NOLA GNU PrivacyGuard (GPG)

Egilea: kurtsik kurtsik_x@euskalerria.org

GPG gako publikoa: www.rediris.net/pgp (kurtsik-berria)

0.5 bertsioa 2003-08-18

LDP-eus : http://www.librezale.org

Aurkibidea:

1.-Sarrera:

Interneten oinarriak finkatu zirenean azkartasuna eta inplementatzeko erreztasuna izan ziren irizpideak baina segurtasuna edo pribazidadea ez zen, inondik ere, eskema horren barruan sartu, batez ere garai horretan tekniko eta informatikoen tresna zelako, laborategiko proba. Ezin izan zuten gaur egungo hedapena aurrikusi.

Internet bidezko komunikazioa, sortu zenetik hona behintzat, askatasunaren paradigma izan da: ustezko anonimatoa, azpiegitura urriarekin informazioa zabaltzeko aukerak, unibersalizazioa,... . Gaur egun gauzak aldatu egin dira: telebistan, ia egunero, ikus ditzakegu pirata informatikoei buruzko berriak gure pasahitz edo kontuen bila; gaztetxoak, aspertuta edo, sarea arakatzen; enpresak datu pribatuen gosez; gobernuak edo gobernuen aparatuak “1984” egi bihurtu nahian;... .

Batez ere “Irailaren 11” famatuaren itzalpean oinarrizko askatasunen izugarrizko murrizketak justifikatu nahi dituzte: Estatu Batuak **Echelon** sistema eta bere troyano partikularra **Magic Lantern** jarri du abian komunikazio elektroniko **guztiak** filtratzeko; Europako gobernuak, bere aldetik **Enfopol** sortu du; Espainako gobernuak, internauta eta legegileen iritziaren kontra, **LSSI** inposatu du; Estatu Batuetan enkriptazio sistemak legez kanpo jartzeko ekimenak; etab... .

Informazio hau guztia gobernuen eskuetan egongo dela pentsatzearekin zure burua lasaitu nahi baduzu hamaika dira adibideak demostratzen digutenak garantiarik gabeko kontrol soziala gehiegikeriak baino ez dakartzala: Estatu Batuetan polizia batek departamentuko datuak erabili zituen bere emazte ohia bilatzeko eta hiltzeko. Australian beste polizia batek datu basea erabili zuen herriko neskeei buruzko informazioa topatzeko, “neska-lagun egokia” topatu nahi zuen. Estatu Batuetan berriro, FBIko funtzionario bat harrapatu zuten bigilantzia elektronikoen bitartez lortutako datuak mafiari saldu nahi zizkionean. Mitxigango polizia burua atzilotu zuten poliziaren sarea erabiltzen ari zelako bere dimisio eskatzen zuen talde bat espiatzeko. Benetan uste duzu lasai egon gaitezkeela?.

Beno, ikusten denez azaltzen saiatu naizen ikuspegia ez da oso lasaigarria, hala ere oraindik aukerak badauzkagu. Horixe azaltzea da lantxo honen helburua.

2-Enkriptazioa da bidea:

Nik ez daukat zer izkutatzerik, zergatik keskatu bekar dut?. Hau da sarritan entzuten dudan galdera enkriptazioa aipatzen dudanean, nik beste galderarekin erantzun ohi dut:ez baduzu zer izkutatzerik zergatik ez dituzu gutunak gutunazalik gabe bidaltzen?. Erantzuna oso sinplea da: zuk idazten duzuna, zure kreditu txartelaren zenbakia, lan eskaera edo maitasun olerkia kontu pribatuak dira, ez ditu inork zertan irakurri behar. Legeak berak zigorrak aurrikusten ditu eskubide hau, intimitate eskubidea hain zuzen, zapaltzen duenarentzat. Ez al da kasu bera posta arruntarena eta elektronikoarena?. Gaur egun interneten bitartez bidaltzen duguna ia beti “gutunazalik” gabe igortzen dugu, edonork gure komuniokazio osoa harrapa dezake eta gainera ez da bitarteko tekniko handirik behar hori lortzeko.

Baina lasai egon, dena ez dago galduta. Arau batzuk segituta gure

komunikazioa, erlatiboki, segurua egin dezakegu. Aukera ona eta erreza gure komunikazioa enkriptatzea da.Baina, zer da hori?

Enkriptatzea gure artxibategiaren karaktereak tresna baten bitartez izkutatzea da, komunikazioa harrapatzea lehen bezain erreza izango da baina inork ezin izango du ezer ulertu. Soilik guk zehaztutako pertsonak, jasotzailea, edukiko du gakoa mezua desenkriptatzeko eta irakurtzeko.

Enkriptatzeko tresna guztien artean GPG aukeratu dut, batez ere hiru arrazoiengatik:
-Oso enkriptazio tresna sendoa da, gaur dagoen maila teknologikoarekin praktikan apurtezina.
-Gako publikoko sistema (ikus 3. puntua) da, sistema hauek ggakoen banaketa errezten dute.
-Software librea da, iturburu kodea edonork eskura dezake. Horrela atzeko ate edo troyanorik ez daukala ziurta daiteke.

3-Enkriptazio sistemak. Gako publikoko sistemak:

Badaezpada enkriptazioaren kontzeptua argi geratu ez den adibide errez bat jarriko dut: demagun “Kaixo mundua” nire lagun bati bidali nahi diodala eta gainera enkriptatua. Horretarako sistema bat pentsatu beharko dut.

ABDEFGHIJKLMNÑOPRSTUXYZ
XYZABDEFGHIJKLMNÑOPRSTU

Konturatzen bazara bi lerroak berdinak dira (alfabetoa) baina behekoan hizkiak hiru posizio daude aurreratuta. Gure adibidean goiko taula **enkriptazio sitema** izango da eta hizkiak hiru postu daudenez mugituta **gakoa hiru** izango da. Hartuko dugu berriro “Kaixo mundua” esaldia, lehenengo hizkia “k” da, goiko lerroan bilatuko dugu eta “k”ren azpian “h” dago, ba hori hartuko dugu. Gero “a”, “a”ren azpian “x”..... horrela amaitu arte. Mezua enkriptatuta daukagu eta horrelako itxura dauka:

HKFSMJRKZRX

Ez da ezer ulertzen. Momentu honetan jasotzaileari enkriptazio sistema (taula) eta gakoa (3) jakinarazi behar diot, taulan beheko lerroan bilatuko ditu hizkiak eta zein dagokie goiko lerroan (gakoa kontuan hartuta). Sistema honek **gako simetrikokoa** du izena, hau da, gako berbera erabiltzen da enkriptatzeko eta desenkriptatzeko. Sistema mota honek desabantaila batzuk ditu: adibidez, gako berbera izanda guztientzat edonork irakurri dezake guk enkriptatutako mezua nahiz eta jasotzailea ez izan, edo gakoa era seguruan zabaltzeko zailtasunak.

Arazo hauek guztiak gako asimetrikoko sistemekin gainditu ziren. Ideia oso sinplea da: gako bakarra sortu beharrean bi gako sortzen dira, bat publikoa (edonork guri zuzendutako mezuak enkriptatu ahal izateko) eta beste bat pribatua (guri zuzendutako mezuak desenkriptatu ahal izateko). Kontzeptua ere oso desberdina da, sistema simetrikoetan igorleak sortzen zuen gakoa eta jasotzailea helerazten zion, kasu honetan justu aldrebes da, jasotzaileak sortzen du gakoa (publikoa) eta igorleak lortu behar du mezua bidali ahal izateko.

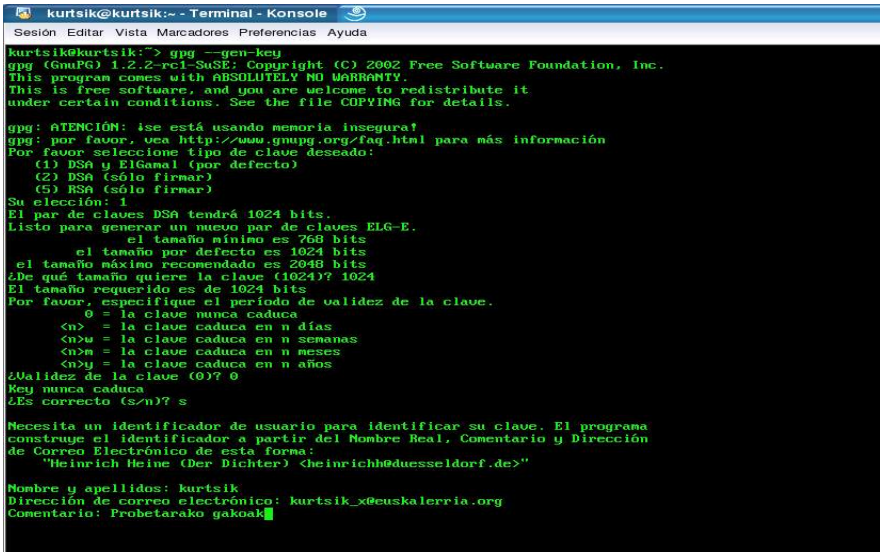
4-Instalazioa eta konfigurazioa.

Instalazioak ez dauka inolako zailtasunik, distribuzio guztiek dakarte rpma, dena den bertsiorik berriena nahi baduzu helbide honetan topatu ahal duzu: www.gnupg.org. Behin instalatuta lehenengo pausua gakoak sortzea da.

4.1-Gakoak sortzen.

Lehen ikusi dugun moduan sistema hauetan bi gako sortzen da: publikoa eta pribatua. Publikoa saiatu behar dugu ahalik eta gehien

zabaltzen edonork lortu ahal izateko, normalean gako bankuetan jartzen dira , adibidez “Rediris”en (Ikus. 6. puntua). Pribatua berriz ondo gorde behar dugu, gainera diska gogorrean gordetzen denez eta edonor gure ekipoan sartzen bada ikusi ahal duenez kontraseinu batekin babezten da (hori da gako pribatua erabili nahi dugunean idatzi behar duguna).



Gakoak sortzea erreza da: konsola batean eta **erabiltzailearen kontuan** hauxe idatziko dugu:

$> gpg –-gen-key

Orduan gako mota aukeratu behar izango dugu, kontrako arrazoi onik ez baduzu defektuzkoa aukeratu, DSA-ElGamal. Ondoren tamaina, defektuzkoa ondo dago (1024 bit) baina nahi izanez gero 2048 bit arte jarri ahal dugu.

Hurrengo pausua iraungitze data zehaztea izango da, kasu gehienetan iraungitze datarik ez jartzea erosoena izango da. Honen ostean identifikadoreak (ID, geroago gako honi erreferentzia egiteko erabiliko duguna) sortzeko galdera batzuk egingo dizkigu: gure izena, eposta helbidea,.... . Eta azkenik gako pribatua babesteko pasahitza eskatuko digu. Gako hau ondo aukeratzea oso garrantzitsua da hau izango baita gure gako pribatua babestuko duena. Ez dago inolako mugarik tamainan eta maiuskulak eta minuskulak nahaztea komenigarria da.

Eskura daukagun beste segurtasun aukera bat errebokatze zertifikatua da, hau oso erabilgarria da gure gako pribatua galtzen badugu eta hura erabiltzeko pasahitza. Zertifikatua egiteko:

$> gpg –gen-revoke [ID] > errebokatze.asc

Zertifikatua leku seguruan gorde behar duzu, pentsa ezazu norbaitek eskuratzen badu zure gakoa erabiltezin bihur dezakeela.

4.2-Gakoak kudeatzen.

Behin gure gakoak sortuta, besteenak gehitu behar ditugu gure eraztunean (horrela deitzen zaio gako publikoen bildumari). Horretarako normalena gako banku batean bilatzea izango da (Hurrengo puntua ikusi), testu artxibategi batean gordeko dugu, laguna.asc adibidez, eta honako hau izatziko dugu kontsolan:

$> gpg –import < laguna.asc

Horrela gorde nahi ditugun guztiekin. Hurrengoa gakoak aktibatzea eta konfidantza maila zehaztea da, horretarako giltzak banan-banan editatuko ditugu:

$> gpg –edit-key [ID]

GPGren shell batean sartuko gara, aukera guztiak ikusi nahi badituzu bartan 'help' idatzi, baina guri interesatzen zaizkigunak bi dira:
-Enable: gako hori gaitzen du.
-Trust: zein kofidantza maila ematen diogun gako horri.

Dena gure gustura daukagunean ideia ona izaten da gure gako guztien backup egitea:

-$> gpg –export-all > eraztuna.asc # Gakoen erastun osoa esportatzeko.

-$> gpg –export-secret-keys # Gako sekretuak esportatzeko

Ondorengo aginduek ez dute konplikazio handirik, egingo dudana beraz zerrendatzea baino ez da izango:

-$> gpg –delete-key [ID] # Gako publiko bat eraztunetik ezabatzeko.

-$> gpg –delete-secret-key [ID] # Gako publiko eta pribatu bat ezabatzeko.

-$> gpg –list-keys # Gure eraztuneko gakoak ikusteko.

-$> gpg –check-sigs [ID] # Gako baten sinadurei buruzko informazioa lortzeko.

Atal honetan, besteetan bezala, askoz aukera gehiago dago, ikusi nahi badituzu man orriak edo beherago dauden loturak ikusi ahal dituzu.

4.3-Gakoak zabaltzen.

Lehen esan dugun moduan sistema honen atal garrantzitsua gure gako publikoa edozeinentzat eskuragarria jartzea da eta horretarako sortu dira **gako bankuak**. Gako bankuak dira gako publikoak jartzeko eta

bilatzeko webguneak, zerrenda bat baherago aurkituko duzu loturen atalean.

Prozesua oso erreza da, lehenengo gauza gure gako publikoa asci formatuan esportatzea da:

$> gpg -a –export [ID] > publikoa.asc

Atera zaigun testua bankuen orrialdeetan dauden horretarako lekuetan kopiatuko dugu eta badago. Ideia ona da gure emezuen sinaduran gure gakoa non topatu ahal den adieraztea.

5-GPG, erabilpena:

GPGren erabilpena oso erreza da. Fitzategi bat enkriptatu nahi badugu honako hau idatziko dugu:

$> gpg –encrypt fitxategia.pdf

Orduan GPGk galdetuko digu zein gako publikorekin enkriptatu nahi dugun (bat baino gehiago aukeratu ahal dugu, guztiak sartutakoan enter sakatu amaitzeko) eta badago. Enkriptatutako fitxategiak .gpg estensioa izango du.

Kontrako prozesua egiteko, hau da, desenkriptatzeko ondorengo lerroa idatzi, gero gako sekretuaren gakoa eskatuko digu eta badago.:

$> gpg –decrypt fitxategia.pdf.gpg > fitxategia.pdf.gpg

Aurreko kasuetan bezala aukera gehiago dago baina eskuliburu txiki honetan ez gara sartuko, badakizu man gpg..... ;-).

5.1-GPG aplikazio baten barruan. Kmail:

Lehenengo gauza da aplikazioa konfiguratzea GPG erabiltzeko, ez badakizu zelan egin www.librezale.org LDP-eu atalean Kmail konfiguratzeko eskuliburu bat lor dezakezu.

Hurrengoa mezua idaztea da. Goiko tresna barran bi irudi ikusiko duzu:

-Sinatzeko soilik 

-Sinatzeko eta enkriptatzeko 

Ondoren gakoa idatzi beharko dugu eta badago mezua enkriptatuta. Dena den gauza bat oso argi eduki behar duzu: sistema

honekin fitxategi erantsiak ez dira enkriptatzen, horrelako fitxategi bat bidali nahi komando lerroan egin beharko zenuke eta gero erantsi.

6-Helbide bilduma:

-Webgune nagusia:
http://www.gnupg.org/(en)/index.html
-GPG gaztelaniaz:
http://www.gnupg.org/(es)/index.html
-Kriptopolis:
http://www.kriptopolis.org

Dokumentazioa:

-Eskuliburu bat:
http://www.colettis.com.ar/~daniel/tutoriales/
-GPG Mutten:
http://www.linux.org.ar/LuCAS/COMO-INSFLUG/COMOs/Mutt-GnuPG-PGP-Como/
-Beste eskuliburu bat:
http://www.linux.org.ar/LuCAS/COMO-INSFLUG/COMOs/GPG-Mini-Como/

Gako bankuak:

-RedIris:
http://www.rediris.es/cert/servicios/keyserver/
-Escomposlinux:
http://pgp.escomposlinux.org/
-Mondragon Unibertsitatea:
http://pgp.eteo.mondragon.edu/