendszermagokat is.
- A rendszermag forráskódja a */usr/local/linux* könyvtárba legyen telepítve.
- Aa telepítésre kiszemelt számítógép i386 felépítésű legyen – a program más felületen is üzembe helyezhető, de egyéb területen még nem vizsgálták a működését, és előfordulhat, hogy az adott i386-ostól eltérő környezetet a program nem támogatja.