

A magánélet biztosítása Szabad Szoftverekkel



Varga Csaba Sándor
sandor.csaba.varga@kim.gov.hu

Mit tekintünk kényes iratnak?

- Mindent olyan adatot, amely nyilvánosságra kerülés esetén kellemetlen lehet

Például:

e-mail/SMS/log/szerződés/hívásnapló/kényes házi videó, okostelefon!

- Alapvető hozzáállás:
 - Nincs olyan titkosítási eljárás, amely bizonyos időn belül ne lenne visszafejthető
 - Kombináljunk, és használjuk ki a maximumot, minden új lehetőséget



Ne csak a dokumentumot védjük!

- Védjük a médiát, amire felkerül (disk, pendrive, flash, dat stb.)
- Védjük adatvesztés ellen, ha nem akarjuk megtudni, hol van a székháza a Kürt Kft.-nek
- A backup is ugyanolyan veszélyes és védendő, mint az eredeti anyag
- Katasztrófa- és rablásvédelmi szempontokból tartsuk a telephelytől távol a mentést
- P: WTC / OEP
- A fénymásoló is lehet intelligens kém 2004-től



Kezdjük a kályhánál!

- Titkosítsuk magát az adatkapcsolatot! Wi-Fi !
- Két telephely között, vagy akár az otthon VPN
- Wi-Fi vagy 3G?

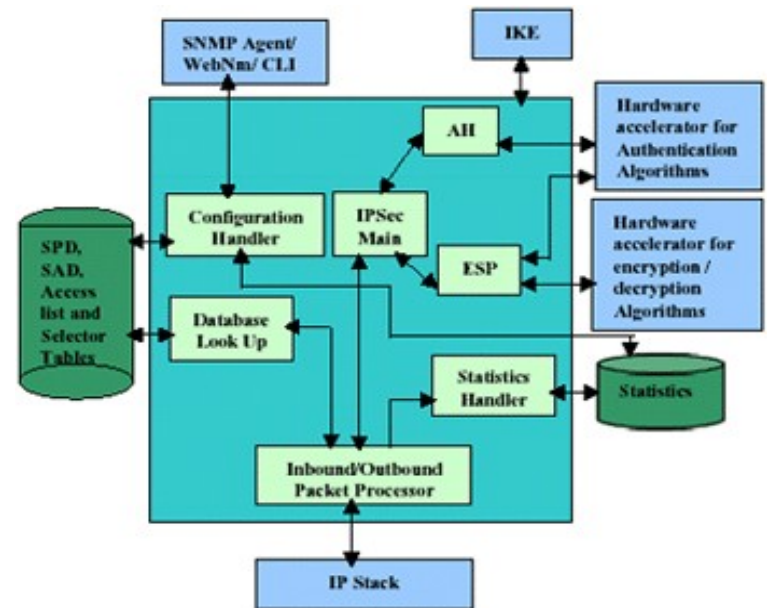
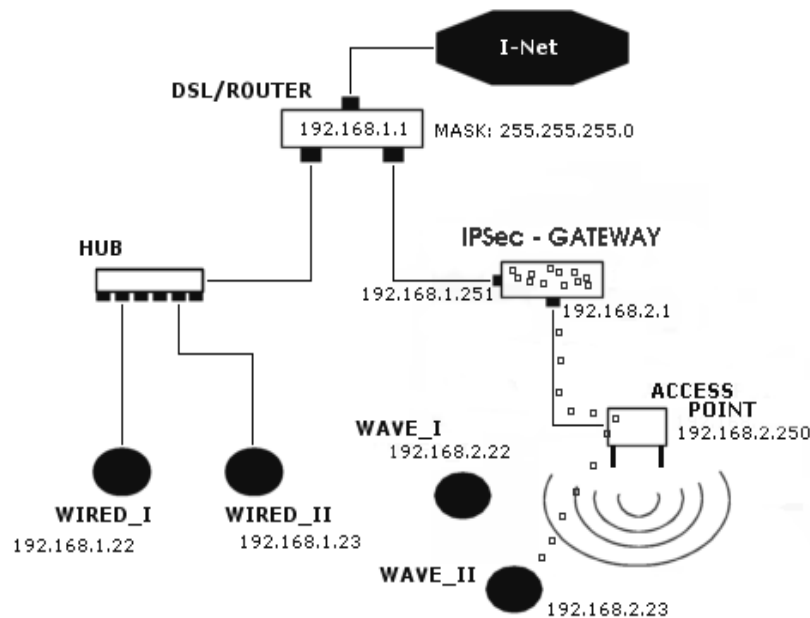
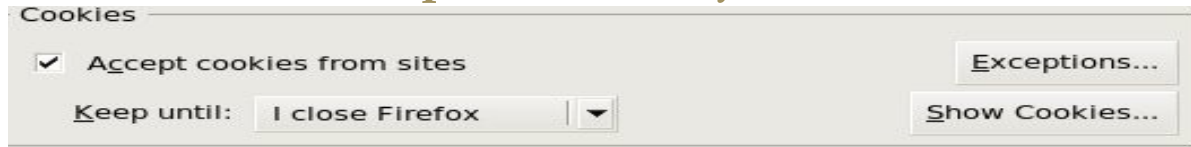


Figure 1. FutureSoft IPSec Architecture

Böngésző – barát vagy ellenség

- Cookie törlés kilépésnél + kényes adatok



- No Script !
- Addbolck+Filter Updater
- Https vagy SSH socket Proxy 2 kattintásból
- Show IP
- Netcraft toolbar
- Adaptive Referer remover/Web GPG plugin
- Flash Block – Kamera és Mic ki/be kapcsolása API-ból
- FF bővítmény kezelése, avagy ki telepít mit és hova ?



Internetbank a kényelmes ellenség

- Miért használnak még mindig 128-256-es titkosítást?
- Nat mögül biztonságos?
- SMS vagy Token?
- Minden esetben egyeztessük az IP-t és az SSL-t is
- Azonosítás telefonban és számlainfó SMS-ben.
- Azonosítás bankfiókban.
- Vásárláskor miért írják fel a kártya számot?
- Ssh socket proxy (tsocks)és Virtualbox Firefox?
- Akkor marad a párna ciha?



Határ a kényelem és a biztonság között

- Google a jó barát?
- Gtalk, Gmail, Gcal, GoogleDoc?
- Skype? - Chroot – Rootkit? Mic Off?
- VOIP hívások az interneten?
- DECT telefonok – Titkosítási algoritmus és hívásnapló



Biztonságos Chat

- Pidgin
- Az összes létező protokoll támogatása: Msn/AOL/ICQ/JABBER/Gtalk/stb
- OFF The Record Plugin
- Gpg Plugin
- Gaim Encryption RSA kulcspárok
- Csevegés rögzítés ki/be
- Kiegészítő hardver kezelése, pl.: villogtatás



Az okostelefon mint PC

- Az Android világszertei törekvései és felépítése – Killing Switch
- Minden egy kézben, OTP auth. bankolás
- Biztonsági megfontolások: egybe épített telefon, Zárolás AES256
- App: csak annyi és csak az és csak olyat telepítsünk, amiben 100%-osak lehetünk
- BYOD: a belső ellenség
- A frissítések fontossága és a gyártók hanyagsága
- IOS hack, mert nem csak az android lukas.
- Mentsük a felhőt!



- A gépeket minden esetben védjük tűzfalal, lehetőleg applikációs szintűvel – firestarter – GUFW (Ubuntu)
- Szinte minden TCP/IP kapcsolat levédhető valahogyan:
 - Ftp: SFTP/ Open SSL Ftp/ SCP,SSHFs
 - Mail: SSL Pop-Imap / SSMTP / végső eset Ssh port fw
 - Ssh: Csak kulcs használatával – AllowUser direktiva
 - Web: apache-ssl, Open SSL
 - VNC: Ultravnc
- Akkor most a logmeIN is jó ?
- Az adminisztratív portokat soha ne a megszokott helyen használjuk – Security by obscurity



Miért nem jó nekünk a felhő ?

A jövő márpedig a cloud computing!

Dropbox :) Ubuntu One stb.



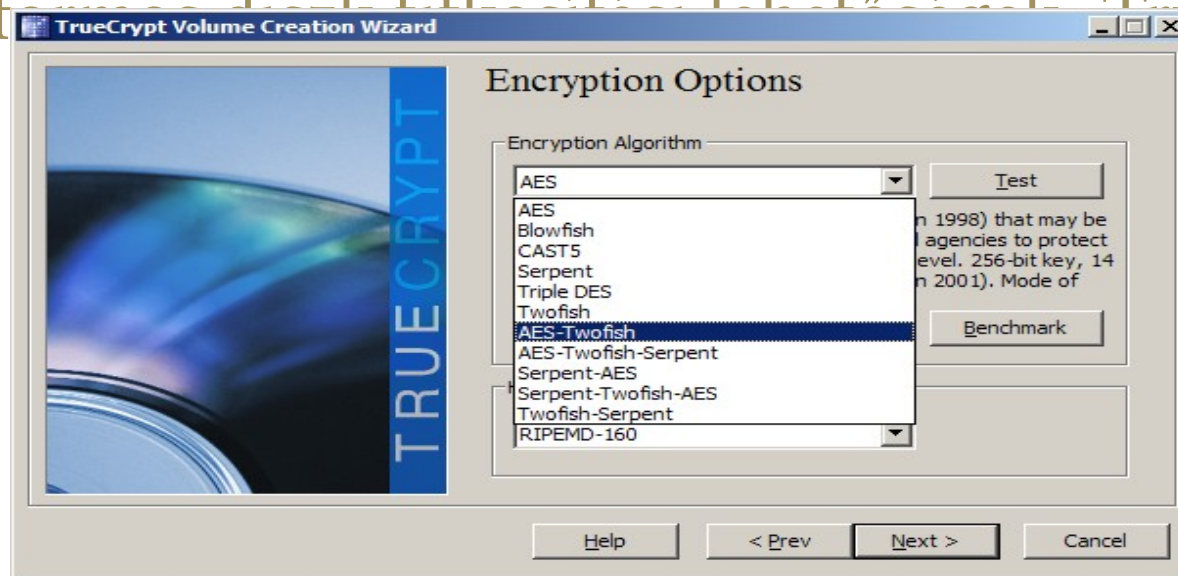
E-mail/SMS

- VI és a GPG szoros kapcsolata plugin segítségével
- Az e-maileket titkosítsuk GPG/PGP párossal, lehetőleg minden esetben, ezzel is megzavarva a lehallgatót, hiszen a jelentéktelen levelek is kódolás alá esnek így.
- Sose írjunk titkosított levélhez valós 'Subject'-et. Hiszen az nincsen titkosítva, a levél törzsébe, amely titkosított, oda már írhatunk.
- A titkosított levél törzsébe mindig rakjuk bele az eredeti feladót és címzettet, mert azt biztosan nem lehet menet közben manipulálni.
- Az SMS ugyanolyan könnyen hamisítható, mint az e-mail.



Adathordozón való tártolás

- Legyen az pendrive vagy 1 TB-os merevlemez, a kényes adatainkat tartsuk Crypto Image-ben.
- Multi platformos titkosítási lehetőségek: True Crypt



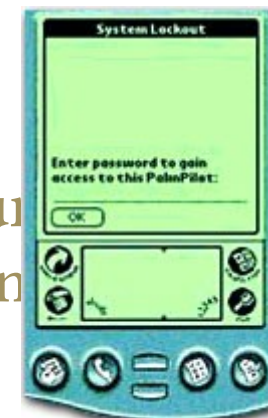
- Loop-AES
- Luks

- A loop-AES titkosítási és adattárolási módszer kombinálható a gpg -vel, így nagyobb adat biztonság érhető el.



Jelszavak és a papír

- Az eddig bemutatott technikák alapja, hogy rendelkezünk egy jelszóval vagy kulccsal, amely nyitja az adattárolónkat. A kulcsot is titkosítva érdemes tartani. :)
- Erre jó lehet egy PDA, akár 10-20e Ft-os is, csak lehessen rá telepíteni olyan applikációt, amely megfelelően védhető, pl. Cryptopad
- A jelszavakat generáljuk, pl. PWGEN-nel, és havonta változtassuk.
- Ha pedig elfelejtettük a jelszó jelszavát, és kizártuk magunkat véglegesen minden rendszerből, akkor kezeljük magunkat pszichiátrián.



Backup

- Artisjus védett CD/DVD lemezek minősége.
- Többszörösen biztosított és különböző titkosítást használó USB drive mentés (más-más gyártó és széria!!) ha nincs kazetta. Remote backup GRSYNC+SSH
- Villám és túlfeszültségre való felkészülés, akár fizikai leválasztás segítségével is.
- Wi-Fi-n nem mentünk, hanem publikálunk!!! (Time Machine)
- Mentés-visszaállítás, időzítetten. Kisvállalati környezetben legalább egy banki trezor.

