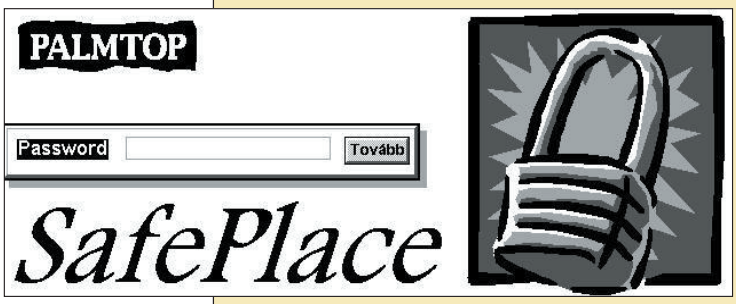
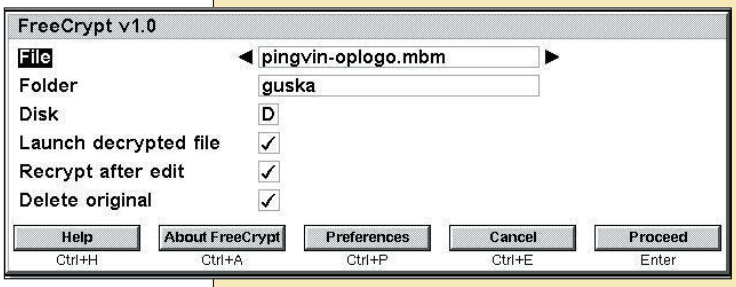
Biztonságosan!

Az informatikusok az elmúlt pár év egyedfejlődése során a „kutyus95” típusú jelszavaktól eljutottak a „GCV”!fAZ@,E)J($rW” típusú jelszavakig. A kérdés tehát: milyen is az a megjegyezhető jelszó, amely megfelelően védi a rendszerünket, továbbá hogyan tároljuk és használjuk? A lelkem mélyén lakozó paranoid azt





súgja, hogy a jelszó mindig a 2. példához hasonló bonyolultságú legyen. Ez idáig rendben is van, de ha egy olyan emberre kényszerítjük rá a fenti jelszót, aki még a kutyus95-öt sem képes megjegyezni, csak azt érjük el, hogy felírja egy papírra. Bár a szólásmondás szerint „a szó elszáll, az írás megmarad”, a mi esetünkben legfeljebb így hangozhatna: „a szó elfelejtődik, a papírra felírt jelszó viszont idegen kézbe kerülhet”. Az eszményihez közelítő állapot, ha bonyolult, általunk sem megjegyezhető jelszót választunk, amelyet egy PDA-n vagy egy titkosított állományban helyezünk el. Bár mindez bonyolultnak és fölöslegesnek tűnhet, ám ha belátjuk, hogy minden géphez külön jelszót kell használnunk, vagy akár minden karbantartáshoz is másikat, a fenti eljárás mindenképpen indokolttá válik. Ha jelszavainkat PDA-n tároljuk, nagyon fontos, hogy olyan alkalmazást válasszunk, amely az adatbázist is megfelelően védi. Számtalan olyan alkalmazás létezik, amely nemcsak az adatbázist (a jelszavainkat) rejti kódoltan, hanem a memóriában is így tárolja őket; és ha az alkalmazás kikerül a működés középpontjából, azonnal jelszóval védi. Ebben az esetben a PDA-t magát érdemes védenünk a lopás és a hozzáférés ellen, viszont ha mégis elhagynánk, akkor sincs nagy baj, csak mielőbb meg kell változtatnunk hozzáféréseink jelszavait. A PDA azonban egy életstílus, amely igen költséges és sokan fölöslegesnek tartják. Ezzel szemben a kereskedelmi forgalomban egyre elterjedtebbek lettek a különféle memóriakártyás megoldások. A sok-sok CF-alapú kártya közül mindenki kiválaszthatja magának a legkedvesebbet, amely méretével illeszkedik az életstílusához, valamint a gépével is együttműködik. Miért is jó kivehető (nem felejtő) memórián tárolni a jelszavakat? Mert bármikor bárhol kéznél van, mert titkosított állományrendszert rakhatunk rá – és mert olcsó. Számomra az USB-felületre csatolható PEN DRIVE volt a legszimpatikusabb, amely 15 000–20 000 forintos árával még az elfogadható kategóriát képezi, és USB-felület szinte mindegyik gépben megtalálható. Ez egy olyan tollalakú eszköz, amely nem nagyobb egy kihúzófilcnél – 64 MB és 128 MB összeállításban kapható. Az USB-kapura csatlakoztatva az `usb-storage` modullal tudjuk meghajtani, amely *0*-ként csatolható rendszerünkhöz. Innentől kezdve adva van a lehetőség, hogy titkosító fájlrendszert rakjunk rá, ezzel is biztosítva magunkat, ha esetleg illetéktelen kezekbe kerülne. A két hónappal ezelőtti számban egy igen részletes írás szólt arról, hogyan készítsünk ilyen rendszert, én mégis a loop-aes rendszer megépítését ajánlom, mert GPL-es program esetén ezen biztosított, hogy titkosító rendszerünk minden rendszermagváltozat alatt használható, illetve olvasható lesz. Telepítése egyértelmű, a letöltés után leírását a README állományban megtaláljuk. A titkosító fájlrendszer elkészítése után még ne dőljünk hátra, hiszen nem tettünk meg mindent a biztonságért. Ha elhagyjuk vagy ellopják, a CFS (titkosított fájlrendszer) véd minket, de ha ezt a GPG biztonságával is kombináljuk, talán végre nyugodtan alhatunk. Így minden jelszót tartalmazó állomány eleve egy titkosított rendszeren tárolódik, ráadásul GPG titkosított állományként. Kínálja magát a lehetőség, hogy SSH-kulcsainkat is ezen a médián tároljuk, így ha kiugrunk ebédelni, a gépből csak kihúzzuk a kártyát, és a nyakunkba akasztva biztosak lehetünk benne, hogy aki ebéd közben a gépünk elé ül, az ma kulcsok nélkül fog távozni.

Éljen a paranoia!

Kapcsolódó címek

- ➲ http://loop-aes.sourceforge.net/
- ➲ http://www.pendrive.com
- ➲ http://www.gnupg.org
- ➲ http://www.openssh.org
- ➲ http://www.crypto.com

Varga S. Csaba (guska@guska.hu) az 1.1-es Slackware óta linuxozik. Kedvtelései közé tartozik a fotózás és Linux telepítése PDA-kra. Legszívesebben a Gerecsében túrázik a barátaival.